UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF GEORGIA
ATLANTA DIVISION

UNITED STATES OF AMERICA *ex rel.* CHRISTOPHER CRAIG and KYLE KOZA,	)	Civil Case No.: 1:22-cv-02698-JPB
Plaintiff,	)	**JURY TRIAL DEMAND**
v.	)	
GEORGIA TECH RESEARCH CORP. and BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA (d/b/a THE GEORGIA INSTITUTE OF TECHNOLOGY),	)	
Defendants.	)	

UNITED STATES' COMPLAINT-IN-INTERVENTION

Plaintiff the United States of America (United States) brings this action against Defendants Georgia Tech Research Corporation (GTRC) and the Board of Regents of the University System of Georgia, doing business as the Georgia Institute of Technology (Georgia Tech), seeking relief under the False Claims Act (FCA), 31 U.S.C. § 1379, *et seq*. and federal common law for their failure since at least May 2019 (the relevant time period) to meet cybersecurity requirements of Department of Defense (DoD) contracts.

In support of its claims, the United States alleges as follows:

NATURE OF THE ACTION

1. The federal government, including the DoD, imposes cybersecurity requirements on defense contractors for the purpose of protecting non-public government information that resides, passes through, or can be accessed by contractor information systems.

2. As DoD has explained, these cybersecurity requirements are "necessary to address threats to the U.S. economy and national security from ongoing malicious cyber activities, which includes the theft of hundreds of billions of dollars of U.S. intellectual property." The threat of cyberattacks is particularly acute for the Defense Industrial Base (DIB), including the hundreds of thousands of defense contractors that work with DoD, which often process, store, or transmit valuable nonpublic government information.

3. As DoD has warned, "[m]alicious cyber actors have targeted, and continue to target [defense contractors and] can exploit the vulnerabilities of contractors' networks and systems and exfiltrate information related to some of the Nation's most valuable advanced defense technologies." In particular, "actors ranging from cyber criminals to nation-states continue to attack companies and organizations that comprise the Department's multi-tier supply chain . . . [and] seek to steal DoD's intellectual property to undercut the United States' strategic

and technological advantage and to benefit their own military and economic development."

4. This is not a theoretical threat, particularly at the nation's top research universities. Since at least 2011, the FBI has warned that universities are prime targets for cyberattacks by foreign adversaries. As the FBI has explained, "foreign intelligence services and non-state actors use US colleges and universities to further their intelligence and operational needs." Georgia Tech itself has fallen victim to cyberattacks. In 2019, Georgia Tech announced that the records of 1.3 million individuals had been compromised because of a cyberattack.

5. Consequently, as DoD has continuously warned for more than a decade since it first began enacting cybersecurity regulations in 2013: "Defense contractors must begin viewing cybersecurity as a part of doing business, in order to protect themselves and to protect national security."

6. The defendants in this action have failed to heed this warning.

7. Through GTRC, over the years, Georgia Tech has entered into numerous contracts with DoD, a significant portion of which are subject to federal cybersecurity requirements.

8. According to a former Georgia Tech employee who was tasked with ensuring Defendants' compliance with federal cybersecurity regulations, there was, for years, "no enforcement" of cybersecurity regulations at Georgia Tech.

This was because, as another former Georgia Tech employee explained, with the tacit and, in some cases, explicit approval of senior leadership, Georgia Tech routinely bent on compliance with federal cybersecurity regulations and was undeterred by the risk of submitting "false claims" to the federal government.

9. This, according to yet another former Georgia Tech employee, was to accommodate "researchers [who were] pushing back" on cybersecurity compliance because they found it burdensome. According to these former employees, senior leadership at Georgia Tech gave in to the demands of these researchers to avoid compliance with cybersecurity regulations because "of the money [the researchers] bring in" from government contracts.

10. As one former employee described it, Georgia Tech had a cybersecurity compliance "culture of somebody up the line is going to overturn me . . . [so] I might as well go ahead and ignore the policy." Another former employee described Georgia Tech's "attitude" to its "obligations to meet cybersecurity requirements" as "oh, I don't want to bother with that."

11. Put simply, according to these former employees, the researchers who brought in significant government contracting money were considered the equivalent of "star quarterbacks" and thus could use their "power on campus" to push back against compliance with federal cybersecurity rules.

12. One such researcher is Emmanouil (Manos) Antonakakis, who runs the Astrolavos Lab at Georgia Tech and whose research focuses on cybersecurity. Notwithstanding the application of federal cybersecurity requirements to the Astrolavos Lab pursuant to a number of DoD contracts for which Dr. Antonakakis and his lab performed work, in the face of resistance from Dr. Antonakakis, Georgia Tech failed to enforce basic cybersecurity at the Astrolavos Lab.

13. Most notably, during the relevant time period, while the lab possessed nonpublic and sensitive DoD information, including information that was "For Official Use Only" (FOUO) or "Controlled Unclassified Information" (CUI), the Astrolavos Lab failed to: (1) develop or implement a system security plan outlining how it would protect from unauthorized disclosure covered defense information in its possession; and (2) install, update, and run antivirus software on servers, desktops, and laptops in the lab which had access to nonpublic DoD information.

14. Additionally, in violation of the conditions of its contracts, and thus conditions of their government funding, Georgia Tech and GTRC failed to: (1) assess the system on which the Astrolavos Lab processed, stored, or transmitted sensitive DoD data using DoD's prescribed assessment methodology; and (2) provide to DoD an accurate summary level score for the Astrolavos Lab to

demonstrate the state of the lab's compliance with applicable cybersecurity regulations. This is because no such score existed for the lab.

15. Instead of calculating and providing to DoD an accurate score for the Astrolavos Lab, Georgia Tech and GTRC provided DoD with a score for a "campus-wide" IT system at Georgia Tech when no such campus-wide IT system existed.

16. According to former Georgia Tech employees, the score reported to DoD was for a "fictitious" or "virtual" environment that was a "construct" because it was not "specifically associated to any active research at Georgia Tech." In fact, according to these employees, the score was "not actually describing something that exists." Most importantly for purposes of this action, the score was not for the Astrolavos Lab, which had no score to report because it never calculated one.

17. Georgia Tech and GTRC knew that the "campus-wide" score that they reported to DoD was false, and they were warned by a member of their own senior leadership team—a now former general manager of GTRC, who also previously served as the executive director of the office at Georgia Tech that oversaw government contracting at Georgia Tech—that providing the campus-wide score to DoD would be "misleading" or an outright "misrepresentation" because the "government would just look [at the score] and think, oh, that's their overall score"—which it was not.

18. Despite these warnings, Georgia Tech and GTRC submitted the false score to DoD because, according to that former senior employee, "[t]hey wanted the money" from DoD contracts, and, according to DoD regulations, posting the score was a "condition of contract award."

19. As detailed below, Defendants intentionally, knowingly, and negligently induced DoD to enter into and retain contracts with them for which they were not eligible under the false pretense that Defendants (i) would comply with applicable cybersecurity regulations, and (ii) had provided an accurate score for Georgia Tech's entire campus, which applied to every research lab at Georgia Tech with a relevant DoD contract, including the Astrolavos Lab. As alleged herein, Defendants' conduct gives rise to claims under the federal common law, including for fraud and negligent misrepresentation, and the FCA.

20. As one former Georgia Tech employee explained, "based on the overall culture at Georgia Tech," 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."

21. The United States brings this complaint-in-intervention against Defendants to recover the damages that the United States has suffered, the ill-gotten gains to Defendants, and applicable penalties because of Defendants'

systematic noncompliance with federal cybersecurity regulations and false statements to DoD.

THE PARTIES

22. The United States brings this action on behalf of DoD, including the U.S. Air Force (Air Force) and the Defense Advanced Research Projects Agency (DARPA).

23. Relator Christopher Craig is a member of Georgia Tech's Cybersecurity Team with the title of Enterprise Security Architect. Craig has worked at Georgia Tech since 2003 in a variety of technical and cybersecurity roles. From 2017 until June 2022, Craig served as the Associate Director of Cybersecurity at Georgia Tech. In this role, Craig managed all cybersecurity personnel at Georgia Tech.

24. Relator Kyle Koza is a Georgia Tech graduate and former employee at Georgia Tech. From 2011 until 2022, Koza worked on Georgia Tech's Cybersecurity Team, most recently as Principal Information Security Engineer from 2017 until June 2022.

25. Georgia Tech is a research university and institute of technology based in Atlanta, Georgia. Georgia Tech is part of the University System of Georgia (USG), which is governed by the Board of Regents of the University System of Georgia (Board of Regents). The Board of Regents is named as a defendant in this

action as the governing body of Georgia Tech, whose conduct is at issue in this matter.

26. GTRC is a Georgia non-profit corporation organized under the laws of the state of Georgia. GTRC is based in Atlanta, Georgia. GTRC is governed by its own Board of Trustees, the members of which are named or elected pursuant to GTRC's bylaws and articles of incorporation.

27. According to its website, GTRC is "the contracting entity for all sponsored activities for colleges and other units at Georgia Tech," with the exception of the Georgia Tech Research Institute (GTRI).

28. The relationship between GTRC and Georgia Tech is defined, in part, by a Memorandum of Understanding executed by those parties on April 1, 1953. According to GTRC's website, pursuant to that agreement: "GTRC contracts and is paid for the research done at Georgia Tech, paying Georgia Tech for all direct costs and 78.3 percent of the overhead. The 21.7 percent of the overhead retained by GTRC are used to establish reserves for the research program and to pay certain expenses that Georgia Tech cannot pay."

29. Accordingly, as a general matter, Georgia Tech itself does not directly enter into contracts for research to be performed at Georgia Tech; instead, this is done through GTRC, who then, pursuant to the Memorandum of Understanding, subcontracts to Georgia Tech for the work to be performed pursuant to the

relevant contract. Then Georgia Tech and GTRC split the proceeds from the contract.

30. According to its website, Georgia Tech is a "University System of Georgia-approved cooperative organization." Pursuant to Section 6.17.2 of the University System of Georgia Policy Manual, an entity may be a "cooperative organization" to a USG institution like Georgia Tech "only if . . . the organization is acting as a legal entity separate from the USG institution." GTRC thus is a legal entity separate from the USG and Georgia Tech, and, by definition, not a Georgia state entity.

31. As the GTRC website makes clear, GTRC is an "individually functioning entit[y] that operates separately" from Georgia Tech.

32. According to financial data published on its website, between fiscal years 2019 and 2022, GTRC entered into more than $1.6 billion in government contracts, primarily with the federal government and specifically DoD. In 2022 alone, GTRC entered into more than $423 million in government contracts, primarily with the federal government and specifically DoD.

33. According to its publicly available financial statements, GTRC retains hundreds of millions of dollars in cash and other assets, which reflect the proceeds from its contracting primarily with the federal government, and especially DoD.

OTHER RELEVANT ACTORS

34. Amongst the trustees for GTRC is Georgia Tech's Vice President for Research, Chaouki T. Abdallah, Ph.D., who also serves as the president of GTRC. According to his profile on Georgia Tech's website, as Vice President of Research at Georgia Tech, Dr. Abdallah serves as the "chief research officer" for Georgia Tech and oversees the "$1.45 billion annual research enterprise that includes [GTRI], 10 interdisciplinary research institutes (IRIs), as well as economic development, and related support units within Georgia Tech."

35. In this position, Dr. Abdallah also oversees the Office of Sponsored Programs (OSP) at Georgia Tech, which, along with GTRC, oversees government contracting at Georgia Tech.

36. Robert Butera is the Chief Research Operations Officer at Georgia Tech. He works under Dr. Abdallah in the Office of the Executive Vice President for Research.

37. Until her retirement in 2022, Rebecca Caravati served as the general manager of GTRC, and as the interim executive director of OSP. Caravati oversaw government contracting at Georgia Tech and GTRC, including with respect to those entities' compliance obligations under federal rules and regulations governing cybersecurity.

38. Leo Howell is currently the Interim Vice President for Information Technology at Georgia Tech. From September 2021 until June 2023, Howell served as the Chief Information Security Officer (CISO) at Georgia Tech. In that role, Howell was responsible for cybersecurity at Georgia Tech. Howell oversaw Georgia Tech's Cybersecurity Team, including Georgia Tech's Governance, Risk, and Compliance (GRC) Team.

39. From 2017 until February 2021, Anant (Jimmy) Lummis was the CISO at Georgia Tech. Prior to that, Lummis was the Deputy CISO at Georgia Tech. Like Howell, Lummis oversaw Georgia Tech's Cybersecurity Team, including its GRC Team. Lummis is currently a lecturer at Georgia Tech.

40. Blake Penn created, and from 2016 until 2021, led the GRC Team at Georgia Tech. According to Penn, the "primary role" of the GRC Team is to ensure "compliance with government and industry regulations that were cybersecurity-related regulations." Penn reported directly to Lummis.

41. Kyle Smith was a member of the GRC Team from 2016 until 2020, and worked under Penn and Lummis.

42. Emmanouil (Manos) Antonakakis, Ph.D. is an Associate Professor in the School of Electrical and Computer Engineering (ECE) and an adjunct faculty member in the College of Computing (CoC) at Georgia Tech.

43. Dr. Antonakakis is the co-director of the Center for Cyber Operations Enquiry and Unconventional Sensing (COEUS) at Georgia Tech. Dr. Antonakakis is also the sole director of the Astrolavos Lab at Georgia Tech, which is now under the umbrella of COEUS. The research of the Astrolavos Lab is focused on cybersecurity, including cyberattack attribution.

44. In connection with the Astrolavos Lab, Dr. Antonakakis, through GTRC, was the principal investigator on contracts with DoD, specifically with the Air Force and DARPA, that imposed cybersecurity requirements on Defendants, and specifically the Astrolavos Lab, in connection with Dr. Antonakakis's research for DoD.

45. Since 2016, William Garrison has been the head of IT at the Astrolavos Lab. Garrison oversees the computers, servers, and networks at the lab.

JURISDICTION & VENUE

46. This court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. §§ 1331 and 1345 because this action is brought by the United States as a plaintiff pursuant to the FCA and under federal common law.

47. Venue is proper in this jurisdiction under 31 U.S.C. § 3732(a) and 28 U.S.C. §§ 1391(b) and 1395(a). Defendants can be found in and/or have transacted business in this district. Additionally, a substantial portion of the events that give rise to the claims alleged herein occurred in this jurisdiction.

LEGAL FRAMEWORK

A. The False Claims Act

48. Under the FCA, any "person" who:

> (A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval; [or]
>
> (B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim . . .
>
> is liable to the United States Government [for statutory damages and penalties].

31 U.S.C. §§ 3729(a)(1)(A)-(B).

49. "Claim" is defined in the FCA as:

> any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property, that— (i) is presented to an officer, employee, or agent of the United States; or (ii) is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest, and if the United States Government— (I) provides or has provided any portion of the money or property requested or demanded; or (II) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded. . . .

31 U.S.C. § 3729(b)(2).

50. The FCA provides that "material" means "having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property." 31 U.S.C. § 3729(b)(4).

51. The FCA further provides that "knowing" and "knowingly":

(A) means that a person, with respect to information

i. has actual knowledge of the information;

ii. acts in deliberate ignorance of the truth or falsity of the information; or

iii. acts in reckless disregard of the truth or falsity of the information; and

(B) requires no proof of specific intent to defraud.

31 U.S.C. § 3729(b)(1).

52. Under the FCA, any person who is found to have violated the FCA "is liable to the United States Government for a civil penalty of not less than $5,000 and not more than $10,000, as adjusted by the Federal Civil Penalties Inflation Adjustment Act of 1990 . . . plus 3 times the amount of damages which the Government sustains because of the act of that person." 31 U.S.C. §§ 3729(a)(1).

53. The current level of civil penalties for violations of the FCA that are assessed after February 12, 2024 is not less than $13,946 and not more than $27,894. 28 C.F.R. § 85.5. These penalties are subject to further adjustment pursuant to the Federal Civil Penalties Inflation Adjustment Act of 1990.

54. The FCA further provides that "[a] person violating this subsection shall also be liable to the United States Government for the costs of a civil action brought to recover any such penalty or damages." 31 U.S.C. § 3729(a)(3).

B. Federal Cybersecurity Regulations

(i) DoD Regulations Mandate that Contractors Provide "Adequate Security" for the Protection of Covered Defense Information on Contractor IT Systems

55. Since 2013, DoD regulations have mandated that "[c]ontractors and subcontractors" provide "adequate security" on their "covered contractor information systems" to protect CUI that belongs to the government or is in the contractors' possession, including controlled technical information (CTI), present on those systems (collectively, "Covered Defense Information"). 48 C.F.R. § 204.7302(a)(1) (effective Nov. 18, 2013) [Defense Federal Acquisition Regulation Supplement (DFARS) 7302]; 48 C.F.R. § 252.204-7012 (effective Nov. 18, 2013) (DFARS 7012). *See also* 48 C.F.R. § 252.204-7008(b) (effective Dec. 30, 2015) (DFARS 7008).

56. "'Covered contractor information system' means an unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information." DFARS 7012(a).

57. Covered Defense Information includes both CUI and CTI, which is either provided to the contractor by DoD and is marked or otherwise identified by DoD, or is "[c]ollected, developed, received, transmitted, used, or stored by" the contractor in support of the contract, whether that information is marked as CUI or CTI, or not. DFARS 7012(a).

58. "'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." DFARS 7012(a).

59. As directed by DFARS 7012(a), "Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents." DoD Instruction 5230.24 directs that technical and other information subject to Distribution Statements B through F are not designated for public release absent further approval from the proper authority in the government, and thus, by definition, are controlled technical information.

60. Under DFARS 7012(a), "'Technical information' means technical data or computer software. . . ." According to DFARS 7012(a): "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."

61. Under DFARS 7012, a contractor must provide "adequate security" under DFARS 7012 before it can process, store, or transmit Covered Defense Information on its information system.

(ii) DoD Regulations Mandate that to Provide "Adequate Security" Contractors Must Implement the 110 Controls under NIST SP 800-171 or Plans of Action to Implement Those Controls by December 31, 2017

62. Since October 2016, DoD regulations have mandated that "[t]o provide adequate security, the Contractor shall implement, ***at a minimum*** . . . the security requirements in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, 'Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations'" that is "in effect at the time the solicitation is issued. . . ." DFARS 7012(b)(2) (emphasis added).

63. For each security requirement that has not yet been implemented, contractors are required to have a plan of action for implementing the controls, along with a date by when the controls will be implemented. Contractors must also actively work to implement those plans of action in a genuine effort to implement all 110 controls.

64. DFARS 7012 further mandates that contractors "shall implement NIST SP 800-171, as soon as practical, but not later than December 31, 2017." DFARS 7012(b)(2)(ii)(A).

(iii) DoD Regulations Mandate that, as a Condition of Contract, Contractors Must Certify Compliance with DFARS 7012 and the Controls in NIST SP 800-171; Variances from These Requirements Must be Approved by the DoD-CIO and the Contracting Officer

65. At the time of contract, and as a condition of contract, pursuant to DFARS 7008(c)(1), all contractors, by submission of their offers, certify and represent that they will comply with DFARS 7012 and implement the controls outlined in NIST SP 800-171.

66. Specifically, as directed by DFARS 7008(c)(1), "[b]y submission of this offer, the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171, 'Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations' (see http://dx.doi.org/10.6028/NIST.SP.800–171) that are in effect at the time the solicitation is issued or as authorized by the contracting officer not later than December 31, 2017."

67. Moreover, pursuant to DFARS 7008(c)(2)(i), "[i]f the Offeror proposes to vary from any of the security requirements specified by NIST SP 800–171 that are in effect at the time the solicitation is issued or as authorized by the Contracting Officer, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of—(A) Why a

particular security requirement is not applicable; or (B) How an alternative but equally effective, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection."

68. DFARS 7012(b)(2)(ii)(B) similarly directs that: "The Contractor shall submit requests to vary from NIST SP 800–171 in writing to the Contracting Officer, for consideration by the DoD CIO. The Contractor need not implement any security requirement adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place."

69. Pursuant to DFARS 7008(c)(2)(ii), "[a]n authorized representative of the DoD CIO will adjudicate offeror requests to vary from NIST SP 800–171 requirements in writing prior to contract award. Any accepted variance from NIST SP 800–171 shall be incorporated into the resulting contract."

70. Absent approval by the DoD CIO of a variance from one of the NIST SP 800-171 controls pursuant to a written request, the contractor is required to implement the NIST SP 800-171 controls and certify or represent as part of the contracting process that it has or will implement controls by December 31, 2017.

71. As explained in the Final Rule implementing DFARS 7008, "DFARS provision 252.204-7008 serves as a notice to offerors. The provision puts the offeror on notice that, when performance of the contract requires covered defense

information on a covered contractor information system, the security requirements in NIST SP 800-171 apply and ***must be implemented*** no later than December 31, 2017." 81 Fed. Reg. 72986, 72990 (Oct. 21, 2016) (emphasis added).

(iv) DoD Regulations Mandate that, as a Condition of Contract Award, Prior to Entering into a Contract with a DoD Entity, Contractors Must Submit an Accurate Summary Level Score for Each and Every Covered Contractor System Relevant to the DoD Contract

72. As a condition of contract, under multiple DoD regulations, since December 2020, contractors are required at the time of contract award to have on file with DoD, in its Supplier Performance Risk System (SPRS), a summary level score that is not more than three years old, which provides DoD with a report of the status of the contractors' compliance with the 110 controls of NIST SP 800-171, for "each covered contractor information system that is relevant to the offer, contract, task order, or delivery order." DFARS 7032(a)(2); 48 C.F.R. §252.204-7019(b).

73. Thus, for contracts where the offeror is required to implement NIST SP 800-171, the contracting officer is not permitted to award the contract to a bidder who has not provided DoD with a summary level score for "each covered contractor information system that is relevant to the offer [or] contract." DFARS 7019.

74. Significantly, as DoD has made clear, "[g]iven the size and scale of the DIB sector, the Department cannot scale its organic cybersecurity assessment capability to conduct on-site assessments of approximately 220,000 DoD contractors every three years." 85 Fed. Reg. 61505, 61509 (Sept. 29, 2020). Thus, it is critical that contractors both (i) comply with federal cybersecurity regulations, and (ii) accurately report the state of their compliance to DoD pursuant to DFARS 7019.

75. Most contractors' summary level scores stem from self-assessment of their implementation of the NIST SP 800-171 requirements on each of the relevant covered contractor systems.

76. For a Basic Assessment, the contractor calculates a summary level score pursuant to an Assessment Methodology developed by DoD. *See* NIST (SP) 800-171 Assessment Methodology version 1.2.1 (Jun. 24, 2020) (DoD Assessment Methodology); DFARS 7302(a)(3). That methodology assigns a point value to each security requirement which is weighted to account for the potential harm that could result from it not being implemented. The score is calculated by deducting from 110 (a perfect score reflecting implementation of all of the security requirements) the value assigned to each unimplemented security requirement.

(v) DoD Contractors Are Required to Create and Implement a System Security Plan and Failure to Do So Constitutes Indisputable Noncompliance with DFARS 7012

77. Since at least December 2016, NIST SP 800-171 Control (NIST Control) 3.12.4 has directed that a contractor: "Develop, document, and periodically update system security plans that describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."

78. Without a system security plan, a contractor cannot calculate a score to be reported in SPRS.

79. Thus, according to the DoD Assessment Methodology, "***[t]he absence of a system security plan would result in a finding*** that 'an assessment could not be completed due to incomplete information and ***noncompliance with DFARS clause 252.204-7012***." (emphasis added)

80. The requirement of a system security plan is so basic that pre-December 2016 versions of NIST SP 800-171 identified a system security plan as something that the federal government: "EXPECTED TO BE ROUTINELY SATISFIED BY NONFEDERAL ORGANIZATIONS WITHOUT SPECIFICATION."

81. Since at least June 2015, NIST Controls 3.12.1 and 3.12.3 respectively have directed contractors to (1) periodically assess their information security

controls to determine if they are effective and (2) monitor the security controls to ensure their continued effectiveness.

82. Reflecting their significance, the Scoring Template that is attached as Annex A to the DoD Assessment Methodology provides NIST Controls 3.12.1 and 3.12.3 with point values of 5, reflecting that "if not implemented, [the absence of each control] ***could lead to significant exploitation of the network, or exfiltration of DoD CUI***." (emphasis added)

83. The Scoring Template provides NIST Control 3.12.2 (put in place plans of action to comply with security controls) with a point value of 3, reflecting that "if not implemented, [the absence of the control would] have a specific and confined effect on the security of the network and its data."

84. With respect to NIST Control 3.12.4, which directs the development and implementation of a system security plan, the Scoring Template provides no point value. This is because "[t]he absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.'"

(vi) Federal Contractors are Required to Install, Run, and Update Antivirus and Incident Detection Software

85. NIST Control Family 3.14 is primarily focused on preventing the infiltration of malicious code in covered contractor systems. NIST SP 800-171 defines malicious code as: "Software or firmware intended to perform an

unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of a system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code."

86. The primary controls in this family are NIST Controls 3.14.2, 3.14.4, and 3.14.5, which collectively require contractors to install, update, and run antivirus and incident detection software. Specifically, NIST Controls 3.14.2, 3.14.4, and 3.14.5 direct contractors to (1) "Provide protection from malicious code at designated locations within organizational systems"; (2) "Update malicious code protection mechanisms when new releases are available"; and (3) "Perform periodic scans of organizational systems and real-time scans of files from external sources as files are downloaded, opened, or executed."

87. Each of the NIST Controls contains a "discussion" providing further explanation of the control. The discussions to NIST Controls 3.14.2, 3.14.4, and 3.14.5 specifically refer to antivirus software, with the discussion for the first two controls explaining that "[m]alicious code protection mechanisms include ***anti-virus*** signature definitions and reputation-based technologies," and the discussion for 3.14.5 stating that "[p]eriodic scans of organizational systems and real-time scans of files from external sources can detect malicious code." (emphasis added)

88. The discussion to NIST Control 3.14.2 refers to NIST Special Publication 800-83, *Guide to Malware Incident Prevention and Handling for Desktops and Laptops* (July 2013), indicating that the publication "provides guidance on malware incident prevention." NIST SP 800-83 directs that "***organizations should deploy antivirus software*** on all hosts for which satisfactory antivirus software is available." NIST SP 800-83 at viii (emphasis added).

89. NIST Control 3.14.1 requires that contractors: "Identify, report, and correct system flaws in a timely manner." The discussion to NIST Control 3.14.1 explains that the control requires contractors to "identify systems that are affected by announced software and firmware flaws including potential vulnerabilities resulting from those flaws" and then run "[s]ecurity-relevant updates includ[ing] . . . ***anti-virus signatures***." (emphasis added)

90. The Scoring Template attached to DoD's Assessment Methodology provides NIST Controls 3.14.1, 3.14.2, and 3.14.4 with point values of 5, reflecting that "if not implemented, [the absence of any one of these controls] could lead to significant exploitation of the network, or exfiltration of DoD CUI." NIST Control 3.14.5 is given a point value of 3 because failure to implement it would "have a specific and confined effect on the security of the network."

91. Additionally, the Scoring Template notes that NIST Controls 3.14.1, 3.14.2, 3.14.4, and 3.14.5 are: "Basic safeguarding requirements and procedures to

protect covered contractor information systems per Federal Acquisition Regulation (FAR) clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems."

92. FAR 52.204-21 imposes certain "basic safeguarding requirements and procedures to protect covered contractor information systems," which are defined to include any contractor information systems that process, store, or transmit federal contract information, which is "information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments." 48 C.F.R. § 52.204–21.

93. FAR 52.204-21 broadly applies to all government contractors, not just DoD contractors. Moreover, unlike DFARS 7012, FAR 52.204-21 does not require the presence of Covered Defense Information, just government information that is not intended for public release.

94. As the final rule enacting this provision explained, "[t]he intent is that the scope and applicability of this rule be very broad, because this rule requires only the most basic level of safeguarding." 81 Fed. Reg. 30439, 30441 (May 15, 2016). As the final rule further explained, "[a] prudent business person would

employ this most basic level of safeguarding, even if not covered by this rule. This rule is intended to provide a basic set of protections for all Federal contract information . . . ." 81 Fed. Reg. at 30441.

95. Amongst the "basic safeguards" required by FAR 52.204-21 are the following antivirus requirements that match up precisely to NIST Controls 3.14.1, 3.14.2, 3.14.4, and 3.14.5:

> (xii) Identify, report, and correct information and information system flaws in a timely manner.
>
> (xiii) Provide protection from malicious code at appropriate locations within organizational information systems.
>
> (xiv) Update malicious code protection mechanisms when new releases are available.
>
> (xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

96. Both the proposed and final rules that enacted FAR 52.204-21 made clear that the provision requires contractors to install, run, and update antivirus software throughout covered contractor IT systems.

FACTUAL ALLEGATIONS

I. Background – Defendants' DoD Contracts and False Claims to DoD

97. Through GTRC, Georgia Tech has entered into billions of dollars in federal government contracts over the years, primarily with DoD.

98. GTRC enters into government contracts with DoD as the prime contractor, and then subcontracts the work to be performed at the Resident

Instruction (RI) side of Georgia Tech (which includes the academic part of Georgia Tech). The monies paid by the government pursuant to those contracts are split between Georgia Tech and GTRC, with GTRC retaining a significant portion of the monies that it receives from the government on its balance sheets from year to year.

99. Where the work pursuant to a government contract is to be performed at RI, it is typically performed by teams at specific research labs at Georgia Tech which are led by Georgia Tech faculty members who act as the "principal investigators" for the relevant contracts. A principal investigator is a key person under a government contract who is responsible for overseeing the work on the contract and delivering the final product to the government.

100. One such research lab is the Astrolavos Lab, which is led by Dr. Manos Antonakakis. Since 2016, the Astrolavos Lab has entered into a series of DoD contracts, principally with the Air Force and DARPA.

101. As detailed below, the key DFARS cybersecurity clauses, DFARS 7302, 7008, 7012, 7019, 7020, as well as FAR 52.204-21, applied to at least two of the DoD contracts for which the Astrolavos Lab performed work and Dr. Antonakakis served as the principal investigator.

A. Air Force Contract FA8750-17-C-0016 (EA)

102. The first contract for which Dr. Antonakakis acted as principal investigator for work performed at the Astrolavos Lab is the "Rhamnousia: Attributing Cyber Actors Through Tensor Decomposition" contract between GTRC and the Air Force, executed on November 17, 2016. The Astrolavos Lab performed work on this contract from December 2016 until the end of 2021.

103. The contract, which is referred to as "EA" or the "EA Contract," is identified by contract number FA8750-17-C-0016. At Georgia Tech, the internal contract numbers for EA were AWD-101187/GT10002480. The EA Contract was a joint effort between the Air Force and DARPA.

104. According to the solicitation for the EA Contract, the goal of the EA project was to develop enhanced attribution technology to permit the Air Force to identify parties behind cyberattacks.

105. The solicitation made clear that the program would have classified and non-classified elements and that DFARS 7012 applied.

106. Specifically, the EA solicitation included the following language specifying that DFARS 7012 would apply to the EA Contract: "Per DFARS 204.7304, DFARS 252.204-7012, 'Safeguarding of Covered Defense Information and Cyber Incident Reporting;' applies to this solicitation and all FAR-based awards resulting from this solicitation."

107. The EA solicitation also warned that contractors would need to protect "DARPA CUI," including by refraining from processing DARPA CUI on "publicly available computers" or posting "DARPA CUI to publicly available webpages or website," and to "ensure that DARPA CUI on mobile computing devices is identified and encrypted and all communications on mobile devices or through wireless connections are protected and encrypted."

108. Consistent with this, the EA Contract itself incorporated FAR 52.204-21 by reference, and included the full text of DFARS 7012.

109. By the explicit terms of the EA Contract, the EA program involved "military applications" and export controls. In the section marked "Export Controls," the EA Contract specifically stated that: "The items to be delivered under this contract are being developed for both civil and military applications."

110. This is consistent with the EA solicitation which warned that "all contracts, other transactions and other awards . . . resultant from this solicitation will include the DFARS Export Control clause."

111. The October 31, 2016 award letter included the full text of DFARS 7008, which mandates that "[b]y submission of this offer, the Offeror represents that it will implement the security requirements specified by [NIST SP 800-171] . . . not later than December 31, 2017."

112. In reference to the text of DFARS 7008, the award letter indicated that "[a] reply to this provision is only required if additional time is needed to implement the derived security requirement identified in para (c) below [referring to NIST SP 800-171], or if a deviation from security requirements in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 is proposed." The Air Force relied on GTRC's representation pursuant to DFARS 7008 in entering in the EA Contract with GTRC.

113. The Contract Data Requirements List attached to the EA Contract indicated that Distribution Statement F applied, stating: "DISTRIBUTION STATEMENT F: FURTHER DISSEMINATION ONLY AS DIRECTED BY AFRL/RIGB, ROME, NY 13441." This indicated that the contract would involve CTI, and thus Covered Defense Information. *See* DFARS 7012(a).

114. Attached to the EA Contract was a completed version of Department of Defense Form 254, known as a DD254, which provides information regarding "Contract Security Classification[s]."

115. The DD254 for the EA Contract indicated that the "contractor" would receive both "classified and unclassified information," up to the level of "Top Secret." This included information that was "for official use only," which is a legacy term for a type of controlled unclassified information that has now largely been replaced by the CUI designation.

116. The DD254 also included the following restriction on the public release of information related to the EA Contract: "No information, except as provided in applicable U.S. Statutes, which is classified or unclassified shall be released for public dissemination without prior written approval of DARPA."

117. The EA Contract also had a Security Classification Guide (CG), which itself was marked Distribution Statement D. The CG reiterated the publication restrictions in the EA Contract applicable to unclassified information, warning that: "The fact that this CG shows certain details of unclassified information does not authorize automatic public release. Proposed public disclosures of unclassified information regarding all DARPA efforts shall be processed in accordance with (IAW) the current DD Form 254."

118. The CG then went on to describe a number of categories of technical documents as FOUO or, in certain circumstances, classified. The FOUO designation applied, at minimum, to information about the "association of contractors and/or subcontractors" to the "contracting agent" or "DARPA." It also applied to "technical details of specific, persistent vulnerabilities of system under development."

119. Among categories marked as potentially classified were "association of contractors and/or subcontractors" with other government agencies, and "actual, simulated, or synthesized data used for testing EA capabilities."

According to the CG, this technical information, whether classified or unclassified, involved "scientific, technological, or economic matters relating to national security."

120. Given the publication restrictions, the application of Distribution Statement F, as well as the presence of information that was marked FOUO or CUI, the EA Contract necessarily involved Covered Defense Information, including both CUI and CT, as warned in the EA solicitation. Thus, the Astrolavos Lab was required to comply with the cybersecurity requirements from the FAR and DFARS, including DFARS 7012 and FAR 52.204-21, before it could process, store, or transmit that Covered Defense Information and Federal Contract Information on its information systems.

121. Defendants processed, stored or transmitted Covered Defense Information during their performance of work on the EA contract, and this work included multiple documents marked as FOUO or CUI. This fact is confirmed by Defendants' admissions, which are detailed below.

B. *DARPA Contract #HR001123C0035* (Smoke)

122. Dr. Antonakakis served as the principal investigator for work performed at the Astrolavos Lab with respect to a second contract with DARPA titled "Antikythera: A Novel Framework to Assess, Statistically Model and Evade CYB" with contract number HR001123C0035. The contract is referred to as

"Smoke" or the "Smoke Contract." The lab began work on this contract in October 2022, which is ongoing as of now.

123. According to the solicitation, the purpose of the Smoke program is to "develop tools to automate the planning and deployment of threat emulated, attribution-aware cyber infrastructure."

124. The Smoke solicitation incorporated DFARS 7012 and 7008. It also noted that "all proposers are required to submit for all award instrument types supplementary DARPA-specific representations and certifications at the time of proposal submission." The DARPA-specific representations and certifications include representations and certifications in connection with DFARS 7019.

125. Accordingly, on July 20, 2022, in connection with GTRC's bid for the Smoke Contract, GTRC executed DARPA's standard form "Representations, Certifications and Other Statements of Offerors," which included a certification and representation by GTRC of compliance with DFARS 7019, the full text of which was written out in the document. The certification was signed by "Ashley Smith, Assistant to Vice President, Georgia Tech Research Corporation" who was identified as the person "signifying accuracy and completeness of the above representations and Certifications."

126. DARPA relied on these representations and certifications, as well as the fact that GTRC had posted a summary level score for the Georgia Tech campus, in entering into the Smoke Contract and its associated modifications with GTRC.

127. GTRC and DARPA first entered into the Smoke Contract on October 5, 2022. The original Smoke Contract called for the Astrolavos Lab to only perform fundamental research, which would not be subject to any publication restrictions. However, even before execution of the contract, the Astrolavos Lab asked to have access to certain Covered Defense Information, so the parties immediately amended the Smoke Contract on November 7, 2022.

128. The modified Smoke Contract, which became effective on November 7, 2022, amended the statement of work for the contract to "add[] Non-Fundamental Research Tasks" along with "Non-Fundamental Research DFARS and FAR clauses." The DFARS clauses that were explicitly added to the contract included DFARS 7012 (adequate security) and DFARS 7020 (summary level score).

129. The original Smoke Contract incorporated FAR 52.204-21 (as well as DFARS 7012 and 7020). Moreover, pursuant to DFARS 7008, GTRC and Georgia Tech made the following certification to DARPA at the time of bidding: "[b]y submission of this offer, the Offeror represents that it will implement the security requirements specified by [NIST SP 800-171] . . . not later than December 31, 2017."

130. Additionally, on September 27, 2022—just over a week before the parties executed the original Smoke Contract on October 5, 2022—DARPA executed the original DD254 for the Smoke Contract. The DD254 for the Smoke Contract indicated that "The CONTRACTOR WILL . . . RECEIVE, STORE, OR GENERATE CONTROLLED UNCLASSIFIED INFORMATION (CUI)" and "The Performer will protect CUI."

131. DARPA executed a revised DD254 for the Smoke Contract on August 23, 2023. The provisions cited above did not change in the revised document. The Smoke Contract was modified by the parties on September 23, 2023 to incorporate the revised DD254.

132. With respect to public release of information related to the Smoke Contract, the DD254 stated that: "The contractor will not release any information (Classified or Unclassified) without prior written approval of the public release authority, except as provided in applicable U.S. Statutes."

133. Given this publication restriction, and the clear statement in both the DD254 and the contract modification that the contractor would receive or develop CUI in connection with the contract, the Smoke Contract necessarily involved Federal Contract Information and Covered Defense Information. Defendants processed, stored, or transmitted Covered Defense Information during their performance of work on the Smoke Contract and this work included multiple

documents marked CUI. Thus, the cybersecurity requirements from the FAR and DFARS, including DFARS 7008 and 7012, as well as FAR 52.204-21, applied to the Smoke Contract.

134. GTRC and Georgia Tech did not tell DARPA of their intention not to comply with federal cybersecurity rules and regulations as required by the contract, DFARS 7302, 7008, 7012, 7019, 7020, and FAR 52.204-21, amongst other provisions.

II. Georgia Tech's Own Documents and Testimony Confirm the Astrolavos Lab Possessed Covered Defense Information for Work on its DoD Contracts.

135. As demonstrated by Georgia Tech's own documents and testimony, the Astrolavos Lab possessed Covered Defense Information in connection with the EA Contract and the Smoke Contract (collectively, the "Astrolavos Lab Contracts").

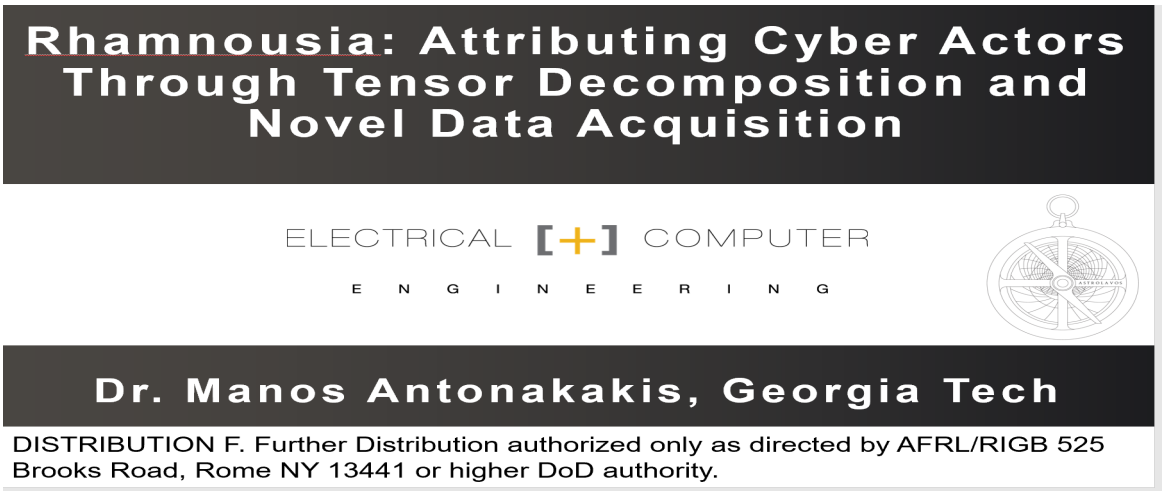
136. As a threshold matter, Dr. Antonakakis admitted in sworn testimony that all the work that he and his colleagues performed for the Astrolavos Lab Contracts occurred in the Astrolavos Lab and on their computer systems. Dr. Antonakakis also admitted in writing and during sworn testimony to handling documents in his lab that were subject to Distribution Statement F, which denotes the presence of CTI, which is Covered Defense Information.

137. For example, in a November 22, 2019 email, Dr. Antonakakis wrote that "my slides for EA are at the UNCLASSIFIED//DISTRIBUTION F level." He explained that this meant that others "*should not* have access to the[m] without explicit permission from DARPA and/or AFRL." Dr. Antonakakis further explained: "To give you an idea, I do not even email the slides to anyone."

138. To eliminate any confusion on the point, in a separate email from November 22, 2019, Dr. Antonakakis wrote: "Let me [be] crystal clear. I cannot give access to the slide decks to anyone but the PM team at DARPA or the AFRL contracting officer."

139. Consistent with this, during sworn testimony, Dr. Antonakakis testified that "[s]ometimes DARPA would effectively ask [him] in some of [his] presentations to mark them as Distribution Statement F." William Garrison, the head of IT at the Astrolavos Lab testified similarly, explaining: "presentations that [Dr. Antonakakis] had given on his laptop would be considered CUI."

140. Dr. Antonakakis in fact created presentations that he provided to DARPA that were marked Distribution Statement F and included Covered Defense Information. For example, a May 28, 2019 presentation to DARPA from Dr. Antonakakis was marked with Distribution Statement F. Below is the cover page to that presentation, which itself does not contain Covered Defense Information (although the rest of the presentation does).



141. Dr. Antonakakis's final report to DoD pursuant to the EA Contract included Covered Defense Information. Once it was in the possession of the Air Force, DoD marked the report as "CUI" on the basis that the information in the report was "Critical Technology" that was "Export Controlled." DoD further applied Distribution Statement D, restricting distribution of the report to the "Department of Defense and U.S. DoD Contractors only." DoD stores the presentation on a system designed to protect Covered Defense Information.

142. Attached to the report is a "Form 298" which is a "Report Documentation" cover page that was filled out by Dr. Antonakakis. Form 298 has a section titled "Distribution/Availability Statement." In that section, Dr. Antonakakis indicated with respect to his report that "Distribution Authorized to Department of Defense and U.S. DoD contractors only" and that the report described "Critical Technology" including "Software Documentation" that is subject to "Export Control."

143. Other Georgia Tech documents further confirm the presence of Covered Defense Information throughout the lab. In late 2021, Garrison was tasked by Dr. Antonakakis to "mak[e] sure that CUI data related to EA is removed from our servers." This is around the time that the EA Contract was ending. Garrison exchanged a number of instant messages with his colleagues regarding the abundance of CUI present at the lab.

144. In one instant message, one of the student researchers at the lab explained to Garrison that deleting all the CUI was "not an easy task" because "I have a shit ton" of EA CUI on various servers.

145. Garrison's communications indicate that a number of people at the lab in addition to Dr. Antonakakis worked with EA CUI. In one instant message, one of Garrison's colleagues referred to the need to give Dr. Antonakakis a "heads up" before they deleted CUI on a particular "box" because "it was mainly a Manos box and had a lot of EA cui."

146. The instant messages further indicate that Garrison indeed deleted EA CUI from a number of workstations and servers, directing researchers in the lab to "mark their non cui directories" so those directories would not inadvertently be deleted in the process.

147. In fact, in a January 14, 2022 instant message, Garrison identified eight different "hosts we need approval to wipe/sanitize, based on the notes I have of which boxes have EA CUI data on them."

148. In a separate instant message with Michael Mitchell from March 11, 2022, Garrison asked Mitchell: "Do you happen to know if SMOKE involves CUI at all?" Mitchell responds: "I believe that everything from this point forward will include CUI." In response, Garrison wrote: "Gotcha. The plan is to segment things that require CUI compliance . . . ." In an April 5, 2022 instant message, Garrison again told Mitchell he knew that the Smoke Contract "would require CUI compliance."

149. Additionally, in a series of instant messages from September 26, 2022—a little over a week before the Smoke Contract was executed, and the day before the original DD254 for that project was executed—Garrison and a student researcher discussed the need to create CUI only servers for the Smoke project.

150. Dr. Antonakakis created a presentation to DARPA in connection with the Smoke kickoff meeting. At least four pages of Dr. Antonakakis's presentation contain the following marking indicating that, according to Dr. Antonakakis, the slide contained CUI:

CUI

III. Defendants Knowingly Violated Federal Cybersecurity Requirements and Fraudulently and Negligently Induced DoD to Enter into and Retain Defense Contracts with Them.

151. In connection at least with the Astrolavos Lab Contracts, beginning at least as early as May 2019 with respect to the EA Contract and November 2022 with respect to the Smoke Contract, Defendants violated applicable federal cybersecurity rules and regulations.

152. Specifically, in violation of DFARS 7012, 7008, 7302, with respect to the Astrolavos Lab, GTRC recklessly failed for multiple years to provide "adequate security" for covered contracting systems relevant to the Astrolavos Lab Contracts by, at the minimum, knowingly failing to (1) develop, document, implement, and periodically update system security plans and associated NIST SP 800-171 security controls for the covered contracting systems at the Astrolavos Lab, and (2) install, update, and run antivirus and incident detection software throughout the covered contracting systems at the Astrolavos Lab.

153. Additionally, in violation of DFARS 7019 and DFARS 7020, with respect to the Astrolavos Lab, GTRC failed to submit a summary level score for any covered contractor system "relevant" to the Astrolavos Lab Contracts. Rather, Georgia Tech and GTRC intentionally, knowingly, and negligently submitted an "enterprise" summary level score for the Georgia Tech campus that was (i) not applicable to the Astrolavos Lab, and, in any event, was for a (ii) "fictitious" or

"virtual" environment that did not "exist," which was a "construct" and not "specifically associated to any active research at Georgia Tech."

154. Thus, pursuant to DFARS 7019 and DFARS 7302, as of December 2020, the Astrolavos Lab was not eligible for any DoD contracts and thus not lawfully eligible to be paid pursuant to any such contracts. Moreover, GTRC's certifications and representations of compliance with DFARS 7019 in connection with DoD contracts, including the Smoke Contract, were false.

A. For Years, the Astrolavos Lab Had No System Security Plan.

155. By their own admission, Georgia Tech and GTRC did not implement a system security plan at the Astrolavos Lab until February 2020. This is more than three years after the lab began work on the EA Contract in late 2016, and more than two years after the December 31, 2017 deadline for Defendants to implement NIST SP 800-171 on all systems they were using to process, store, or transmit Covered Defense Information.

156. At no point did Defendants inform DoD that the Astrolavos Lab did not have a system security plan.

157. According to Kyle Smith, the member of the GRC Team who drafted the lab's February 2020 system security plan (the "Astrolavos Lab 2020 SSP"), "this [was] the first lab-wide security plan for the Astrolavos Lab." William Garrison,

the head of IT at the Astrolavos Lab, agreed, admitting that "prior to February 18, 2020, the lab did not have a system security plan put in place."

158. This means that in addition to not having a system security plan in place until February 2020, in violation of NIST Control 3.13.4, for this same period, the Astrolavos Lab had taken no action to implement, assess, or monitor the required NIST Security Controls for the lab, much less put in place any required plans of action to address deficiencies. This violates NIST Controls 3.12.1 (assess security controls), 3.12.3 (monitor security controls), and 3.12.2 (put in place plans of action to comply with security controls).

159. Defendants knew that they were required to develop and implement a system security plan for the EA Contract. In an August 8, 2019 email from Rebecca Caravati, on which Dr. Antonakakis was copied, Caravati wrote that "Manos also needs an SSP for AWD-101187/GT10002480," which refers to the EA Contract.

160. The failure to develop and implement a system security plan in connection with a DoD contract that required one was not unusual at Georgia Tech during this period. As Blake Penn, the head of the GRC team at the time, testified, for a substantial period there was "no enforcement" of the cybersecurity requirements at Georgia Tech, including the requirement for a system security plan. According to Penn, this was the case for at least a "couple of years."

161. Significantly, according to Smith, who drafted the Astrolavos Lab 2020 SSP, which purported to be a "lab-wide" system security plan, the scope of the Astrolavos Lab 2020 SSP did not include most of the desktops and laptops in the lab. Rather, at the direction of Garrison and others at the Astrolavos Lab, the scope was limited to the servers in the lab as well what is described in the Astrolavos Lab 2020 SSP as a personal laptop belonging to Dr. Antonakakis, which, according to the lab, would possess CUI, such as presentations to DARPA.

162. As Smith explained, by not protecting desktops and laptops that access servers with Covered Defense Information you "increase [the] risk" of a breach "if, for example, there were any screen grabbing software or anything along those lines, someone could take control of that system and be able to view the data that the person is remoting in to see."

163. In sworn testimony, Garrison admitted that it "wasn't correct" to exclude from the system security plan "endpoints"—such as desktops and laptops—that "would remotely connect" to servers in the lab, which he described as a "scoping problem."

164. Since February 2020, the Astrolavos Lab 2020 SSP was updated only once, in July 2020, when the names of additional members at the lab were added to the roster of individuals involved in the work for the relevant DoD contracts. The updates were non-substantive, and according to Garrison, the July 2020

system security plan was effectively a "continuation" of the original one from February 2020.

165. NIST Control 3.12.4 requires that system security plans be updated "periodically." According to both Smith and Leo Howell, Georgia Tech's most recent Chief Information Security Officer, Georgia Tech has interpreted this provision to require "yearly" updates of lab-wide system security plans.

166. For his part, Smith agreed that failure to update a lab-wide system security plan "would be noncompliance" with NIST Control 3.12.4, the "same way the failure to create an SSP in the first place is not in compliance."

167. This is consistent with guidance from NIST, which directs that to properly assess compliance with NIST Control 3.12.4, the assessor should confirm that (1) "a frequency to update the system security plan is defined" and (2) the "system security plan is updated with the defined frequency." NIST Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information (Jun. 2018) (NIST SP 800-171A) at 52.

168. On August 18, 2023, Georgia Tech implemented what it calls a Fundamental Research Exception SSP ("FRE SSP") at the Astrolavos Lab with respect to the Smoke Contract, in which Dr. Antonakakis specifically attested that the Smoke Contract "does not contain CUI" and agreed, pursuant to his signature

on the document indicating his approval of the FRE SSP, that the contract has no publication restrictions and all technical deliverables are marked Distribution A.

169. This was (i) nine months *after* GTRC and DARPA executed the modification of the Smoke Contract to include "non-fundamental research" tasks that would involve "Controlled Unclassified Information (CUI)" and require compliance with DFARS 7012 and 7020; (ii) ten months *after* DARPA issued the original DD254 for the Smoke Contract which affirmed that the contractor would "receive, store or generate controlled unclassified information (CUI)" and imposed a publication restriction as to all "Classified or Unclassified" information associated with the contract that is the equivalent of Distribution Statement F; and (iii) the same month that DARPA issued the revised DD254 for the Smoke Contract that contained the same provisions.

170. Dr. Antonakakis's attestation in the FRE SSP for the Smoke Contract was thus false, which was known to him, Georgia Tech, and GTRC at the time. In reality, as of November 2022, in connection with the Smoke Contract, the Astrolavos Lab was required to have a system security plan in place that was compliant with NIST Control 3.12.4.

171. The August 2023 FRE SSP does not qualify because it is not an actual system security plan. Neither does the Astrolavos Lab 2020 SSP because it has not been updated or reevaluated in any substantive way since February 2020.

172. Thus, in the period since November 2022, after the Smoke Contract modifications went into effect, the Astrolavos Lab has had no NIST compliant system security plan developed or implemented at the lab.

173. Accordingly, GTRC and Georgia Tech knowingly failed to develop and implement any kind of system security plan in the Astrolavos Lab until September 2019, when the Astrolavos Lab began its efforts to create a system security plan.

174. Additionally, Defendants knowingly excluded from the scope of the Astrolavos Lab SSP virtually all laptops and desktops in the lab, all of which regularly accessed the lab's servers which contained Controlled Defense Information. Thus, with respect to those covered contractor systems, the Astrolavos Lab never had a system security plan or security controls in place.

B. For Years, the Astrolavos Lab Failed to Install, Update, or Run Antivirus or Incident Detection Software on Endpoints, Servers, or its Network.

175. From at least 2016 when the Astrolavos Lab was started until December 2021, the Astrolavos Lab admittedly failed to systematically install, update, or run antivirus software on endpoints, such as desktops and laptops, servers, or the network on which the lab operates. The network and these endpoints were used to process, store, and transmit Covered Defense Information and/or Federal Contract Information.

176. Garrison, the Astrolavos Lab's head of IT, testified that as a general matter the Astrolavos Lab did not install, update, or run antivirus software on desktops, laptops, or servers at the lab. To the extent that some of the laptops or desktops might have had antivirus software installed on them, this was because those devices came with the antivirus software preinstalled. There was no requirement at the lab that the preinstalled antivirus software on those devices be run or updated.

177. Garrison testified that, during the lengthy multi-year period that the lab did not install, update, or run antivirus on its own machinery, he had believed that Georgia Tech employed antivirus on Georgia Tech's network, which the lab used. Garrison admitted, however, that this assumption was incorrect and that he later learned that the Georgia Tech network in fact never provided any such antivirus protection.

178. As Garrison testified, he learned that the "feature was not turned on or available"; and, thus, Garrison agreed that "the entire time . . . until December of 2021 . . . the firewall [on Georgia Tech's network] was . . . not running antivirus." There is no indication that the network employed antivirus prior to February 2020 either.

179. In any event, even if such antivirus software had been employed on Georgia Tech's network (which it was not), it would not have provided the

Astrolavos Lab sufficient protection from outside threats. This is because the lab permitted researchers to remove laptops from the lab and use them on unprotected networks outside of the lab.

180. Thus, even if Georgia Tech's network had provided antivirus detection at the lab for internet traffic entering the lab through that network (which it did not), this would not have provided protection from malicious code entering the lab through these unprotected laptops. This is particularly the case given that those laptops and desktops were not scoped into the Astrolavos Lab SSP, and thus were not subject to other important mandated cybersecurity protections, like required passcodes, two-factor authentication, and mandatory logging.

181. NIST Control 3.14.2 requires that antivirus software be installed throughout an IT environment, including "on various types of hosts, including workstations, servers, mobile computing devices, firewalls, email servers, web servers, and remote access servers."

182. At no point did Defendants inform DoD that the Astrolavos Lab was not running antivirus software, or seek or obtain permission from the DoD CIO to not satisfy this requirement or put in place an alternative to it.

183. Smith testified that in 2019, when he first began working on the system security plan for the Astrolavos Lab, it was his understanding that the lab did not employ antivirus and incident detection software.

184. In fact, pursuant to Georgia Tech's "Controlled Unclassified Information" policy, enacted in December 2017, like all Georgia Tech standard solutions for NIST SP 800-171 controls, antivirus software is required to be installed on all endpoints—such as desktops and laptops—at Georgia Tech where CUI may be present, unless installation of the antivirus software "is deemed too difficult or impractical to implement at the present time," in which case a compensating control may be implemented.

185. Consistent with this policy and the federal cybersecurity rules described herein, Smith suggested that the Astrolavos Lab install antivirus software. He was met with immediate and vigorous resistance, most notably from Dr. Antonakakis.

186. For example, in a November 22, 2019 email, Garrison explained to Smith: "I spoke with [Dr. Antonakakis] briefly this morning about . . . the policy requirement that he install active endpoint [antivirus] protection . . . and he wasn't receptive to such a suggestion." For his part, in a follow-up to Garrison's email to Smith, Dr. Antonakakis was more direct. He wrote in a November 22, 2019 email to Smith: "Endpoint [antivirus] agent is a nonstarter."

187. According to Garrison, other than Dr. Antonakakis's opposition, there was nothing preventing the lab from running antivirus protection. Dr. Antonakakis simply did not want to run it.

188. According to Smith, under pressure from the "executive leadership" at Georgia Tech, the GRC Team permitted the Astrolavos Lab not to run antivirus software, and instead to take "mitigating measures," such as relying on Georgia Tech's network firewall. These "compensating control[s]" were put in place in violation of Georgia Tech's CUI Policy, which only permitted the use of such compensating controls where the installation and use of antivirus was "deemed too difficult or impractical to implement," which was not the case at the Astrolavos Lab.

189. Smith did not agree with this decision. According to Smith, these mitigating measures, were "not the same thing as [running] an antivirus" on the devices in the lab. As far as Smith was concerned, these mitigating measures were "not a reasonable solution in this case." They were just the solutions imposed by Georgia Tech leadership in response to Dr. Antonakakis's complaints as a "star quarterback."

190. Ultimately, in late November/early December 2021, the relators in this action, both of whom worked on Georgia Tech's cybersecurity team, learned of the Astrolavos Lab's failure to install, update, and run antivirus and incident detection software, which they immediately identified as a violation of NIST SP 800-171 and applicable federal cybersecurity regulations, including DFARS 7012.

191. Relators then informed Rebecca Caravati, who at the time was the general manager of GTRC and the executive director of OSP at Georgia Tech (which oversees Georgia Tech's government contracting), and others on her team about the cybersecurity violations at the Astrolavos Lab. In response, Caravati and OSP suspended invoicing on the EA Contract due to this "noncompliance," and in order to avoid a "false claim."

192. Within a few days of the invoicing for his contracts being suspended, Dr. Antonakakis relented on his years-long opposition to the installation of antivirus software in the Astrolavos Lab. Georgia Tech's standard antivirus software was installed throughout the lab.

193. Referring to the installation of antivirus software throughout the Astrolavos Lab, Howell explained in a December 9, 2021 email: "Over the past three days, cybersecurity worked with IT staff from Dr. Antonakakis' lab to correct the two items 3.14.2 and 3.6.1 flagged as non-compliant with the current lab-wide SSP. As of late this evening, these two items have been corrected to bring the lab back into compliance."

194. As Defendants themselves have concluded, for years, the Astrolavos Lab was not compliant with NIST 800-171 because the lab had not installed, updated, or run antivirus software on covered contractor systems. In addition to being a violation of DFARS 7012, this is a violation FAR 52.204-21, which explicitly

requires the deployment of antivirus software on all federal contractor systems that process, store, or transmit nonpublic government information as Defendants did here.

195. Further, as Defendants themselves concluded when they suspended billing on the EA Contract, this noncompliance implicates the EA Contract. The submission of claims by Defendants to DoD when the Astrolavos Lab was processing, storing, or transmitting Controlled Defense Information and/or Federal Contract Information without the protection of antivirus software did, as those parties previously concluded, result in "false claims."

196. Thus, all the claims that Defendants submitted to DoD pursuant to the EA Contract from at least as early as May 2019 up to and until December 2021 are false.

197. As demonstrated by Caravati's emails suspending payments on the EA Contract, Defendants' years of cybersecurity noncompliance and submission of false claims to DoD were indisputably actually known to Defendants by at least December 2021, and Defendants recklessly disregarded and deliberately ignored the falsity of those claims even earlier.

198. Notwithstanding this, Defendants never informed DoD of their admitted non-compliance with NIST 800-171, DFARS 7012, or FAR 52.204-21, nor their submission of false claims to DoD for years in connection with the EA

Contract. Nor have Defendants refunded any of the amounts that they knew were unlawfully paid to them pursuant to those false claims.

C. Georgia Tech and GTRC Intentionally, Knowingly, and/or Negligently Provided DoD With a False Summary Level Score to Obtain and Retain DoD Contracts.

199. With the intention of inducing DoD to award and retain government contracts with GTRC and Georgia Tech, in December 2020, GTRC and Georgia Tech, through employees of both, submitted to DoD a false summary level score for the Georgia Tech campus that GTRC and Georgia Tech knew would mislead DoD to believe that the score applied to all of Georgia Tech's campus, and, at minimum, to actual IT systems at Georgia Tech where Georgia Tech intended to process, store, or transmit Controlled Defense Information in connection with its research pursuant to DoD contracts.

200. In fact, there is no campus-wide IT system at Georgia Tech and the summary level score that GTRC and Georgia Tech provided to DoD applied to no actual IT system at Georgia Tech, much less the Astrolavos Lab or any other environment at Georgia Tech that performs or might perform research pursuant to DoD contracts.

201. On December 3, 2020, Blake Penn, who at the time was the head of the GRC Team at Georgia Tech, and Eric Gill, who also worked on Georgia Tech's Cybersecurity team, submitted to DoD a summary level score on behalf of GTRC.

202. According to DoD records, the summary level score that Georgia Tech submitted to DoD on behalf of GTRC was a 98 out of 110. The "Standard used to Assess" was "NIST SP 800-171." The "assessment scope" was "enterprise" level. The "System Security Plan Assessed" was "CAMPUS RI SSP – GEORGIA TECH." And the "System Security Plan Date" was "11/30/2020." The "Plan of Action Completion Date" for those controls for which GTRC recognized that the Georgia Tech campus was not compliant was "12/31/2021."

203. According to Penn, shortly before he and Gill submitted the 98 score for the Georgia Tech campus to DoD, the GRC team was instructed by OSP that Georgia Tech needed to submit a score for the campus and that the GRC team should (i) create a system security plan for the entire Georgia Tech campus, (ii) score that system security plan, and then (iii) provide the campus' score to DoD.

204. As Penn explained it, "the decision was made by OSP that we needed to . . . have an SSP for Georgia Tech. There was some . . . requirement coming from the outside, I believe, that said Georgia Tech needs to have a SSP and needs to" submit the score for it to DoD. According to Penn, OSP informed the GRC team that the score was a "requirement" from DoD. As Penn understood it from OSP, "we now have to input this scoring – a self-scoring -- it's a self-evaluation essentially -- of compliance" with NIST 800-171.

205. The problem for Georgia Tech was that, according to Penn, there was "no way of evaluating [] Georgia Tech as a whole." This is because there is no one overarching IT system on Georgia Tech's campus. Rather, as Kyle Smith explained, there are "hundreds of different" IT systems across Georgia Tech's campus that "are all operating independently," including at least one in virtually every research lab. According to Smith, "most labs at Georgia Tech have their own IT system."

206. In response, the GRC Team created a "Georgia Tech system security plan," for the Georgia Tech campus, and calculated a score for that system security plan, which was a 98, and submitted that score to DoD, knowing that the score was not for any actual IT system at Georgia Tech.

207. Smith was tasked with creating the Georgia Tech campus-wide system security plan (GT SSP). As Smith described the GT SSP in his sworn testimony, it was a "model" for how a lab at Georgia Tech could comply with most of the NIST SP 800-171 controls by implementing certain solutions that were available at Georgia Tech. As Smith testified, what the GT SSP ''was meant to do was model if, like, everyone on campus were to use all of our standard solutions, and if everything were implemented in that way as designed, this is what that assessment would look like."

208. As Penn explained it, to come up with the 98 score that he and Gill reported to DoD on behalf of Georgia Tech and GTRC, the GRC team "assessed [Georgia Tech's] overall, kind of, ***fictitious*** environment for this, like, making, like, a ***virtual*** lab or something like that. And then we -- and then we scored it like we would any other" system security plan. (emphasis added)

209. Put simply, Georgia Tech assessed the model GT SSP, calculated a score of 98, and reported that score to DoD as if the score applied to an overarching IT system on the Georgia Tech campus or the campus at-large.

210. But the score did not apply to the Georgia Tech campus-at-large—and Penn knew at the time that he submitted the score to DoD that it is not possible to calculate an enterprise level score for the Georgia Tech campus. As Penn put it, "[i]t's beyond impossible." Moreover, Penn agreed that "[t]here is no, and there never has been . . . an SSP at the enterprise level implemented for Georgia Tech on the resident instruction side." As Penn put it, "[t]here's no way you could have something that's an actual -- actual, you know, operational plan for all those things." Penn went further, testifying that the campus-wide "SSP in no way said what happens at [the] Georgia Tech enterprise" level. In fact, according to Penn, "there's no document that exists that describes that . . . There can't be."

211. In his sworn testimony, Smith, who drafted the GT SSP, agreed that "this is not a scoring of an actual IT system at Georgia Tech." According to Smith,

the 98 score and the GT SSP "is not specifically associated to any active research at Georgia Tech," and, Smith agreed that its "not . . . identifying a particular IT system, much less a campus-wide IT system at Georgia Tech and saying, this is being done at Georgia Tech and therefore we deserve this score."

212. Nor did the individual labs throughout campus implement all of the controls precisely as set out in the GT SSP. It was merely a model.

213. Lummis was tasked with approving all system security plans at Georgia Tech, and thus all deviations to the model GT SSP in particular labs. When asked "How often were you approving deviations from the [model] SSP," Lummis answered: "Pretty much every single SSP. I don't think there's a single lab that can -- that was able to 100 percent do explicitly what was there." Lummis testified that the GT SSP "was not implemented throughout Georgia Tech as written." This was because it was "generally the situation" that "every SSP . . . [Lummis's] office approved involved at least one deviation from the GT SSP."

214. The Astrolavos Lab likewise did not implement the GT SSP. As Smith admitted, the Astrolavos Lab 2020 SSP does not "match" the GT SSP because "changes were made from the model SSP . . . to create the SSP for the Astrolavos Lab." This includes, at minimum, the decision by Georgia Tech to permit the Astrolavos Lab not to install, update, and run antivirus software at the lab. Accordingly, as Smith testified, the Astrolavos Lab "[a]bsolutely [can]not" rely

"on the campus-wide model SSP to establish its compliance with the system security plan requirements." This, Smith agreed, is because "the model SSP is . . . not actually evaluating anything, much less that lab," and "the score for the Georgia Tech campus-wide SSP . . . is not a score for the SSP for the Astrolavos Lab."

215. In fact, according to Smith, the Astrolavos Lab has no summary level score, because Georgia Tech never calculated one for it. And, based on DoD's records, Georgia Tech and GTRC never submitted a score for the Astrolavos Lab separate from the false 98 score that they submitted for the entire Georgia Tech campus.

216. This is consistent with the practice at Georgia Tech. Leo Howell, who is Georgia Tech's most recent Chief Information Security Officer, testified that "I don't think we do a score on a project-by-project or a lab-wide basis." Rather, according to Howell, the only score that Georgia Tech calculates is the campus-wide score that Georgia Tech and GTRC submit to DoD.

217. This is not because Georgia Tech is unable to calculate a summary level score for individual labs. As Howell explained, "I don't think there's anything, technically, that prevents it." Georgia Tech simply chooses not to calculate the score for individual system security plans.

218. The enterprise-level score of 98 that Georgia Tech and GTRC submitted to DoD in December 2020 is false. It does not reflect a score for any information system used to process, store, or transmit Controlled Defense Information in connection with Defendants' DoD contracts, including the Astrolavos Lab.

219. Georgia Tech and GTRC knew that the score was false when they submitted it to DoD. They knew that there was no campus-wide IT system at Georgia Tech, nor could there be. They knew that the score of 98 that they reported to DoD was not for any actual IT system at Georgia Tech, much less for one that would or could process, store, or transmit Covered Defense Information. They also knew that the score was not for the Astrolavos Lab or any other lab at Georgia Tech that performed work for DoD pursuant to government contracts.

220. Notwithstanding this knowledge, Georgia Tech and GTRC intentionally submitted the false 98 campus-wide score to DoD. During the relevant time period, December 2020 through December 2023, Georgia Tech and GTRC never clarified for DoD that the score is not for the entire campus or, in fact, any IT system at the Georgia Tech campus, much less any of the labs that perform work for DoD pursuant to government contracts, including the Astrolavos Lab. Further, GTRC falsely certified compliance with DFARS 7019, at least with respect to the Smoke Contract, and likely many others.

221. Thus, in December 2021, Georgia Tech and GTRC intentionally, knowingly, and negligently submitted a false enterprise level summary level score of 98 to DoD for the Georgia Tech campus, and falsely certified compliance with DFARS 7019, to induce DoD to award and retain government contracts with Georgia Tech and GTRC.

IV. Defendants Knew the Federal Cybersecurity Rules; They Knowingly, Intentionally, and/or Negligently Violated Those Rules In Connection with a Culture of Cybersecurity Noncompliance.

222. Defendants, as large, sophisticated government contractors with billions of dollars in DoD contracts over the years, knew the federal cybersecurity requirements at issue here. Defendants knew what those regulations required and that they were not compliant with them. Notwithstanding this, Defendants knowingly and intentionally submitted false claims to DoD, certifying each time that those claims were "in accordance with the agreements set forth in the application and award documents."

A. Defendants Knew the Federal Cybersecurity Requirements, What They Require, Their Importance, and that Violating those Requirements Could Lead to False Claims.

223. Defendants knew the federal cybersecurity requirements and the consequences for violating those requirements.

(i) DFARS 7012/NIST 800-171/FCA Compliance

224. Rebecca Caravati testified that as the general manager of GTRC, as well as the executive director of OSP, she understood that "invoicing the government when you are not compliant [with NIST 800 requirements] would be interpreted as a false claim."

225. Caravati further testified that "I trained my staff" on these requirements, namely, "Georgia Tech employees [from the] Office of Sponsored Programs," who worked with GTRC on government contracting. According to Caravati, "Dr. Abdallah and Rob Butera were present" for her trainings on NIST SP 800-171 and the FCA.

226. In these trainings, Caravati would "talk about that this is your contract, you have to comply." Caravati "would hand out . . . some slides to show them what the penalties were . . . . I had a slide -- and I had some examples of some universities that had paid a lot of money. You know it really happens; it's not just hypothetical."

227. Other Georgia Tech employees, including Georgia Tech's last two permanent Chief Information Security Officers, similarly testified that they understood that Defendants had to comply with federal cybersecurity requirements in order for Defendants to contract with the federal government.

228. Jimmy Lummis testified that: "In my understanding from Georgia Tech's perspective, Georgia Tech executes research on behalf of the federal government. And they obtain research contracts, and those contracts obligated us to comply with DFARS 7012." Leo Howell testified similarly, agreeing that "Georgia Tech needs to comply with NIST 800-171 if there's a 7012 clause in the contract."

229. This testimony is consistent with Georgia Tech's official policies. Georgia Tech's website identifies the following as part of the "Georgia Tech Controlled Unclassified Information Policy," which makes clear that "Georgia Tech is ***obligated*** to ensure that all systems and processes involved with CUI are compliant with NIST 800-171 ***to continue receiving Federal funds*** associated with the use of this data (either directly received from the government or indirectly through associated covered contracts and contractors)." (emphasis added)

230. Georgia Tech's website further demonstrates Georgia Tech's understanding of its obligations under federal cybersecurity regulations, declaring that "***compliance with NIST SP 800-171 . . . is required by December 31st, 2017 by the DoD*** for all entities that handle controlled unclassified information (CUI). Associated direct and indirect federal funding related to CUI is in the 100's of millions USD." (emphasis added)

231. Moreover, Georgia Tech's website leaves no doubt that it understood why it was important for Georgia Tech to comply with federal cybersecurity regulations, explaining in a section titled "Why is this important to Georgia Tech?" that "a failure to meet existing compliance requirements ***may result in contract termination and the loss of contract funds.***" (emphasis added).

232. Penn explained that he and Lummis were also well aware of the potential effect of Georgia Tech's widespread noncompliance with DFARS 7012 and NIST (SP) 800-171. Summarizing his prior testimony, Penn agreed that he and "Lummis knew that if Georgia Tech did not comply with the 7012 clause and 800-171 regulations that it could potentially lose some of the $360 million that it had earned in these government contracts," explaining that it was a "huge financial risk" for Georgia Tech.

(ii) System Security Plan and Security Controls

233. Defendants knew that they were required by federal cybersecurity regulations to develop and implement a system security plan as well as implement the 110 security controls under NIST SP 800-171 for all IT systems governed by DFARS 7012.

234. Defendants' employees including Caravati, who was a senior employee at Georgia Tech/GTRC and Kyle Smith knew that, at a minimum,

compliance with DFARS 7012 required having a system security plan for each relevant information system.

235. Consistent with this, Georgia Tech's "Resident Instruction System Security Plans (SSP's)" policy recognizes that a "System Security Plan (SSP) is ***required*** for Resident Instruction (RI) research efforts that will be performed on RI computers/networks or at RI locations if the contract includes the 7012 clause." (emphasis added)

236. This policy was adopted during the time that Lummis was Georgia Tech's CISO. Lummis explained the policy this way: "It is saying a system security plan must be in place when research is being conducted in resident instruction and performed on RI computers and networks." In other words, according to Lummis, "[i]f there is a [DFARS 7012] clause and it's being executed on campus systems and networks, then it has to have a campus SSP." Howell testified similarly, agreeing that "every lab or project that has a DFARS 7012 . . . [must] have their own SSPs."

237. As Blake Penn testified, for multiple years, there was "no enforcement" at Georgia Tech of the requirement for a system security plan. As Penn explained, labs at Georgia Tech routinely began work on DoD contracts without first developing and implementing system security plans or the associated NIST controls. This included the Astrolavos Lab.

238. Thus, at the time that Defendants entered into contracts with DoD, including the Astrolavos Lab Contracts, they knew that Georgia Tech was not and would not by December 31, 2017 be compliant with the controls in NIST SP 800-171, including its most basic requirement for a system security plan and plans of action to implement unimplemented security controls.

239. As Penn testified, the researchers "got money for doing something in a contract to where they had not yet even made an SSP for compliance with 800-171 and the compliance efforts came post facto," if at all. This, Penn understood was not permitted, because as Penn admitted, "[NIST] 800-171 actually requires the existence of an SSP . . . [s]o if the researchers didn't have a SSP they would -- by definition they would not have complied."

240. Thus, at the time they contracted with DoD, Defendants knew that they were not complying, and would continue not to comply, with the system security plan requirement, as well as the requirements to implement and monitor applicable security controls, as well as to put in place specific plans of action to comply with all the controls.

(iii) Antivirus

241. Defendants knew that they were required by federal cybersecurity rules to install, run, and update antivirus software throughout covered contractor systems. Lummis, Georgia Tech's former CISO, explained it succinctly in sworn

testimony: "DFARS 7012 requires compliance with NIST 800-171, and NIST 800-171 has antivirus requirements."

242. This is consistent with Georgia Tech's antivirus software policy, which requires the installation of antivirus on all systems at Georgia Tech except those that are public facing, such as Georgia Tech's public websites.

243. Georgia Tech, thus, knew that the Astrolavos Lab was not in compliance with federal cybersecurity regulations when it operated for years without antivirus.

244. Defendants confirmed this knowledge in contemporaneous emails. For example, on December 3, 2021, after learning that the Astrolavos Lab had not been running antivirus software for years, Caravati sent an email to Dr. Abdallah, Georgia Tech's Vice President of Research and the President of GTRC, and others, informing them that: "the Cybersecurity Team has just been advised that Professor Antonakakis is not compliant with his System Security Plan and thus GT is not compliant with the terms of its DARPA contract that support[s] Professor Antonakakis's research. Since the contract contains the 7012 clause, compliance is necessary to ***prevent risk of a GT false claim***." (emphasis added)

245. A few days later on December 6, 2021, Glen Campopiano, a director of project accounting at Georgia Tech, sent Dr. Antonakakis an email, copying others, that informed Dr. Antonakakis that "G&C Accounting has been instructed

to freeze" billing on the EA Contract "to prevent any further expenses from posting to these accounts effective today December 5. The reason for the spending freeze is your lab's non-compliance with NIST."

246. The email contained a note from Rebecca Caravati that read: "***Since we are not compliant at this time***, I am asking Grants and Contracts Accounting to suspend charges to the DARPA project until such time as we can confirm his lab's compliance with NIST. This is necessary to prevent invoicing the government while we have a ***known non-compliance, since invoices billed to the government could be considered a false claim***." (emphasis added).

247. Others at Georgia Tech also knew at that time that by not running antivirus software the Astrolavos Lab was not compliant with NIST 800-171. For example, Howell testified under oath to the following:

> Q. And did you agree with Ms. Caravati, when she looked into the issue, that there was non-compliance?
>
> A. Yes.
>
> Q. So as of December 2021, the Astrolavos Lab was not in compliance with NIST?
>
> A. Correct.

(iv) Summary Level Score

248. As with the other cybersecurity requirements, Defendants were aware of the requirement that they provide DoD with accurate summary level scores for each of the relevant IT systems as a condition of contracting with DoD.

249. For her part, Caravati testified as to the following:

> Q. . . . Ms. Caravati, do you understand that DoD contracts containing the Section 7012 clause require contractors to submit a self-assessment score to the Department of Defense?
>
> A. Yes.
>
> Q. And do you understand that this self-assessment score is based on a review of a system security plan that's associated with the information system that's being used when performing a DoD contract subject to the 7012 clause?
>
> A. Yes.
>
> . . .
>
> Q. And was it your understanding that Georgia Tech had to report this self-assessment score via the DoD portal in order to be eligible to bid on DoD contracts containing the 7012 clause?
>
> A. Yes.
>
> Q. Did you share that understanding with anybody else?
>
> A. Yes, I did.
>
> Q. Who did you share that understanding with?
>
> A. Rob Butera. Dr. Abdallah. GRC. OIT. My colleagues in OSP.

250. As Caravati understood the requirement for a summary level score, and explained it to others at Georgia Tech: "you can't even propose [for a DoD contract] unless you have this SSP and you have this self-assessment score in that portal." As Caravati put it, if Georgia Tech and GTRC did not report a score for Georgia Tech then: Georgia Tech "would not be able to submit proposals on contracts where you knew the resulting contract would have 7012."

251. This is consistent with the testimony of Lummis and Howell, both of whom testified that they were familiar with the requirement that Defendants had

to provide a summary level score to DoD. As Lummis explained, "we had to log in to a particular system and attest to our compliance."

252. Blake Penn, who submitted the first summary level score for GTRC and Georgia Tech to DoD, explained that he understood that the score "was a thing that the government used to rate its -- or DoD used it to rate its suppliers on compliance with the 171." According to Penn, OSP informed him that "we now have to input this scoring – a self-scoring -- it's a self-evaluation essentially -- of compliance into the SPRS system."

253. Kyle Smith testified similarly, explaining that he understood that Defendants were required to report a separate score for each lab because the labs were all different and had different and unique system security controls in place.

254. Caravati concluded that it would be "misleading" for Georgia Tech and GTRC to report a score for the Georgia Tech campus to DoD as Georgia Tech's only score. As Caravati testified, "my concern was, it was going to look to the government as if that was our score, when that was a score of a whole bunch of little things. It wasn't, you know -- well, maybe not that little. But they would think that was the score for everything, that -- ***it could be misleading***." (emphasis added). As Caravati further explained, "my concern was that the government . . . would just look at that in the portal and think, oh, that's their overall score."

255. According to Caravati, she voiced her concern at Georgia Tech that posting a score for the Georgia Tech campus would "mislead" the government, be "less than forthright," or an outright "misrepresentation." Notwithstanding these warnings, Georgia Tech and GTRC reported the "misleading" score to DoD.

256. After posting a single enterprise level score of 98 for the Georgia Tech campus in December 2020, neither GTRC nor Georgia Tech (i) corrected that score, nor (ii) provided DoD with individual scores for any of the labs at Georgia Tech.

V. Violations of Federal Cybersecurity Regulations are Material.

257. Compliance with federal cybersecurity requirements is material to the United States' contracting and payment decisions on DoD contracts.

A. DoD Cybersecurity is Critical to National Defense.

258. Lax cybersecurity compliance poses an existential threat to the federal government, DoD, federal contractors, and the national security of the United States. The problem is so significant that each of the last three presidents has issued executive orders addressing the issue.

259. Most recently, on May 21, 2021, President Biden issued an "Executive Order on Improving the Nation's Cybersecurity." In that executive order, the President warned that:

> The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy.

> . . .
>
> The Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems, whether they are cloud-based, on-premises, or hybrid.
>
> . . .
>
> It is the policy of my Administration that the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security. The Federal Government must lead by example. All Federal Information Systems should meet or exceed the standards and requirements for cybersecurity set forth in and issued pursuant to this order.

260. A few years earlier, on May 11, 2017, then President Trump issued a "Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure." That executive order noted that the federal government's "IT and data should be secured responsibly using all United States Government capabilities." This is because "cybersecurity risk" poses a threat "to national security."

261. Several years earlier, on February 12, 2013, then President Obama issued an "Executive Order" on "Improving Critical Infrastructure Cybersecurity." As that executive order explained: "The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront. The national and economic security of the United States depends on the reliable functioning of the Nation's critical infrastructure in the face of such threats."

262. Finding the issue of cyber-attacks on U.S. interests so dire, almost a decade ago, on April 1, 2015, President Obama issued an executive order to "declare a national emergency to deal with" the "threat" of "malicious cyber-enabled activities originating from, or directed by persons located, in whole or in substantial part, outside the United States." The executive order declared that that the threat of cyber-attacks on American interests "constitute an unusual and extraordinary threat to the national security, foreign policy, and economy of the United States."

263. For its part, DoD has been clear that: "The protection of controlled unclassified information on contractor information systems is critically important to the Department of Defense." Memorandum, Office of the Under Secretary of Defense, *Contractual Remedies to Ensure Contractor Compliance with Defense Federal Acquisition Regulation Supplement Clause 252.204-7012,* at 1 (Jun. 16, 2022) (Under Secretary Memo).

264. DoD has been dire in its warnings regarding the threat of cyberattack on DoD and its contractors. In 2015, in adopting an interim rule that implemented the current version of DFARS 7012, DoD highlighted the "urgent need to protect covered defense information and gain awareness of the full scope of cyber incidents being committed against defense contractors." This was because of the

"increased [] vulnerability of DoD information via attacks on its systems and networks and those of DoD contractors." 80 Fed. Reg. 51739, 51741 (Aug. 26, 2015).

265. In 2020, DoD sounded the alarm on the urgent need for defense contractors to comply with federal cybersecurity requirements. In the interim rule enacting DFARS 7019 and 7020, DoD declared that "urgent and compelling reasons exist to promulgate th[e] interim rule" because "[m]alicious cyber actors have targeted, and continue to target, the DIB sector, which consists of over 200,000 small-to-large sized entities that support the warfighter." 85 Fed. Reg. at 61517-518.

266. According to DoD, "[t]he Department has been focused on improving the cyber resiliency and security of the DIB sector for over a decade as evidenced by the development of minimum cybersecurity standards and . . . [the] implementation of those standards in the FAR and DFARS." *Id.* at 61518.

267. Congress recognized the same threat. As DoD explained: "In the Senate Armed Services Committee Report to accompany the NDAA for FY 2020, the Committee expressed concern that DIB contractors are an inviting target for our adversaries, who have been conducting cyberattacks to steal critical military technologies." *Id.*

268. DoD thus warned in 2020 that: "There is an urgent need for DoD to immediately begin assessing where vulnerabilities in its supply chain exist and

take steps to correct such deficiencies, which can be accomplished by requiring contractors and subcontractors that handle DoD CUI on their information systems to complete a NIST SP 800-171 Basic Assessment." *Id.*

269. As importantly, DoD further warned: "It is equally urgent" that "DIB contractors that have not fully implemented the basic safeguarding requirements under FAR clause 52.204-21 or the NIST SP 800-171 security requirements pursuant to DFARS 252.204-7012 begin correcting these deficiencies immediately. These are cybersecurity requirements contractors and subcontractors should have already implemented (or in the case of implementation of NIST SP 800-171, have plans of action to correct deficiencies) on information systems that handle CUI." *Id.* at 61518-519

270. According to DoD, the purpose of DFARS 7019 and 7020 is to "ensure[] contractors and subcontractors focus on full implementation of existing cybersecurity requirements on their information systems and expedite[] the Department's ability to secure its supply chain." *Id.* at 61519.

271. The U.S. Department of Justice (DOJ) has echoed these concerns. On October 6, 2021, DOJ announced "the launch of the department's Civil Cyber-Fraud Initiative to "utilize the False Claims Act to pursue cybersecurity related fraud by government contractors and grant recipients [and] 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."

272. The President's National Cybersecurity Implementation Plan, version two of which was published in May 2024, specifically highlighted DOJ's Civil Cyber Fraud Initiative as a critical tool in promoting effective cybersecurity for the federal government, explaining:

> The Civil Cyber-Fraud Initiative (CCFI) uses DOJ authorities under the False Claims Act to pursue civil actions against government grantees and contractors who fail to meet cybersecurity obligations. The CCFI will 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 cyber incidents and breaches.

B. Cybersecurity Compliance is a Condition of Contract.

273. In light of the importance of cybersecurity compliance, DoD has made compliance with federal cybersecurity mandates a condition of contract, and thus a condition payment.

274. By its very terms, compliance with DFARS 7019 "is a condition of contract award." 85 Fed. Reg. at 61509; DFARS 7019. The requirement is so significant, contracting officers at DoD are not lawfully permitted to enter into most contracts with bidders unless they have submitted to DoD the summary level score required by DFARS 7019.

275. In 2022, DoD reemphasized this requirement in a memorandum from the Office of the Under Secretary of Defense that was directed to be distributed to DoD contracting officers, declaring that: "Contracting Officers are also reminded . . . [that] if a contractor is required by a contract containing DFARS clause 252.204-7012 to implement NIST SP 800-171 on a covered contractor information system relevant to a new contract . . . ***the Contracting Officer must verify, prior to award, the contractor has the summary level score*** of a current NIST SP 800-171 DoD Assessment posted in SPRS." Under Secretary Memo at 2-3 (emphasis added).

276. DoD also requires contractors to expressly certify or represent their compliance with DFARS 7019. For example, at the time of bidding, DARPA mandates such a certification or representation of compliance with DFARS 7019 in connection with all of its contracts. GTRC provided such a certification or representation of compliance with DFARS 7019 in connection with its bid for at least the Smoke Contract.

277. A similar representation of compliance with DFARS 7012 is required in virtually every DoD contract pursuant to DFARS 7008. In connection with bids for DoD contracts, defense contractors are required to represent "[b]y submission of this offer" that they "will implement" all the security controls in NIST SP 800-171 "not later than December 31, 2017."

278. Moreover, DoD regulations mandate in no uncertain terms that "Contractors and subcontractors are ***required*** to provide adequate security on all covered contractor information systems," DFARS 7302(a)(1) (emphasis added), and that "[t]he security requirements ***required*** by [DFARS 7012], ***shall*** be implemented for all covered defense information on all covered contractor information systems that support the performance of this contract." DFARS 7008(b) (emphasis added).

279. This is why the Under Secretary of Defense has emphasized that "Contractors must implement all of the NIST SP 800-171 requirements and have a plan of action and milestones . . . for each requirement not yet implemented [and that failure to do so] . . . may be considered ***a material breach of contract*** requirements." (emphasis added)

280. Consistent with this, on August 8, 2024, DARPA sent a "cure notice" to Georgia Tech and GTRC in connection with the SMOKE Contract. The cure notice referenced the alleged violations of federal cybersecurity rules (including DFARS 7012 and 7019) detailed herein, which the notice indicated "endangers performance of the contract." The notice further demanded that Georgia Tech and GTRC "cure any deficiencies within 30 days of receipt of this notice." The notice further indicated that the "Government reserves the right to issue a notice of

termination" of the SMOKE Contract "for noncompliance with the terms" of that contract.

281. Given this, DoD cybersecurity requirements, including those at issue here, go to the heart of the bargain of all DoD contracts that involve covered defense information, including the Astrolavos Lab Contracts.

VI. GTRC Submitted False Claims to DoD.

282. GTRC knowingly submitted false claims to DoD for the Astrolavos Contracts.

A. The EA Contract

283. 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.

284. 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.

285. The last of these invoices (with invoice number CI-00049292) was submitted to DoD on April 22, 2022 for $265,490.51, for work that was performed in July and August 2021.

286. For the period May 2019 through the end of performance under the EA Contract, GTRC and Georgia Tech submitted invoices totaling $10,237,621.79 in connection with work performed on the EA Contract. These invoices were paid in full by DoD. GTRC and Georgia Tech split between them the amounts that were paid to them by DoD pursuant to the EA Contract.

B. The Smoke Contract

287. The Astrolavos Lab began work on the Smoke Contract in October 2022. On June 26, 2023, GTRC submitted its first invoice (with invoice number CIOO61405) to DoD for work on the Smoke Contract for $816,069.77. GTRC submitted its next two invoices (with invoice numbers CI0069278 and CI0061864) to DoD for the Smoke Contract on July 21, 2023 for $1,217,612.02 and $1,562,882.39 respectively.

288. In all, GTRC submitted 14 invoices to DoD for work performed on the Smoke Contract. Each of the invoices described the services provided or goods purchased in connection with the contract. Each invoice included the following certification: "I certify the amounts herein claimed are in accordance with the application and award documents and have not been previously claimed." None

of the invoices mention Georgia Tech or GTRC's failure to comply with applicable federal cybersecurity rules and regulations.

289. The last of these invoices (with invoice number CI0082883) was submitted to DoD on April 24, 2024 for $322,273.39. In total, to date, GTRC has submitted invoices totaling $9,279,799 in connection with the Smoke Contract. These invoices were paid in full by DoD. GTRC and Georgia Tech split between them the amounts that were paid by DoD pursuant to the Smoke Contract.

VII. Damages

290. The United States has suffered damages because of Defendants' failure to comply with applicable federal cybersecurity rules and regulations, and their false representations of compliance in connection with the Astrolavos Lab Contracts. DoD has paid Defendants millions of dollars under the Astrolavos Lab Contracts on false pretenses.

291. At bottom, DoD paid for military technology that Defendants stored in an environment that was not secure from unauthorized disclosure, and Defendants failed to even monitor for breaches so that they and DoD could be alerted if information was compromised. What DoD received for its funds was of diminished or no value, not the benefit of its bargain.

292. Additionally, Defendants were unjustly enriched and paid by mistake at the expense of the United States.

CAUSES OF ACTION

COUNT I
Presentment of False Claims; 31 U.S.C. § 3729(a)(1)(A)
(Against GTRC)

293. The United States incorporates and re-alleges all the allegations contained in this Complaint-in-Intervention into this paragraph.

294. GTRC knowingly presented or caused to be presented material false or fraudulent claims for payment or approval to the United States in violation of DFARS 7302; 7008; 7012; and FAR 52.204-21, that were false or fraudulent because despite having Covered Defense Information, Defendants failed for multiple years to provide "adequate security" for covered contractor information systems relevant to the Astrolavos Lab Contracts by, at the minimum, knowingly failing to (i) develop, document, implement, and periodically update system security plans and associated NIST SP 800-171 security controls for the covered systems at the Astrolavos Lab, and (ii) install, update, and run antivirus and incident detection software throughout the covered systems at the Astrolavos Lab.

295. GTRC knowingly presented or caused to be presented material false or fraudulent claims for payment or approval to the United States in violation of DFARS 7302; 7019; and 7020 that were false or fraudulent because GTRC and Georgia Tech failed to submit an accurate summary level score for GTRC, Georgia Tech, the Astrolavos Lab or any other lab at Georgia Tech for which GTRC entered

into contracts with DoD which required submission of a summary level score, and instead submitted a false or fraudulent score for the Georgia Tech campus.

296. GTRC failed to disclose to the United States that (1) each of its certifications was false; (2) that it had not provided adequate security on all covered contractor systems; (3) that it had not implemented the required NIST Controls on all covered contractor systems or implemented plans of action for unimplemented controls; (4) that it had failed to install, run, and update antivirus software on covered contractor information systems; (5) that the score of 98 reported to DoD for the Georgia Tech campus was false because (i) Georgia Tech neither has nor could it ever have a campus-wide IT system, and (ii) the score did not apply to any actual IT system at Georgia Tech where research for DoD involving Covered Defense Information was or would be performed, or to any actual IT system at Georgia Tech that could or would possess or transmit Covered Defense Information in connection with a DoD contract, including any IT system at the Astrolavos Lab; and (6) Defendants had otherwise failed to comply with DFARS 7302; 7008; 7012; 7019; 7020; and FAR 52.204-21.

297. GTRC's conduct was material to the United States and induced the United States to enter into and/or retain contracts with GTRC, make payments to GTRC to which it was not entitled pursuant to those contracts, and otherwise damaged the United States. The United States is entitled to an award of treble its

damages, plus statutory penalties pursuant to 31 U.S.C. §§ 3729(a)(1). The United States is also entitled to its costs prosecuting this litigation against GTRC, pursuant to 31 U.S.C. § 3729(a)(3).

COUNT II
False Record or Statement; 31 U.S.C. § 3729(a)(1)(B)
(Against GTRC)

298. The United States incorporates and re-alleges all the allegations contained in this Complaint-in-Intervention into this paragraph.

299. GTRC knowingly made, used, or caused to be made or used, false records or false statements that were material to claims for payment or approval to the United States.

300. GTRC falsely represented or certified to the United States that: (1) pursuant to DFARS 7008, that it "will implement the security requirements specified by [NIST (SP) 800–171] . . . not later than December 31, 2017"; and (2) on each and every invoice that it submitted to DoD that it "certif[ies] that all payments are for appropriate purposes and in accordance with the agreements set forth in the application and award documents" or that it "certif[ies] the amounts herein claimed are in accordance with the application and award documents and have not been previously claimed."

301. GTRC falsely represented or certified to the United States that it complied with DFARS 7019 and DFARS 7020 by submitting an accurate summary

level score for "each" IT system that was "relevant" to the applicable bid and contract.

302. GTRC failed to disclose to the United States that (1) each of its representations was false; (2) it had not provided adequate security on all covered contractor systems; (3) it had not implemented the required NIST Controls on all covered contractor systems or put in place plans of action to implement those controls that had not been implemented; (4) it had failed to install, run, and update antivirus software on covered contractor information systems; and (5) it had otherwise failed to comply with DFARS 7302; 7008; 7012; and FAR 52.204-21.

303. GTRC failed to disclose to the United States that: (1) the summary level score of 98 for the Georgia Tech campus was false because (i) Georgia Tech neither has nor could it have a campus-wide IT system, and (ii) the score did not apply to any actual IT system at Georgia Tech where research for DoD involving Covered Defense Information was or would be performed, or to any actual IT system at Georgia Tech that could or would possess or transmit Covered Defense Information in connection with a DoD contract, including any IT system at the Astrolavos Lab; and (6) Defendants had otherwise failed to comply with DFARS 7302; 7008; 7012; 7019; 7020; and FAR 52.204-21.

304. GTRC's representations and certifications were material to the United States and the United States relied on them in making the decision to enter into

contracts with GTRC and to retain those contracts. GTRC's conduct thus induced the United States to enter into and/or retain contracts with GTRC, and caused the United States to pay monies to GTRC to which it was not entitled, thereby damaging the United States.

305. The United States is entitled to an award of treble its damages, plus statutory penalties pursuant to 31 U.S.C. §§ 3729(a)(1). The United States is also entitled to its costs prosecuting this litigation against GTRC, pursuant to 31 U.S.C. § 3729(a)(3).

COUNT III
Fraud; Federal Common Law
(Against Georgia Tech and GTRC)

306. The United States incorporates and re-alleges all the allegations contained in this Complaint-in-Intervention into this paragraph.

307. In December 2020, Georgia Tech and GTRC intentionally submitted to the United States a false and fraudulent summary level score of 98 for the Georgia Tech campus.

308. At the time that Georgia Tech and GTRC submitted the false and fraudulent score to the United States, Georgia Tech and GTRC knew that the score was false and fraudulent because they knew: (1) that the Georgia Tech campus had no campus-wide IT system; (2) the Georgia Tech campus could never have a campus-wide IT system; (3) that the score reported to DoD did not apply to any

actual IT system at Georgia Tech, much less one that was campus-wide, much less one where active research for DoD was taking or would take place, much less one for the Astrolavos Lab or any other lab at Georgia Tech; (4) that all of the labs at Georgia Tech, including the Astrolavos Lab, had no summary level score because, as a matter of policy and practice, Georgia Tech did not calculate scores for individual lab environments where actual research for DoD was or would be performed; and (5) that no lab at Georgia Tech was required to implement the GT SSP, from which the 98 score reported to DoD was derived, and that, in fact, labs at Georgia Tech, including the Astrolavos Lab, had generally not implemented the GT SSP as written.

309. At the time that Georgia Tech and GTRC submitted the false score to the United States, they were warned by their own employee, Rebecca Caravati, that providing the false score to DoD would would "mislead" the government, be "less than forthright," or constitute an outright "misrepresentation" to the government.

310. Notwithstanding these warnings, Georgia Tech and GTRC submitted the false score for the Georgia Tech campus. This is because Georgia Tech and GTRC understood that submitting a score was a "condition of contract." And that if a score was not provided to the United States that applied to all the labs at Georgia Tech that performed work with DoD, those labs in particular, and Georgia

Tech and GTRC in general, would no longer be eligible for DoD contracts. Put simply, Georgia Tech and GTRC intentionally submitted the false score because "[t]hey wanted the money."

311. Georgia Tech and GTRC thus intended to deceive DoD into believing that the score it reported to DoD applied to a campus-wide IT environment that applied to the work to be performed by labs at Georgia Tech that would seek to contract with DoD.

312. The United States relied on the false 98 score that Georgia Tech and GTRC posted in December 2023 to determine that GTRC, on behalf of Georgia Tech, was eligible to bid on contracts for DoD, including the Smoke Contract. DoD believed, as represented by Georgia Tech and GTRC, that the 98 score applied to the Georgia Tech campus and thus the lab environments at Georgia Tech that would perform research for DoD pursuant to applicable government contracts. The false score was material to the United States' contracting and payment decisions with respect to contracts that it entered into with GTRC for work that was to be performed by Georgia Tech.

313. The United States relied on the false summary level score that Georgia Tech and GTRC posted in December 2023 to enter into contracts with GTRC on behalf of Georgia Tech, including the Smoke Contract, and to make payments to GTRC that would later be shared with Georgia Tech pursuant to those contracts.

314. The United States has suffered damages because of Georgia Tech and GTRC's alleged conduct.

COUNT IV
Negligent Misrepresentation; Federal Common Law
(Against Georgia Tech and GTRC)

315. The United States incorporates and re-alleges all the allegations contained in this Complaint-in-Intervention into this paragraph.

316. In December 2020, Georgia Tech and GTRC submitted to the United States a false summary level score of 98 for the Georgia Tech campus.

317. At the time that Georgia Tech and GTRC submitted the false score to the United States, Georgia Tech and GTRC were at least negligent and in fact knew that the score was false because they knew: (1) that the Georgia Tech campus had no campus-wide IT system; (2) the Georgia Tech campus could never have a campus-wide IT system; (3) the 98 summary level score reported to DoD did not apply to any actual IT system at Georgia Tech, much less one that was campus-wide, much less one where active research for DoD was taking or would take place, much less one for the Astrolavos Lab or any other lab at Georgia Tech; (4) all of the labs at Georgia Tech, including the Astrolavos Lab had no summary level score, because, as a matter of policy and practice, Georgia Tech did not calculate summary level scores for individual lab environments where actual research for DoD was or would be performed; and (5) no lab at Georgia Tech was required to

implement the GT SSP, from which the 98 score reported to DoD was derived, and that, in fact, labs at Georgia Tech, including the Astrolavos Lab, had generally not implemented the GT SSP as written.

318. Georgia Tech and GTRC had a duty of competence and reasonable care in reporting the summary level score to the United States. Georgia Tech and GTRC knew that reporting the score was a "condition of contract" and that the United States would rely on the existence of the score in assessing their eligibility for DoD contracts. Further, Georgia Tech and GTRC certified and represented to the United States in connection with individual contracts (including the Smoke Contract) that they complied with DFARS 7019, which is the regulation that mandated that GTRC and Georgia Tech submit an accurate summary level score to the United States.

319. Georgia Tech and GTRC violated their duty of competence and reasonable care by negligently certifying and representing their compliance with DFARS 7019 and by negligently representing to the United States that the 98 score was for a campus-wide IT system that actually existed at Georgia Tech on which labs at Georgia Tech could or would perform research for DoD in connection with government contracts and where covered defense information could or would be transmitted or stored.

320. Georgia Tech and GTRC further violated their duty of competence and reasonable care by negligently omitting in their communications to the United States that the 98 score was (1) false; (2) not for a campus-wide IT system at Georgia Tech, because no such campus-wide IT system did or could exist at Georgia Tech; and (3) did not apply to the Astrolavos Lab or any other lab at Georgia Tech where research was or would be performed for DoD in connection with a government contract with GTRC or Georgia Tech, or to any IT system at Georgia Tech that would or could possess Covered Defense Information.

321. The United States reasonably relied on the false summary level score that Georgia Tech and GTRC posted in December 2020 to determine that GTRC, on behalf of Georgia Tech, was eligible to bid on certain contracts for DoD, including the Smoke Contract, based on the representation by Georgia Tech and GTRC that the score applied to the Georgia Tech campus and thus the lab environments at Georgia Tech that would perform research for DoD pursuant to applicable government contracts and that may possess or transmit Covered Defense Information.

322. The United States reasonably relied on the false summary level score that Georgia Tech and GTRC posted in December 2020 to enter into contracts with GTRC on behalf of Georgia Tech, including the Smoke Contract, and to make

payments to GTRC that would later be shared with Georgia Tech pursuant to those contracts, to which neither party was entitled.

323. The United States has suffered damages because of GTRC and Georgia Tech's alleged conduct.

COUNT V
Negligent Misrepresentation; Federal Common Law
(Against GTRC)

324. The United States incorporates and re-alleges all the allegations contained in this Complaint-in-Intervention into this paragraph.

325. In connection with the Astrolavos Lab Contracts, GTRC negligently represented or certified to the United States (1) pursuant to DFARS 7008, that it "will implement the security requirements specified by [NIST (SP) 800–171] . . . not later than December 31, 2017"; and (2) on each and every invoice that it submitted to DoD that it "certif[ies] that all payments are for appropriate purposes and in accordance with the agreements set forth in the application and award documents" or that it "certif[ies] the amounts herein claimed are in accordance with the application and award documents and have not been previously claimed."

326. GTRC had a duty of competence and reasonable care in certifying and representing its compliance with applicable federal regulations, including DFARS 7012, and in certifying in connection with invoices it submitted to the United States

that "all payments are for appropriate purposes and in accordance with the agreements set forth in the application and award documents" or "the amounts herein claimed are in accordance with the application and award documents."

327. The United States reasonably relied on GTRC's false certifications to enter in the Astrolavos Lab Contracts with it to make payments pursuant to the invoices that GTRC submitted to the United States that contained the above referenced certifications.

328. The United States has suffered damages because of GTRC's alleged conduct.

COUNT VI
Unjust Enrichment; Federal Common Law
(Against Georgia Tech and GTRC)

329. The United States incorporates and re-alleges all the allegations contained in this Complaint-in-Intervention into this paragraph.

330. This is a claim for the recovery of monies by which Defendants have been unjustly enriched. By obtaining government funds to which they were not entitled, Defendants were unjustly enriched, and are liable to account and pay such amounts, or the proceeds therefrom, which are to be determined at trial, to the United States.

COUNT VII
Payment by Mistake; Federal Common Law
(Against GTRC and Georgia Tech)

331. The United States incorporates and re-alleges all the allegations contained in this Complaint-in-Intervention into this paragraph.

332. This is a claim against GTRC and Georgia Tech for the recovery of monies paid by the United States to them as a result of a mistaken understandings of facts.

333. The false claims which GTRC submitted to the United States' agents were paid by the United States based upon mistaken or erroneous understandings of material fact. GTRC then distributed a portion of the monies that the United States paid to it to Georgia Tech.

334. The United States, acting in reasonable reliance on the truthfulness of the claims and the truthfulness of Defendants' certifications and representations, paid GTRC certain sums of money to which it was not entitled, a portion of which GTRC then distributed to Georgia Tech, and thus, GTRC and Georgia Tech are liable to account and pay such amounts, which are to be determined at trial, to the United States.

COUNT VIII
Breach of Contract; Federal Common Law
(Against GTRC)

335. The United States incorporates and re-alleges all the allegations contained in this Complaint-in-Intervention into this paragraph.

336. GTRC entered into the Astrolavos Lab Contracts with the United States.

337. As alleged herein, GTRC breached those contracts by violating its obligations under DFARS 7302, 7008, 7012, 7019, 7020, and FAR 52.204-21, which were incorporated into their contracts with the United States, and by falsely certifying their compliance with DFARS 7012, 7019, and 7020.

338. The United States has suffered damages because of GTRC's alleged conduct.

PRAYER FOR RELIEF

WHEREFORE, the United States demands and prays that judgment be entered in its favor against Defendants, specifically against GTRC on all counts, and against Georgia Tech on Counts 3, 4, 6, and 7:

- On the First and Second Counts under the False Claims Act, for the amount of the United States' damages, trebled as required by law, and such civil penalties as are permitted by law, as well as its costs pursuing this action, together with all such further relief as may be just and proper.
- On the Third, Fourth, Fifth, and Eighth Counts for Fraud, Negligent Misrepresentation, and Breach of Contract, the amount

of the United States' damages and applicable interest together with all such further relief as may be just and proper.

- On the Sixth Count for unjust enrichment, for the amounts by which Defendants were unjustly enriched, plus interest, costs, and expenses, and for all such further relief as may be just and proper.

- On the Seventh Count for payment by mistake, for the amounts the United States paid by mistake, plus interest, costs, and expenses, and for all such further relief as may be just and proper.

DEMAND FOR JURY TRIAL

The United States demands a trial by jury.

Respectfully submitted,

BRIAN M. BOYNTON
Principal Deputy Assistant Attorney General

RYAN K. BUCHANAN
United States Attorney
Northern District of Georgia

By: s/ Jake Shields
JAMIE ANN YAVELBERG
SARA MCLEAN
JAKE M. SHIELDS
DC Bar No. 493460
U.S. Department of Justice
Civil Division, Fraud Section
175 N. Street N.E.
Washington, DC 20002
Tel: (202) 514-9401
Fax: (202) 514-0280
jake.m.shields@usdoj.gov

By: s/ Adam D. Nugent
ADAM D. NUGENT

ASSISTANT U.S. ATTORNEY
Georgia Bar No. 381008
MELANIE D. HENDRY
Georgia Bar No. 867550
600 Richard B. Russell Federal Bldg.
75 Ted Turner Drive, SW
Atlanta, Georgia 30303
Telephone: (404) 581-6000
Facsimile: (404) 581-6181
adam.nugent@usdoj.gov
melanie.hendry@usdoj.gov

Counsel for the United States