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

UNITED STATES OF AMERICA ex rel. CHRISTOPHER CRAIG and KYLE KOZA,	)
Plaintiff-Relators,	) **FILED UNDER SEAL**
v.	) Case No. _____
	) **JURY TRIAL DEMANDED**
GEORGIA TECH RESEARCH CORPORATION and GEORGIA INSTITUTE OF TECHNOLOGY,	)
Defendants.	)

COMPLAINT

1. Relators Christopher Craig and Kyle Koza bring this action on behalf of themselves and the United States of America against Defendants Georgia Tech Research Corporation and Georgia Institute of Technology for violations of the federal False Claims Act, 31 U.S.C. §§ 3729 *et seq*. ("False Claims Act" or the "FCA").

JURISDICTION AND VENUE

2. This Court has jurisdiction over this action pursuant to 31 U.S.C. § 3732(a) and 28 U.S.C. §§ 1331, 1345.

3. Venue is proper in this district under 28 U.S.C. §§ 1391(b) and 31 U.S.C. § 3732(a), as one or more of the defendants resides or transacts business in this

jurisdiction and violations of the False Claims Act described herein occurred in this district.

PARTIES

4. Defendant Georgia Tech Research Corporation ("GTRC") is a Georgia-incorporated domestic nonprofit, with its principal place of business at 926 Dalney St. NW, Atlanta, GA 30332-0415.

5. Upon information and belief, GTRC is a party to hundreds of contracts with the Department of Defense (DoD), which are subject to NIST compliance and are therefore at issue in this matter, as well as subcontractor to many DoD contracts held by Lockheed Martin.

6. Defendant Georgia Institute of Technology ("GIT") is a public research university established by the State of Georgia in Atlanta in 1885. GIT is a premier research institution, maintaining a one-billion-dollar portfolio of research, which includes the Georgia Tech Research Institute and ten other interdisciplinary research institutes.

7. Defendant Georgia Tech Research Institute ("GTRI") is a nonprofit, applied research division of GIT. GTRI has more than 2,800 employees, supporting eight laboratories, in over twenty locations around the country, and performs more than $782 million of problem-solving research annually for

government and industry.

8. Collectively, Defendants GTRC, GIT, and GTRI are referred to as "Georgia Tech."

9. Relator Christopher Craig is employed by Defendant GIT and currently serves as the Associate Director of Cyber Security at Georgia Tech. In this role, he manages all cyber security personnel through his direct reports, the Principal Engineer, the Operations Manager, and the Policy and Compliance Manager. In this position, Relator Craig has direct and firsthand information about the allegations contained herein.

10. Relator Kyle Koza graduated from GIT with a Bachelors in 2009 and a Masters in 2015 in Information Security. Since 2010, he has been employed by GIT, beginning his tenure as an Information Security Engineer in 2013. Relator Koza served as Georgia Tech's Principal Information Security Engineer from 2017 to June 2022. From this position, Relator Koza has direct and firsthand information about the allegations contained herein.

FACTUAL ALLEGATIONS

Background

11. Contractors like GTRC who are given access to certain information from the Department of Defense are required to provide "adequate security" for

covered defense information that is processed, stored, or transmitted on their internal information systems.

12. This obligation is found in the Defense Federal Acquisition Regulations (DFARS) 252.204-7012 ("Safeguarding Covered Defense Information and Cyber Incident Reporting").

13. Such covered information is known as Controlled Unclassified Information (CUI).

14. CUI is defined as information owned or created by the federal government that is sensitive but not classified, such as technical data, patents, or information relating to the manufacture or acquisition of goods and services.

15. "Adequate" security for protection of CUI is defined, at a minimum, as implementation of National Institute of Standards and Technology (NIST) Special Publication 800- 171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations" ("NIST 800-171").

16. DoD Contractors were first directed to be compliant with NIST 800-171 by December 31, 2017.

17. NIST 800-171 was first published in June 2015 and has received regular updates in line with evolving cybersecurity threats and emerging technologies. The latest revision was issued in February 2020.

18. NIST 800-171 has 110 security requirements, which are organized into fourteen groupings. These fourteen groupings are access control, awareness and training, audit and accountability, configuration management, identification and authentication, incident response, maintenance, media protection, personnel security, physical protection, risk assessment, security assessment, system and communications protection, and system and information integrity.

19. Each of these groups contain parts and subparts. For example, Requirement 3 is "Audit and Accountability," Control 3.9 is "Personnel Security," and Control 3.9.1 states the entity must "Screen individuals prior to authorizing access to information systems containing CUI."

20. There is no certification body or official audit procedure to determine whether a contractor is adhering to NIST 800-171 requirements.

21. DoD contractors instead must self-attest that they have conducted a points-based self-assessment. The organization gains one point for each implemented requirement but subtracts weighted penalty points for each unimplemented or partially implemented requirement. Final scores must be registered in the DoD's Supplier Performance Risk System (SPRS) and must be submitted before contract award or renewal.

22. Any NIST 800-171 requirements not met by a DoD contractor should be

stated within a Plan of Actions and Milestones (POA&M). The POA&M sets out key dates and timelines for achieving full compliance and must be submitted before the contract begins. The POA&M can be updated as the organization addresses areas of non-compliance and as their cybersecurity practices mature.

23. Defense contractors must also submit a System Security Plan (SSP) as part of their evidence of NIST 800-171 compliance. The SSP provides a comprehensive overview of an organization's IT network, including hardware and software, as well as security processes and policies. Both the SSP and any related NIST 800-171 POA&M are important evidence of compliance required by the DoD and are uploaded and updated in SPRS.

History of NIST implementation at Georgia Tech

24. Prior to the 2017 deadline, Georgia Tech rolled out a presentation entitled "CUI Program & DFARS 252.204-7012: How to Determine Whether the CUI Rule or 7012 Clause Applies to Your Contract."

25. On June 26, 2017, Georgia Tech Cyber Security acknowledged this requirement, sending a memo to "Campus Labs and Units Involved with Controlled Unclassified Information (CUI)" regarding "New federal security standards." The memo stated Cyber Security's intention to meet with individual labs and units to "ascertain your current level of compliance and identify any

compliance gaps." The Cyber Security would then "work with you to develop and implement a plan to comply with these security standards by the deadline."

26. The memo goes on to lay out the new standards, including citations to NIST and DFARS, and noting that these documents "mandate that all non-federal entities that receive CUI from the Department of Defense, directly or indirectly, as part of contracts or grants comply with these security standards by December 31, 2017."

27. On September 21, 2017, Georgia Tech received a copy (dated September 19, 2017) of the "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," over the signature of Shay D. Assad, Director, Defense Pricing/Defense Procurement and Acquisition Policy (the "NIST Memo"), which set forth guidance for acquisition personnel in implementing the NIST standards by the December 31, 2017 date.

28. To implement the NIST Memo, Georgia Tech established the Government Risk and Compliance (GRC) team within GIT's IT Department. The GRC team was tasked with working with system administrators to create an SSP, to conduct compliance assessments, and to create a Report on Compliance (ROC) for each lab. Through the ROC, the GRC team also attests to NIST compliance.

29. In theory, this team reported to Relator Craig, but in reality, the team lead

handled the process independently.

30. There are several problems with how NIST was implemented at Georgia Tech.

31. As a starting point, the assessors themselves were not qualified to determine whether a lab's practices actually complied with a given control. This, in and of itself, violates 800-171 3.2.2, which requires that the organization "[e]nsure that personnel are trained to carry out their assigned information security-related duties and responsibilities."

32. For example, in the Manos SSP (discussed below), the SSP listed FileVault (a MacOS disk encryption system) as an anti-malware control. However, as a properly trained auditor would know, FileVault does absolutely nothing to prevent the installation of malicious software and thus could not meet that control.

33. Compounding the problem, the untrained GRC team was under enormous pressure to find a way to interpret the NIST controls to allow whatever was already happening in each lab to be designated as "compliant."

34. This required the GRC team to be willing to allow the controls to mean different things in different labs, resulting in multiple interpretations—a practice with which Relator Craig openly disagreed, and which led to him being cut out

of the process as much as possible.

35. As one example of how far the untrained GRC team was willing to push the "interpretations" of controls, NIST requires that a system containing CUI will "Terminate (automatically) user sessions." This is commonly understood to mean that if there is no activity for a set time, the user's session will be terminated and further action on the system will require the user to log in again. On several SSPs for Georgia Tech labs, however, a policy allowing only manual termination of a user session has been permitted, because the parenthetical has been "interpreted" to mean that automating the process is optional. Needless to say, this interpretation renders the control meaningless.

36. Moreover, it is an openly acknowledged practice that while the GRC team should "do its best" to evaluate compliance, in situations where that is not possible, they would simply take the IT team's word for it.

37. In a properly functioning assessment, the GRC team should ask for a random sampling of evidence that the system is configured as stated. Here, however, the evidence was self-selected by the system administrator (instead of randomly sampled) and frequently was not sufficient to actually establish compliance.

38. For example, the Manos SSP (further discussed below) stated that as to

network anti-malware, "Observed all systems in-scope are behind Palo Alto NGFW at all times," but this was untrue. Relators expect that in that instance, GRC gathered evidence that showed the lab had an NGFW and that some systems were behind it. Many of the listed systems, however, were not behind a Palo Alto NGFW and of those that were, some had anti-malware turned off.

39. Even some people on the GRC team objected to this approach; at one point, a GRC team member insisted the Report on Compliance be modified so that rather than signing that a project was "compliant," he was merely stating that the things he had documented were "implemented."

40. GRC's ability to adequately assess and audit compliance was further handicapped by the fact that it was the perception of the business that GRC's job was to "make the system compliant." This was so even though, as auditors, GRC should have had responsibility to **find** the problems with the system, not **fix** them.

41. When the person or team charged with determining compliance is tasked with "fixing" the problems they identify, this creates an obvious conflict of interest. It is also in violation of NIST 800-171 3.1.4 Separation of duties, which includes, *inter alia*, ensuring that security personnel administering access control functions do not also administer audit functions.

42. The system administrators work for the Principal Investigators, not for campus IT. As such, their concern and loyalty is to the research projects, and their chief responsibility with respect to NIST is to make sure there is an attestation on file that will allow funding to be paid.

43. There are no consequences to the system administrators if they misrepresent (whether intentionally or accidentally) their compliance, even if they are caught—in such instances, complaints will then be directed at GRC or the people (like Relators) who catch the misrepresentation.

44. For example, the system administrator for the Manos labs, discussed below, was not even made aware that he had done something wrong by claiming to have installed Palo Altos when he actually did not. In fact, he blamed GRC for misleading him into thinking the labs were compliant—even though their finding of compliance was based on his own misrepresentations.

45. As a final failing of the system, GRC does not continue to monitor the environments for the entire time the contract was being performed.

46. This is arguably a violation of every single requirement in Section 3.3, Audit and Accountability, because all of the requirements in that section require access to system audit logs and records that allow for "monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity." It is

certainly not supportable under Control 3.4.4, which requires that the contractor "analyze the security impact of changes prior to implementation."

47. In summary, to minimize disruptions and placate researchers, the GRC team stretched the meaning of the controls to accommodate what it was told already existed in the labs. It then permitted system administrators assigned to each lab to state whether (a) what was allegedly in place was actually in place; and (b) whether any needed changes had actually been implemented, which further watered down the GRC's supervision. Finally, the GRC team failed to assess compliance past the point of creating the SSP, permitting changes to occur to the environment without assessing their impact on compliance.

48. Taken together, these flaws mean that when a problem was discovered by Relators, even if the stated actions had been taken by the lab (which was not always the case), the underlying interpretation of the control might be so faulty as to have been rendered meaningless.

GTRC'S SELF ATTESTATIONS OF NIST COMPLIANCE ARE FALSE

49. Thus, although GTRC provided self-attestations of compliance as requested by December 31, 2017, the process was flawed from the beginning. As early as July 2018, Relator Koza had begun to identify issues.

50. As noted above, these issues were rooted in the way that the GRC team

was restricted from completing its compliance function.

51. In November 2019, a project team was created to assess and correct two factor authentication for endpoint issues campus wide. As the Project Charter notes, two factor authentication is required by "several compliance requirements including but not limited to NIST 800-171".

52. The Project Scope was as follows:

> 1. Implement a solution that will satisfy NIST 800-171 obligations mandating two-factor authentication on client devices. This solution should also be minimally invasive to the end user and should be feasible to expand to other areas that may not have a compliance obligation should campus units choose to adopt it.
>
> 2. Ensured compliance of each endpoint device identified by the OIT Cyber Security Governance, Risk & Compliance Team.

53. This project began December 9, 2019—nearly two years *after* Georgia Tech had been certifying compliance with NIST 800-171.

54. In late 2021, due to the incident in the Astrolavos Lab that is described below, Relator Koza realized that the Astrolavos Lab had never been compliant with certain NIST requirements. He approached his boss, Relator Craig, and the two had several conversations about the creative interpretations and lack of monitoring going on across the board.

55. In the course of that same investigation of the Astrolavos Lab, for the first time, Relators saw billing be restarted before the security issues were resolved,

even after the issue had been noted as a "false claim."

56. After reporting the matter internally over the course of several months without satisfaction—and, in fact, with increasing retaliation—Relators sought legal advice to help secure the CUI they are charged with protecting.

A. In late 2021, Relators Discover the Astrolavos Lab Has Never Been Compliant With NIST.

57. Per its website, the Astrovalos Lab is "a computer security group at Georgia Institute of Technology. Our research aims to provide generalizable solutions to security problems with high operational impact. The group is made up of Ph.D. and postdoc researchers from the schools of Electrical and Computer Engineering (ECE) and Computer Science (CS), accompanied by a team of SysAdmins to build and maintain the infrastructure needed for the group's research."

58. The Astrolavos Lab is run by Professor Manos Antonakakis, and it is sometimes referred to as one of the "Manos labs" on the Georgia Tech campus.

59. In or about November 2021, Relator Koza was asked to open the Astrolavos lab's servers to the internet.

60. As Relator Kyle prepared to open the lab, he saw that it lacked the malware and incident detection software that was mandated campus wide, as required by, *inter alia*, NIST 800-171 3.14.6.

61. Accordingly, on November 11, 2021, he notified the system administrator via email that, before Koza could make the requested changes, the system administrator would first need to install "the required endpoint protection agents: Qualys Cloud Agent and Cortex XDR."

62. "Endpoint Agents" refer to programs to combat malware and detect incidents, for which the greater Tech campus uses FireEye Endpoint Security (pre-2021) and Cortex XDR (post-2021) to cover controls 3.6.1, 3.14.2, 3.14.3, 3.14.4 and 3.14.5. In addition, the campus-wide security plan requires the Qualys Cloud Agent to be installed, which partially covers controls 3.11.2 and 3.14.1.

63. The system administrator responded the next day that "Manos won't approve of having endpoint agents installed on our servers, we previously had a conversation with OIT policy team in creation of a lab-wide System Security Plan that exempted us from that requirement. I'd be happy to send over the most recent copy of it, if needed (we're supposed to renew the SSP every year, I'm just waiting on [GRC] to get back to me about it)."

64. After speaking with the GRC team, Relator Koza found that "Manos does not have a lab wide exemption for endpoint agents," a fact which he reported via email the same day to the system administrator. He added that "[t]his also most likely indicates that Manos' SSPs are not compliant. I cannot approve this

firewall rule at this time."

65. The system administrator responded within minutes that the lab needed to get the exemption because "[t]his will directly impact our ability to perform research." Later that afternoon, the system administrator sent over the lab wide SSP that had been in place, which explicitly noted that endpoint protection was not being used.

66. A few days later, on December 3, 2021, Relator Koza again reached out at the direction of Georgia Tech's relatively new Chief Information Security Officer (CISO). Relator Koza again instructed that "[t]o open this host to the Internet, we'll need Cortex XDR and Qualys Cloud installed on it," and offered to problem solve if there was some impact of which he was not aware of installing the necessary programs. The system administrator responded that:

> As I explained to [the CISO], Manos has told OIT in the past that he doesn't want endpoint agents installed on hosts (including this one). It's my understanding that we have a lab-wide SSP to cover this. If I'm missing something (like if we need to update the SSP, need some additional type of exception), please let me know. We've been waiting almost a month now to get this firewall exception pushed through, which is holding up research efforts.

67. After further discussion of the specifics of the problem between the system administrator and the CISO, Relator Koza ultimately responded on December 6 that he would be following up with the Office of Sponsored Programs (OSP) but

to his knowledge, "there isn't such a thing as a labwide exception and 800-171 requires malware protection."

68. Relator Koza then had an email exchange with Rebecca Caravati (Georgia Tech Interim Vice President for Research Administration; General Manager, Georgia Tech Research Corporation; General Manager, Georgia Tech Applied Research Corporation) about the noncompliance.

69. Ms. Caravati confirmed that Professor Antonakakis's DARPA contract required compliance with NIST 800-171 and that noncompliance would have to be assessed as a reportable event and invoices/charges might need to be suspended. She specifically stated that, "If he is not compliant, we will need to suspend effort on the project and not bill his sponsor for any activity until he is compliant as we are at risk for a false claim." She then set up a call to discuss.

70. Following that call, Relator Koza immediately reached out to "give [the system administrator] a heads up about the outcome" of the conversation with OSP. OSP had requested that "we officially notify them that the Astrolavos SSP is non-compliant with NIST 800-171 and they advised us that they are going to discontinue billing the project sponsor until a new SSP (compliant with 800-171) is written and reported compliant. OSP has notified Manos' management chain of these developments." In return, the system administrator expressed surprise

and requested help in getting the SSP "updated and compliant ASAP."

71. This response cued an internal discussion between the assigned GRC team member, the CISO, and both Relators, in which the CISO requested that everyone "hold on all activities around this one until you hear back from me." Relator Koza further explained his concerns about the lab's violations and the system administrator's proposed solutions, and the CISO urged that the issue be approached first by "addressing the two issues [Relator Craig] flagged so we can get the research restarted" and then by doing "a more in-depth review of our SSP/ROC development process and fix any gaps."

72. Also on December 6, 2021, Relator Craig complied with OSP's instructions to formally report the incident and later confirmed via email that conversation with Rebecca Caravati, Albert Concord (Director/Facility Security Officer, Research Security), and Dan Sibble (Contracting Officer, Department of Defense Awards for GTRI) (with a cc to Relator Koza, the GRC team member, and the CISO), in which he had explained that:

> during the course of looking into controls for a non-contract matter in Manos's Astrolavos lab, our security engineering team identified that at least two, and possibly more, controls in NIST 800-171 are not implemented within their lab. The controls are 3.14.2 (anti-malware at designated points) and 3.6.1 (incident response). We do not have any known security incidents within the lab, only noncompliance with requirements.

> The control listed for 3.14.2 is PaloAlto firewall malware detection which is not in place for some systems within the lab and likely does not meet the requirements because of how it is implemented elsewhere. In general we depended on FireEye HX and now PaloAlto XDR for both host-level anti-malware and detection, analysis, and containment of security incidents and this is not installed in the lab.
>
> I do not have evidence at this time that would indicate we have a reportable incident but I do recommend any steps that must be taken to re-evaluate the compliance of the lab before we assert to sponsors that their posture is compliant with NIST 800-171.

73. On December 7, the CISO emailed the team of Relator Koza, the system administrator, and the GRC representative (with a cc to Relator Craig), summarizing the steps to be taken to address the issues and restart research. The GRC team member responded with the upshot of his call with the GRC team, which addressed other potential issues with the SSP, but was quickly pulled back by the CISO, who instructed the team to "please hold off on the SSP steps until we've addressed the current issues and get them back to operational. If this goes as fast as I expect we have but a couple days to wait. Then I want to discuss the process for compliance before the do his new SSP." The GRC team member agreed.

74. On December 8, 2021, Relator Koza notified the CISO via email that there was a firewall issue with "some of the Astrolavos networks" that allowed grant access for external collaborators because the CISO had previously requested that

further communications with OSP go through him.

75. In the background of these discussions, however, the CISO was already putting pressure on Relators to stop further investigations of the SSP.

76. As evinced by an EthicsPoint report filed on December 9, 2021, Relator Koza was already complaining of "unethical requests from management," specifically the CISO. As Relator Koza stated:

> Upon identifying an issue with a security plan in a lab, I reported this concern to the contract officers in OSP, who immediately stopped billing on the contract.
>
> I was later admonished for doing so by our CISO as he "does not want to be in the business of stopping research." He revised the email admonishment, but it was also done verbally on the phone. The conversation afterwards switched to my imminent promotion and I suspect there was an implied relation between the two subjects.
>
> Currently, he has insisted clearly in writing that he does not want us to look further into issues with the SSP because as he stated on the phone "we would most likely have to shut down all research."
>
> I feel the ethical course of action would be to advise OSP that we've discovered issues with the SSPs required for contracts and let them make a determination if they should stop billing while we sort this out. Instead we have been told to not talk with OSP as he [the CISO] will be the one talking with them from now on. Instead, his stated intention is to tell OSP we have resolved the original issues we identified so that they can resume billing. Since we have since identified other issues that we have not reported to them, I believe this would become illegal if we were to resume billing.

77. A few days later, on December 10, Relator Koza added the following notes:

> [The CISO] has now informed me that he has told OSP that the issues identified were fixed, despite me and others clearly stating that only several very scoped issues were fixed but there still remains at least a few other unresolved compliance issues.
>
> Also, I want to ensure my use of witness is being understood correctly in this report. [The GRC team member] and [Relator Craig] are named as witnesses because they are also trying to help Georgia Tech do the ethical thing and have observed the same behavior that I have[.]

78. Following these reports, Relator Koza had a meeting with an investigator in December in which he provided the email and instant messenger screenshot evidence. After that meeting, Relator Koza continued updating the complaint; on January 31, 2022, Relator Koza added:

> Last week, in a staff meeting, after we once again expressed concern over the non-compliant state of DFARS labs, [the CISO] reaffirmed that we are not to report anything directly to OSP. He also stated that OSP should have never stopped billing for the Astrolavos incident. When we mentioned that the contract officers would know best about the requirements of the contract, he said that we "do not work for the DoD, you work for GT" and then went on to say how our primary job is to ensure that Georgia Tech can keep billing.
>
> In a separate meeting, earlier in the week, in reference to the [University System of Georgia] Endpoint Audit, I stated that I didn't think the new plan met the policy requirements and he stated that he "doesn't want the [University System of Georgia] to think they can tell us how to do security."

79. While Relator Craig was not present for the conversation referenced in Paragraph 76, he has been told the same thing by the CISO on at least two

occasions.

80. Relator Koza next updated the EthicsPoint site on February 28, 2022, writing that:

> Last week, due to a security incident, more non-compliance came to light. Despite asking multiple times for [the CISO] to inform OSP of the incident and request to discuss action, he ultimately decided not to report anything to OSP. In this case, once again, it turned out that the dfars [sic] covered lab had not been on a network that could have been compliant at the time of the SSP's creation (in use by other non-covered/non-compliant labs, no firewall) and then later moved hosts to a different network without updating inventory or the SSP.
>
> These are things that should not be possible for a compliant lab.

81. Finally, on April 27, 2022, Relator Koza added that:

> I just want to note that [Relator] Christopher Craig (my supervisor) had his performance review last week with [the CISO]. He was marked as "Needs Improvement" on things that were justified by [Relator Craig's] unwillingness to violate the DFARS contractual obligations I've mentioned previously. White this didn't affect me directly because I still report to Christopher, I feel it does justify my concerns that we will be penalized for not performing unethical actions. This will impact me directly as the reorganization that [the CISO] is doing has me reporting directly to [the CISO]. I expect I will also receive a negative performance review next year for the same reasons.
>
> I am also concerned that we're going on 5 months of this case. Based on the ethics materials sent out the other week, lying about the state of compliance for DFARS labs seems pretty cut and dry unethical[.]

82. As a result of these events and failure of the administration to address these concerns, in June 2022, Relator Koza was forced to resign his position.

83. At this time, Relator Craig continues in his position at Georgia Tech, although as the negative performance review demonstrates, he is already experiencing retaliation for his stand against these practices.

Specific examples of Non-compliance

84. At this time, based on their personal observations, Relators believe that all labs/projects that involve CUI have at least one issue with their SSP that render them noncompliant, and that most have many issues. The following are provided as examples of failures, but Relators know that there are many more.

85. At the outset, Relators note that there are many controls marked "Not applicable" in the Georgia Tech SSPs. All are problematic because controls are not to be marked "not applicable" without authorization from the Department of Defense to make a substitution of an equally effective measure.

86. Therefore, any plan with "Not Applicable" is out of compliance unless the lab can show a prior authorization and what "equally effective" security measure was used in its place.

87. 3.1.1 - Limit system access to authorized users, processes acting on behalf of authorized users, and devices (including other systems). ROC states, "Observed system access to servers managed by System IT. Confirmed only authorized staff have access to servers. Confirmed only PI and System IT can

access in-scope laptop."

88. In revising firewall rules for the network, Relators Craig and Koza have both observed multiple systems with inbound connections allowed from external corporations not listed on the SSP. In several cases, when asked specifically what individuals were using it and if they were authorized, the answer from System IT was, "we have an arrangement with [third party corporation] and anyone from there could be logging in." This was specifically raised with the CISO prior to his assertion that the SSP was compliant and was included in Relator Koza's report to Ethics/Internal Audit.

89. 3.1.2 - Limit system access to the types of transactions and functions that authorized users are permitted to execute. ROC states, "Observed system access to servers managed by System IT. Confirmed only authorized staff have access to servers. Confirmed only PI and System IT can access in- scope laptop." This is both untrue and non-responsive.

90. ROC also states, "Lab receives malware trace data from SpamHaus (external) and internal (IMPACT/GT) and the mechanism used by SpamHaus (and other unnamed partners) to upload trace data is unrestricted remote shell access which was found in multiple places throughout the lab."

91. 3.12.4 - 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. ROC states, "Confirmed SSP signed by PI and ROC completion by assessor signature," which is nonresponsive.

92. More than one hundred systems, located on over half a dozen networks, are listed on the SSP, but connection and relationships between those systems is not documented. Unlisted systems also exist on those networks and are managed by personnel not listed on the SSP, are not vetted for US Person status, and may not have had a background check.

93. The lack of an information system boundary is important because it means that even if a small subset of computer systems listed in the SSP actually contain information covered by the contract and those computer systems did meet 3.1.1 and 3.1.2, the contract is still noncompliant because there is no boundary between those systems and the rest of the systems on the SSP, and the SSP was specifically designed not to have a boundary so that information could flow within all listed systems.

94. 3.1.21 - Limit use of organization portable storage devices on external information systems**.** SSPs are completed with "Not applicable –No portable storage devices are in use on external information systems." Even if none of the

labs truly used any portable storage (which seems highly suspect), as discussed above, controls cannot be marked non applicable without prior DOD approval.

95. Additionally, mere non-use at this time does not satisfy the requirement. The questions in the assessment handbook (NIST HB 162) for 3.1.21 in particular contains, "Are restrictions imposed on authorized individuals regarding the use of company-controlled removable media on external systems?" The clear intent of the requirements to "limit" or "control" behavior is to have actual "limits" or "controls" placed on it, not to assert it is not currently being used, with no policy or technical control preventing future use.

96. 3.1.22 - Control CUI posted or processed on publicly accessible information systems. Like 3.1.21, this is marked "Not applicable" without DoD adjudication.

97. 3.5.3 - Use multifactor authentication for local and network access to privileged accounts and for network access to non-privileged accounts. The GRC SSP template states that the standard solutions for 3.5.3 are GT 2FA, LastPass, and Thycotic Secret Server. Of these solutions, only GT 2FA (Duo) are capable of protecting "local access for privileged account."

98. To utilize LastPass for local access to privileged accounts, the privileged user would need to check a password out of LastPass and have it automatically

changed after using it. This would also assume the LastPass account is set up to use two factor authentication. Thycotic Secret Server could be utilized the same way as LastPass, but unless the local password is set up for rotation in Secret Server, this would have the same issues as LastPass.

99. This was identified as a gap, and a project was recommended to investigate a central solution for local multi factor authentication, but it was not successful and ultimately dropped. To actually meet the local access part of this control, the local accounts would need to be set up to require two factor authentication using Duo. Relators do not believe that any departments (other than GTRI) use Duo for Windows or that any departments use Duo for Macs.

100. 3.13.1 - Monitor, control, and protect company communications (i.e., information transmitted or received by organization information systems) at the external boundaries and key internal boundaries of the information systems. At the time the SSP and ROC were signed for the Astrolavos lab, the majority of the systems listed on the inventory were on a network that did not have a firewall and was outside the Georgia Tech border firewalls. A firewall was added in 2021 as part of a long-delayed project. No controls with "Palo Alto NGFW" listed as the solution were accurate at the time of signing.

101. 3.13.6 - Deny network communications traffic by default and allow

network communications traffic by exception (i.e., deny all, permit by exception). For the Astrolavos lab, the firewalls that were in place, were not configured for default deny for outbound connections. Few networks on campus are configured in a deny outbound default configuration.

102. 3.14.2 - Provide protection from malicious code at designated locations within organizational systems. This was one of the issues reported to OSP. In the Astrolavos lab, no endpoint protection agents were configured and the firewall (listed as the control) did not have anti-malware protections turned on.

COUNT I
VIOLATIONS OF 31 U.S.C. § 3729–FEDERAL FCA
(All Defendants)

103. Relators hereby incorporate and reallege herein all other paragraphs as if fully set forth herein.

104. As set forth above, Defendant knowingly presented or caused to be presented false or fraudulent claims for payment or approval, in violation of 31 U.S.C. § 3729(a)(1)(A).

105. As set forth above, Defendants knowingly made, used, or caused to be made or used a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money or

property to the Government, in violation of the False Claims Act, 31 U.S.C. § 3729(a)(1)(G).

106. Due to Defendant's conduct, the United States Government has suffered substantial monetary damages and is entitled to recover treble damages and a civil penalty for each false claim, record, or statement. 31 U.S.C. § 3729.

107. Relators are entitled to reasonable attorneys' fees, costs, and expenses. 31 U.S.C. § 3730(d)(1).

COUNT II
VIOLATION OF 31 U.S.C. § 3730(h) – RETALIATION AGAINST RELATOR CRAIG
(Defendant Georgia Institute of Technology)

108. Relators hereby incorporate and reallege herein all other paragraphs as if fully set forth herein.

109. Defendant GIT violated Relator Craig's rights pursuant to 31 U.S.C. § 3730(h) by retaliating against him for lawful acts done by him in furtherance of an action under the federal FCA and other efforts to stop one or more violations alleged in this action, including, *inter alia*, increasingly scrutinizing his performance, pressuring him to violate the pertinent laws, rules, and regulations, and ultimately constructively terminating his employment.

110. As a result of Defendant's actions, Relator has suffered damages in an amount to be shown at trial.

111. Relators are entitled to reasonable attorneys' fees and costs, pursuant to 31 U.S.C. § 3730(h).

COUNT III
VIOLATION OF 31 U.S.C. § 3730(h) – RETALIATION AGAINST RELATOR KOZA
(Defendant Georgia Institute of Technology)

112. Relators hereby incorporate and reallege herein all other paragraphs as if fully set forth herein.

113. Defendant GIT violated Relator Koza's rights pursuant to 31 U.S.C. § 3730(h) by retaliating against him for lawful acts done by him in furtherance of an action under the federal FCA and other efforts to stop one or more violations alleged in this action, including, *inter alia*, increasingly scrutinizing his performance, pressuring him to violate the pertinent laws, rules, and regulations, and ultimately constructively terminating his employment.

114. As a result of Defendant's actions, Relator has suffered damages in an amount to be shown at trial.

115. Relators are entitled to reasonable attorneys' fees and costs, pursuant to 31 U.S.C. § 3730(h).

PRAYER FOR RELIEF

WHEREFORE, Relators pray for judgment against Defendant:

(a) awarding the United States treble damages sustained by it for each of the false claims;

(b) awarding the United States a maximum civil penalty for each of the false claims, records, and statements;

(c) awarding Relators the maximum relator's share from the proceeds of this action and any alternate remedy or the settlement of any such claim;

(d) awarding Relators all relief available, including special damages, resulting from retaliation pursuant to 31 U.S.C. § 3730(h);

(e) awarding Relators litigation costs and reasonable attorneys' fees; and

(f) granting such other relief as the Court may deem just and proper.

DEMAND FOR JURY TRIAL

Relators hereby respectfully demand trial by jury on all issues and counts triable as of right before a jury.

Respectfully submitted,

/s/ Julie Bracker
Julie Bracker
Georgia Bar No. 073803
Jason Marcus

Georgia Bar No. 949698
Bracker & Marcus LLC
3355 Lenox Rd., Suite 660
Atlanta, Georgia 30326
Telephone: (770) 988-5035
Facsimile: (678) 648-5544
Julie@fcacounsel.com
Jason@fcacounsel.com