IN THE UNITED STATES DISTRICT COURT
FOR THE EASTERN DISTRICT OF PENNSYLVANIA
PHILADELPHIA DIVISION

UNITED STATES OF AMERICA ex rel. MATTHEW DECKER,	)
Plaintiff-Relator,	) **FILED UNDER SEAL**
v.	) Case No. 2:22-cv-03895-PD
	) **JURY TRIAL DEMANDED**
PENNSYLVANIA STATE UNIVERSITY,	)
Defendant.	)

FIRST AMENDED COMPLAINT

1. Relator Matthew Decker brings this action on behalf of himself and the United States of America against Defendant Pennsylvania State University 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 Pennsylvania State University ("Penn State") is a Pennsylvania-based Non-Profit Corporation, with its principal place of business at 208 Old Main, University Park, PA 16802.

5. Relator Matthew Decker has served as the Chief Information Officer for Penn State's Applied Research Laboratory (ARL) since 2015, and as the Interim Vice Provost and CIO of Penn State itself in 2016.

FACTUAL ALLEGATIONS

Background

6. DFARS 252.204-7012 ("Safeguarding Covered Defense Information and Cyber Incident Reporting"), requires contractors like Penn State to provide "adequate security" for covered defense information that is processed, stored, created, or transmitted on its internal information systems.

7. Such covered information is known as Controlled Unclassified Information (CUI). CUI is information owned or created by the government that is sensitive, but not classified, such as technical data, patents, or information relating to the manufacture or acquisition of goods and services. Specific definitions and categories of CUI are published by government agencies.

8. "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").

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

10. Notably, under an interim rule that took effect in September 2020 and which is expected to be applied almost universally by late 2025, all defense contractors must carry out Basic Assessments of their compliance with NIST SP 800-171 and submit their scores to the Department of Defense ("DoD") as a condition of receiving a DoD contract.

NIST 800-171 Requirements

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

12. NIST 800-171 has 110 security requirements, which are organized into fourteen groupings, which are listed below.

13. **Access Control**: this family of twenty-two requirements is aimed at ensuring that only authorized users have access to networks, systems, and information, as well as controlling access to sections of information within the system that may have a higher level of sensitivity.

14. **Awareness and Training**: this family of three requirements is devoted to

educating system administrators and users about security risks and their roles in cyber security protocols.

15. **Audit and Accountability**: this grouping of nine requirements focuses on audit and analysis of system and event logs; recording and storing reliable audit records for reporting; and regular review of same.

16. **Configuration Management**: these nine requirements are devoted to the proper configuration of hardware, software, and devices; preventing unauthorized installations, and restricting non-essential programs.

17. **Identification and Authentication**: based on these eleven requirements, organizations must ensure that only authenticated users can access the network, including password/authentication procedures and policies; reliable user identification; and distinction between privileged and non-privileged accounts.

18. **Incident Response**: three requirements set forth the capabilities deemed necessary for an organization to respond to serious cybersecurity incidents, to ensure procedures are in place to detect, contain and recover after incidents as well as training, planning, and testing of these procedures.

19. **Maintenance**: best practice maintenance procedures, including regular maintenance and secure external maintenance, are the subject of these six requirements.

20. **Media Protection**: these nine requirements cover best practices for storage

or destruction of sensitive information and media in both physical and digital forms.

21. **Personnel Security**: the first of these two requirements deals with the need for security screening of individuals prior to accessing systems containing CUI. The second deals with protection of CUI during termination or transfer of personnel with such access, including return of devices, hardware, passes, etc.

22. **Physical Protection**: these six requirements are aimed at protecting physical access to CUI within the organization, including visitor access and restricting hardware access to authorized personnel.

23. **Risk Assessment**: Under these two requirements, organizations are required to scan systems regularly for vulnerabilities and keep devices and software updated. Regular risk assessments are also required.

24. **Security Assessment**: Development, monitoring, and renewing of system controls are the subject of these four requirements. Security procedures are to be regularly reviewed and updated to ensure that plans remain effective.

25. **System and Communications Protection**: Sixteen requirements in this grouping cover the monitoring and safeguarding of systems and transmission of information. Requirements include prevention of unauthorized information transfer and default denial of network communication traffic, as well as best practice cryptography practices to protect CUI.

26. **System and Information Integrity**: These seven requirements focus on monitoring and ongoing protection of systems within the organization, including processes for identifying unauthorized use and system security alerts.

27. Each of the groups identified in Paragraphs 13 through 26 contain parts and subparts, which are separated by a period. 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."

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

29. Instead, contractors must conduct a self-assessment and self-attest to compliance. This involves a points-based system of self-assessment against the 110 requirements outlined in the NIST 800-171, scoring compliance with each of the individual requirements.

30. Organizations gain a point for every implemented requirement, up to a maximum of 110, but subtract weighted penalty points (from -1 to -5) for each unimplemented or partially implemented requirement.

31. Final scores must be registered in the DoD's Supplier Performance Risk System (SPRS); scores must be submitted before contract award or renewal.

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

stated within a Plan of Actions and Milestones (POA&M).

33. The POA&M sets out key dates and timelines for achieving full compliance and must be submitted before the contract begins.

34. The POA&M can be updated as the organization addresses areas of non-compliance and as their cybersecurity practices mature.

35. Defense contractors must also submit a System Security Plan (SSP) as part of their evidence of NIST 800-171 compliance.

36. The SSP provides a comprehensive overview of an organization's IT network, including hardware and software, as well as security processes and policies.

37. Both the SSP and any related NIST 800-171 POA&M are important evidence of compliance that are required by the DoD and should be uploaded and updated in SPRS.

38. A proper implementation of NIST standards begins with an audit. In order to see the full breadth of the failures at Penn State, it is helpful to understand how the audit function ought to operate. For this purpose, it can be viewed as a series of steps, which are listed below.

39. **Step 1:** At the beginning of a NIST implementation, an auditor must first determine which NIST controls are met and which are deficient by evaluating the existing systems. To do so, the auditor starts by getting the scope and

architecture of the system from the system administrators (i.e., the person or group in IT who owns the system). This may take multiple iterations; under questioning from the auditor, the system administrators may realize that there are connections that had not previously been considered, because although the system administrators are IT-professionals, they are typically not trained in cybersecurity.

40. **Step 2:** The systems administrators explain to the auditor how each control is currently being implemented.

41. **Step 3:** The auditor verifies that the system is configured as the system administrators have represented.

42. In a typical audit, if a control is not met there would be a "finding" to address. However, since the goal of a NIST implementation audit is to achieve a fully compliant environment, the process continues.

43. **Step 4:** Corrective action: the system administrator or other IT personnel design a way to meet the control and then return to Step 1.

44. Even after the audit is completed successfully, NIST requires that the contractor continue to monitor the environments for the entire time the contract is being performed.

45. Failure to conduct ongoing monitoring is itself a violation of Section 3.3, Audit and Accountability; 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."

46. More specifically, Control 3.4.4 requires that the contractor "analyze the security impact of changes prior to implementation."

47. NIST HB 162 (the assessment handbook for NIST 800-171) provides five questions assessors should ask:

- Are changes that affect system security requirements tested prior to implementation?
- Is testing the effectiveness of the changes performed?
- Are only those changes that continue to meet compliance requirements approved and implemented?
- Are configuration changes tested, validated, and documented before installing them on the operational system?
- Has testing been ensured to not interfere with system operations?

48. These questions make it very clear that whatever control is used to meet 3.4.4 should prevent changes to the environment that bring the system out of compliance.

PENN STATE'S COMPLIANCE SELF ATTESTATIONS ARE FALSE

49. Although Penn State has provided self-attestations of compliance to DoD as required since December 31, 2017, these were false. In this section, we provide the background to Relator's involvement in the PSU cybersecurity efforts and explain his personal knowledge of this falsity.

50. In 2015, the Penn State campus experienced a significant cyber breach that included the College of Engineering and College of Liberal Arts.

51. In light of this breach and with the anticipated need for DFARS compliance, Relator was recruited to bring the IT and cybersecurity environment of the Applied Research Laboratory ("ARL") into control and compliance.

52. ARL is physically, logically, and operationally separated from the Penn State campus; accordingly, as the ARL CIO, Relator had no responsibility for bringing Penn State's research departments into compliance with DRARS.

53. Relator joined ARL on November 15, 2015 and by diligent work was able to achieve compliance for ARL by the target date of December 31, 2017. His efforts there included assessment of the situation, establishing the roadmap for compliance, building a team, establishing policies and processes, performing capability implementations and systems configuration.

54. Since January 1, 2018, ARL has been periodically inspected, audited, and questioned by sponsors—including its main sponsor, NAVSEA—as well as prime contractors, and the Inspector General, with satisfactory results.

55. In late 2015, Dr. Neil Sharkey approached Relator about providing help to Penn State research areas, so they could better understand upcoming compliance requirements.

56. Dr. Sharkey was concerned about how Penn State could get all of the

disparate research areas into compliance, how much it would cost, and how difficult the effort would be.

57. Relator provided a high-level overview of the upcoming compliance requirements, which was well-received.

58. In December 2015, Penn State Provost, Dr. Nick Jones, asked Relator to assume a concurrent role of Interim CIO and Vice Provost, Information Technology for Penn State. This appointment was in addition to his role CIO of ARL. Relator then began to split his time between ARL and Penn State.

59. At that time, Penn State IT consisted of approximately 84 separate IT organizations across twenty-four campuses that supported Administration, Academics, and Research.

60. At that time, Penn State had also recently appointed Dr. Andrew Sears, Dean of the College of Information Sciences and Technology, as interim Chief Information Security Officer (CISO). This meant that, like Relator, Dr. Sears also split his time – in his case, between his leadership role at the College and as Penn State CISO.

61. During his approximately eight months as interim CIO, Relator met several times with Penn State constituents, including Research, to discuss compliance requirements. As part of those conversations, he suggested Penn State begin assessing environments, especially within the College of Engineering,

which housed the most projects requiring DFARS compliance outside of ARL.

62. Beginning January 11, 2016, Relator attended Monthly Compliance Meetings regarding Penn State's DFARS / NIST 800-171 compliance with Dean Sears. These monthly compliance meetings continued until Dr. Don Welch was named CISO for Penn State, at which time they stopped.

63. On January 15, 2016, Relator introduced the College of Engineering to "Cavirin," a Governance, Risk and Compliance software package, to establish a baseline and assist with gap assessment.

64. On January 16, 2016, Relator held a meeting to discuss DFARS / NIST compliance requirements for the Penn State WorkDay implementation.

65. On February 26, 2016, there was an additional meeting with Dr. Sears to discuss Penn State compliance with DFARS / NIST 800-171.

66. On September 1, 2016, Relator's time as interim CIO concluded, and he returned full time to ARL.

67. Relator was then limited within Penn State to executive stakeholder roles for the PSU WorkDay implementation and the Enterprise Resource Planning (ERP) implementation. To the best of Relator's knowledge at that time, those projects took DFARS/NIST compliance seriously and ensured appropriate investments and configurations of the solutions would meet DFARS requirements.

68. Relator recently discovered, however, that Penn State disregarded some of his suggestions concerning NIST compliance in the ERP implementation, which may have left more CUI exposed.

69. In July 2019, Dr. Don Welch became the Interim CIO/VP for Penn State and named Richard Sparrow as Interim CISO.

70. Mr. Sparrow established a CISO advisory group and invited Relator's participation. Within this setting, as well as one-on-one conversations with Mr. Sparrow, Relator continued to inform Penn State of the changing compliance requirements, including the upcoming DFARS 252.204-7019.

71. It did not appear to Relator that the requirements for 7012 had ever been fully understood, and now 7019 was further complicating the situation.

72. Around this time, Relator discovered that Penn State's registration within SPRS for a specific project showed missing records for SPRS entries.

73. Relator asked Mr. Sparrow about this issue.

74. As Relator later discovered, under Mr. Sparrow's direction, OIS personnel simply uploaded template documents to "solve" the missing records problem.

75. The risk assessment scores, artifacts, and incomplete records entered into SPRS were knowingly false and were added merely to "check the box" so that there would be no "missing" records.

76. In early 2020, Relator suggested to Mr. Sparrow that a Penn State CUI

"Center of Excellence" be established so that stakeholders and experts could better understand the requirements, gaps, and capabilities within the campuses, and advise Penn State Research. Mr. Sparrow again stated that he believed that Penn State was sufficiently compliant.

77. In October 2020, PSU announced the conclusion of their Box contract. Box is a FedRAMP certified solution, which is a requirement of DFARS 252.204-7012. However, Penn State instead decided to migrate its remaining Box data to Microsoft Office 365 (M365) OneDrive.

78. However, Penn State uses the commercial version of M365, which is not certified for CUI. Accordingly, any CUI in the Box data was migrated to a non-compliant platform.

79. In January 2021, Relator was invited by CISO Welch to be a part of the Research IT ("RIT") Constituency Group. For the rest of the year, within this forum, Relator continued to press for priority and to offer assistance on DFARS compliance, but here was no interest in forming a working group to address the matter.

80. Relator specifically asked the RIT group chair if he understood Relator's concerns and whether he wanted to establish a more focused effort, but the RIT group chair did not have any interest and believed that compliance had been satisfied.

81. In February 2022, Dr. Karen Thole and Dr. Puneet Singla began to raise concerns regarding NASA contracts that contained DFARS requirements and expectations of CUI protection.

82. Dr. Thole is an advisor to ARL and had heard Relator discuss the compliance requirements often, and she began to question Penn State's actual state of compliance, asking questions about compliance readiness.

83. In response, Penn State's new Interim CISO, Keith Brautigam, took the position that Penn State Policy AD95 was based upon the NIST 800-171 standards, and therefore PSU was compliant wherever OIS had issued an Authority to Operate (ATO) based off of AD95.

84. However, AD95 does not satisfy NIST 800-171, because as described, it does not address CUI nor does it address the entire control family of 800-171.

85. In fact, AD95 is not actually based on NIST SP 800-171 as Brautigam was apparently told.

86. In June 2022, Relator had a conversation with Kyle Crain regarding compliance, which revealed that Penn State was working on their first Systems Security Plan (SSP).

87. This was very alarming because every environment supporting a contract containing the DFARS 252.204-7012 and now 7019 clause is required to have—and should already have had—an SSP. Without an SSP, there is no way to

truthfully attest compliance, nor can the required risk assessment be performed.

88. Yet as Relator investigated further, it became clear that actual SSPs within these research environments did not exist.

89. Relator took his growing list of concerns to Mr. Brautigam, who himself appeared to be beginning to be troubled by the apparent gaps in Penn State's policies and processes for DFARS compliance.

90. In a RIT meeting on April 12, 2022, Mr. Brautigam introduced these concerns, but as usual, there was no interest from the group in further understanding or resolving the issues.

91. In late March, Dr. Thole, who knew enough about AD95's differences with NIST from prior conversations with Relator to be uncomfortable with the CISO's answer, reached out to the Senior Vice President of Research, Dr. Lora Weiss.

92. As a result, on April 1, 2022, Dr. Weiss requested to meet with ARL's Senior Executive Director and Relator (ARL's CIO) to discuss Dr. Thole's concerns.

93. As a result of that meeting, Dr. Weiss asked Relator to lead a tiger team to evaluate Penn State's DFARS compliance and report back to her. Kyle Crain in OIS was named co-lead of the effort.

94. This first tiger team consisted of:

- Kyle Crain, Office of Information Security (OIS)
- Matthew Decker, Applied Research Laboratory (ARL)

- Wayne Figurelle, Institute for Computational and Data Science (ICDS)
- Michelle Gluck, Office of General Counsel (OGC)
- Dr. John Hanold, Office of Sponsored Programs (OSP)
- Tami Hemingway, Export Compliance
- Kristen McNitt, Office of Sponsored Programs (OSP)
- Clinton Schmidt, Research Security
- Jim Taylor, Research IT

95. In June 2022, the first tiger team finished gathering contract information and compliance artifacts. In going through this process, Relator determined that Penn State had never reached actual DFARS compliance and thus had been falsely attesting to compliance since January 1, 2018.

96. Specifically, Relator confirmed his belief that Penn State had never reached DFARS compliance in any of the investigated projects, that the "ATO" process was based on PSU Policy AD95, and that AD95 was not truly aligned to the NIST 800-171 framework.

97. Relator and Mr. Crain were both concerned that sharing this information, even within the tiger team, could be disruptive. Accordingly, the report was emailed only to Dr. Weiss on June 6, 2022.

98. The next day, on June 7, 2022, Mr. Crain and Relator met with Dr. Weiss to discuss the report and findings. Relator had prepared a PowerPoint summary with findings and recommendations.

99. To the surprise of Relator and Mr. Crain, instead of considering the limited distribution of the report to be a courtesy to her, Weiss suggested that the pair

did not have the full concurrence of the team.

100. Prior to the June 7 meeting, Dr. Weiss had scheduled for Relator to discuss the effort with the University Research Committee on June 9, 2022, but during the June 7 meeting she instructed Relator to only share the concept of what the tiger team was investigating and the fact of the investigation, not the results.

101. On June 24, 2022, Relator was asked by a member of the Research group, who was aware of the Penn State compliance struggles, to meet with now Interim Provost, Dr. Justin Schwartz, to discuss the situation.

102. Relator informed Dr. Weiss about the request, who instructed him not to meet with the Provost because, *inter alia*, he did not have the full team's concurrence. Relator informed her at that time that there was concurrence within the group and from the CISO.

103. Relator also provided the report to the others, including the CISO (Keith Brautigam), the Director for the Office of Sponsored Programs (Dr. John Hanold), and the Associate CIO for Research IT (Jim Taylor).

104. In general, the reaction was one of surprise that Penn State was not in compliance, because the group had been told that the ATOs were adequate to demonstrate DFARS compliance.

105. Also on July 13, 2022, Dr. Weiss also finally acknowledged reading the report by sending back a heavily edited version that she felt would be more

appropriate for distribution.

106. Relator responded unequivocally that "PSU is not compliant today and has not been DFARS compliant since it became mandatory per clause in January, 2018."

107. Dr. Weiss then asked if "anyone has put a freeze to work on those contracts for which we are not compliant?"

108. Despite her articulated concerns, no work was stopped.

109. After reviewing her edits, Relator declined to make Dr. Weiss's requested changes, explaining that the report was the tiger team's notice to her and to the CIO of the gravity of Penn State's situation. He suggested that if she wanted to have a record that could be more widely distributed, it would need to be produced by someone else.

110. The next day, by telephone, Dr. Weiss apologized for asking Relator to change the report and then asked if he was willing to lead a second tiger team to investigate further and determine if Penn State actually was in violation on any specific contracts. She provided a list of active projects that Relator instructed the team to investigate.

111. The same day (July 14, 2022), Kyle Crain requested a "driveway discussion" at Relator's house. Mr. Crain expressed concerns that he might lose his job over the non-compliance issues and that previously, Penn State had only

worked to "look" compliant. He mentioned that the new CISO, Keith Brautigam, was also fearful for his job.

112. Using a list of projects provided by Dr. Weiss on July 18, 2022, Relator initiated the second tiger team on August 2, 2022. He prepared a template to profile and assess each contract as to DFARS applicability, indications of compliance or gaps, and recommendations for action.

113. The team struggled to find the pertinent data.

114. Relator discovered that all twenty records submitted to the SPRS system had been falsified.

115. When he asked Mr. Crain, who had submitted the records, whether he was correct that the records were inaccurate, Mr. Crain confirmed.

116. No SSPs had been produced; rather than specific systems or research compute space owners, the records referred only generically to colleges or institutes; no proper, DFARS 7020 risk assessment had been performed; and the risk assessments that had been uploaded were merely templates in order to "check the box," as instructed by Rich Sparrow.

117. Given that no SSPs exist, Relator assumes that the scores submitted were either made up or based on some internal security policy.

118. Upon further investigation, Relator also uncovered work tickets in which CUI-involved research had been configured with "secure enclaves" within M365.

119. As noted above, M365 at Penn State is commercial grade and not approved for CUI, and the effort to create secure enclaves within this version of Microsoft Office demonstrates that there is a lack of comprehensive understanding of the DFARS requirements.

120. About ten days after the second tiger team started, on August 12, 2022, Relator explained to the tiger team that he was concerned about falsified records being submitted to the government. Following that meeting, Relator notified the director of OSP of this concern as well.

121. On August 15, 2022, Dr. Weiss requested another phone call with Relator to ask that Jim Taylor (Associate CIO of Research for IT who was complicit in much of the existing problems) be added to the second tiger team, where he effectively replaced Relator as team lead.

122. In summary, Penn State has, at best, inconsistently sprinkled in some small levels of cyber security best practices, but these half measures are not systemic.

123. Given that the organization can neither identify where CUI is nor where it should be, nor validate existing CUI, there is no chance that comprehensive protection or compliance can be truthfully attested.

124. Given that it took Relator two years to move ARL into compliance and maintain compliance readiness, it seems there is virtually no chance that Penn State could respond effectively and quickly enough to maintain the contract if a

sponsor should investigate the false attestations.

125. Dr. Weiss has since denied access to the first tiger team report to the new Chief Ethics and Compliance lead, Tabitha Oman.

126. At this time, the second tiger team has stalled out, but has positively identified active CUI-involved projects that have attested compliance. The second tiger team cannot positively locate the systems on which the CUI exists or what (or where) the CUI is.

127. Penn State has no SSPs.

128. Penn State's SPRS entries are falsified.

129. There are dozens of projects where Penn State has attested compliance but never met it.

130. To this day Penn State does not appear to be working toward compliance.

131. Relator is concerned that due to all of the aforementioned issues, sensitive government research and national security information is at the very least at risk.

COUNT I
VIOLATIONS OF 31 U.S.C. § 3729–FEDERAL FCA

132. Relator hereby incorporate and reallege herein all other paragraphs as if fully set forth herein.

133. 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).

134. As set forth above, Defendant 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).

135. 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.

136. Relator is entitled to reasonable attorneys' fees, costs, and expenses. 31 U.S.C. § 3730(d)(1).

PRAYER FOR RELIEF

WHEREFORE, Relator prays 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 Relator the maximum relator's share from the proceeds of this action and any alternate remedy or the settlement of any such claim;

(d) awarding Relator litigation costs and reasonable attorneys' fees; and

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

DEMAND FOR JURY TRIAL

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

Respectfully submitted,

/s/ Darth M. Newman
Darth M. Newman
Pennsylvania Bar No. 209448
Law Offices of Darth M. Newman
1140 Thorn Run Rd # 601
Coraopolis, PA 15108
Telephone: 412-436-3443
darth@dnewmanlaw.com

Julie Bracker (applying for *pro hac vice*)
Georgia Bar No. 073803
Bracker & Marcus LLC
3355 Lenox Rd., Suite 660
Atlanta, Georgia 30326
Telephone: (770) 988-5035
Facsimile: (678) 648-5544
Julie@fcacounsel.com