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,<br><br>Plaintiff–Relators,<br><br>v.<br><br>GEORGIA TECH RESEARCH CORP. and BOARD OF REGENTS OF THE UNIVERSITY SYSTEM OF GEORGIA (d/b/a THE GEORGIA INSTITUTE OF TECHNOLOGY),<br><br>Defendants. | ) | Civil Action No. 1:22-cv-02698-JPB |

**DEFENDANTS' BRIEF IN SUPPORT OF THEIR MOTION TO DISMISS**

# TABLE OF CONTENTS

# TABLE OF AUTHORITIES

Page(s)

## CASES

**STATUTES**



**RULES**



**REGULATIONS**

**OTHER AUTHORITIES**

## INTRODUCTION

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"), move to dismiss the government's Complaint-in-Intervention ("Complaint") under Rule 12(b)(6) for failure to state a claim and under Rule 9(b) for failure to plead the claims with particularity.

The government alleges that employees of a state university defrauded the Department of Defense ("DoD") by not following novel cybersecurity rules purportedly incorporated in two DoD contracts when performing research on campus. Based on a false legal premise, the government attempts to assert claims under the False Claims Act ("FCA") against the university's non-profit contracting arm and tort claims against both the university and the non-profit. But its allegations fail to state a claim because the Complaint artfully omits the governing DoD documents that gut its claims, ignores contractual provisions that defeat its theories, relies on the wrong versions of regulations, and otherwise mangles the applicable law. The government's own inability to untangle this complex and evolving contractual and regulatory scheme demonstrates why the government cannot plead its claims at all, much less under the heightened Rule 9(b) pleading standard applicable here.

The government's allegations all rest on the premise that GTRC falsely represented that a Georgia Tech lab, when performing research under two DoD contracts, was compliant with cybersecurity regulations that apply to contractor computer systems that process specific types of government information. But the contracts, by their express terms and *as confirmed in writing* by DoD, were for "fundamental research"—academic research that, by definition, is not subject to those regulations. The government's FCA claims must be dismissed because they are premised on purported failures to comply with regulations that *do not apply at all* to university systems used to carry out fundamental research.

The government also fails to state a claim under its FCA theories because it confuses which cybersecurity rules applied at which times. The Complaint's chief contentions about the computer system in Georgia Tech's on-campus Astrolavos Lab—that it did not timely have a "System Security Plan" or run antivirus software—rely on versions of the cybersecurity rules that were released *after* the relevant contract was solicited, awarded, and executed, and therefore, were not applicable. The government cannot manufacture claims by ignoring express terms in the DoD contract to retroactively apply more stringent requirements that never applied to the research at issue.

Even if the Georgia Tech lab had operated a system to which DoD's (later version of its) cybersecurity rules applied, the government fails to allege an FCA

claim because the Complaint never plausibly alleges that GTRC promised—let alone *falsely* promised—that it would follow those future rules or that it ever certified that it complied with them. The government does not (and could not) allege that DoD awarded the relevant contracts because of a false cybersecurity promise, nor that GTRC ever said that it complied with DoD's rules when seeking payment.

The FCA claims also fail under both the plausibility and particularity standards because the government has not alleged that strict cybersecurity compliance was material to DoD's decision to pay GTRC. The government does not contest the excellence of the research that led DoD to repeatedly award work to the lab. Nor does it allege that DoD ever—even once—inquired about the lab's cybersecurity compliance when awarding it contracts or paying its claims. And it never grapples with the fact that DoD knew of alleged noncompliance with these rules for years and continued to make payments. Instead, the government unsuccessfully tries to fill these obvious gaps with presidential proclamations and other generic expressions of the importance of cybersecurity. But such general appeals do not satisfy the government's obligation to plead materiality with particularity—that in *this case*, under *these solicitations*, DoD would not have awarded *these contracts* or paid *these invoices* had it known of the status of *these specific cybersecurity controls.*

Finally, the government's common-law claims, which seek to haul Georgia Tech (in addition to GRTC) into this action with the same deficient set of allegations

as the FCA claims, also fail because they rest on the same flawed premise as the FCA claims against GTRC—i.e., that the Astrolavos Lab was subject to DoD cybersecurity requirements for the contracts at issue. In addition to that threshold defect, the Complaint also fails to plead facts essential to these common-law theories of liability—i.e., that the entities made misrepresentations that DoD relied upon, that GTRC breached any contractual provisions, or that DoD suffered an economic injury. Accordingly, the Complaint should be dismissed in full.

## BACKGROUND

### A. DoD's Ever-Evolving Cybersecurity Rules

Over the past decade, DoD has imposed an evolving set of cybersecurity requirements on contractor information systems *if* those systems handle a defined category of information called covered defense information ("CDI"). 48 C.F.R. §252.204-7012 ("DFARS 7012"). When the requirements apply, contractors must implement a lengthy set of cybersecurity controls, which has varied over time based on the version incorporated in the applicable contract. Since late 2020, a bidding contractor—in certain, specified cases—must also provide DoD a self-assessment of its implementation of those controls.

#### 1. Cybersecurity Rules Apply Only to Systems with CDI

DoD's cybersecurity regime applies to contractor systems that handle CDI. Systems used to perform "fundamental research," which by definition does not involve CDI, are not subject to the regime. DoD regulations and guidance dictate

how one determines whether information qualifies as CDI, how that information must be marked, and who has authority to make these determinations. Given the complexity of these rules, DoD's adherence to its own procedures is essential for contractors to ensure their own compliance.

**CDI.** CDI is unclassified information that DoD has determined should be subject to limits on distribution. It includes two categories of information: Controlled Technical Information ("CTI"), *see* DFARS 7012(a), and Controlled Unclassified Information ("CUI"), *see* 32 C.F.R. §2002.4. CDI can either be provided by DoD to a contractor or created by a contractor during contract performance. DFARS 7012(a).

An overlapping set of DoD documents define the process for identifying and marking CDI, CTI, and CUI. Only the DoD entity overseeing the contract can designate CDI, and only in accordance with DoD regulation.[1] To ensure that a contractor knows how to identify and handle CDI, DoD regulations mandate that DoD officials inform contractors "in the contract, task order, or delivery order" what CDI might be implicated when performing the contract and explain how contractors

[1] *See* Ex. 1, DFARS PGI 204.7303-1(b)(1)-(2) (rev. Nov. 18, 2015); *see also* Ex. 2, FAQs regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73 (hereafter "DFARS FAQs") Q23, bit.ly/3NyOJVG.

should "mark[]" that CDI to indicate how it can be distributed to third parties. Ex. 1, DFARS PGI 204.7303-1(b)(1)-(2) (rev. Nov. 18, 2015).

Contractors may be required to mark information with "distribution statements" that may govern how certain information can be distributed and to whom. Distribution statements may, but do not necessarily, indicate that information is CDI. Information marked as Distribution Statement "A" is not subject to distribution limits and may be shared freely, and therefore cannot contain CDI. Ex. 3, DoD Instruction ("DoDI") 5230.24 at 14-15 (Apr. 28, 2016). Distribution Statements "B" through "F," when properly applied, impose controls that potentially indicate that the information is CDI. *Id.* at §4.2(b)-(f). DoD prohibits Distribution Statement "F"—the most restrict statement—from being applied to research performed on university campuses because of the importance of freely distributing such research. *See* Ex. 4, DoDI 3200.12 §§2(a)(2), 3(a)(5) (Aug. 22, 2013).[2]

[2] According to the DoD instruction governing distribution statements, DoDI 5230.24, Distribution Statement F "will not be used on … documents governed by the DoD Scientific and Technical Information Program described in [DoDI 3200.12]," Ex. 3, DoDI 5230.24 at 19 (Apr. 28, 2016), which applies to "[s]cience and technology programs consisting of basic research [and] applied research … which are identified as budget activities (BA) 1 [and] 2," Ex. 4, DoDI 3200.12 §2(a)(2) (Aug. 22, 2013). GTRC's on-campus research at issue in this case was BA 2 (which was previously defined as budget category 6.2). *See* Ex. 5, DARPA Statement (academic performers "are funded with 6.2 funds"); Ex. 6, DoD, Memo. re Contracted Fundamental Research at 2 (June 26, 2008) ("'budget category 6.2' [was] replaced by … Budget Activity … 2.").

The Complaint appears to allege that certain information was CDI because it was marked "For Official Use Only" ("FOUO"), *e.g.*, Compl. ¶118, a legacy term that DoD used before the CDI framework. However, an FOUO marking "alone does not indicate that [the document] is [CDI]." Ex. 2, DFARS FAQ Q25. To the contrary, "[m]ost FOUO information does not meet" the definition of CDI. *Id.*

**Fundamental Research.** Fundamental research is "basic and applied research in science and engineering, the results of which ordinarily are published and shared broadly within the scientific community." Ex. 7, National Security Decision Directive 189, *National Policy on the Transfer of Scientific, Technical and Engineering Information* (Sept. 21, 1985). According to NSDD-189, which has been adopted by DoD, the "products of fundamental research [are to] remain unrestricted" "to the maximum extent possible." *Id.* Thus, as DoD has reiterated, fundamental research "by definition cannot involve any [CDI]." 48 C.F.R. §252.204-7000(a)(3).

### 2. Contractor Systems that Handle CDI Must Comply with Evolving DoD Cybersecurity Requirements

Information systems that handle CDI were required, beginning in 2018, to implement a suite of cybersecurity controls identified by the National Institute of Standards and Technology ("NIST"). *See* DFARS 7012(b)(2). As of December 2020, contractors bidding for work that requires them to handle CDI on their systems must also assess and report to DoD the status of the implementation of those controls. *See* 48 C.F.R. §252.204-7019 ("DFARS 7019").

The trigger for whether these cybersecurity requirements apply to an information system is whether that system handles CDI under the relevant contract. Thus, even though DoD requires that components include the cybersecurity clauses in every contract, *see* 48 C.F.R. §204.7304, the clauses operate only when the relevant information system handles CDI. *See* DFARS 7012(a)-(b) (regulation applies to "covered contractor information systems," which are systems that "process[], store[], or transmit[] [CDI]"); *see also* DFARS 7019(a) (regulation applies to "covered contractor information systems" as defined in DFARS 7012).

**Cybersecurity Controls for CDI (DFARS 7012).** As of 2018, contractor information systems that handle CDI are required to implement the catalog of security requirements set out in NIST Special Publication 800-171, titled "Protecting [CUI] in Nonfederal Systems and Organizations" ("NIST SP 800-171"). DFARS 7012(b)(2)(i). NIST SP 800-171, now in its fourth version, currently identifies 110 cybersecurity controls to be implemented on contractor systems. Ex. 8, NIST SP 800-171 Rev. 3, §3 (2024). Contractors must implement the version of NIST SP 800-171 "in effect at the time the [contract] solicitation is issued or as authorized by the Contracting Officer." DFARS 7012(b)(2)(i).

Each version of NIST SP 800-171 has imposed different requirements on contractors. As relevant here, the initial version, which was in effect through December 2016, identified 109 security requirements to be implemented. Ex. 9,

NIST SP 800-171, ch. 3 (2015). It did not require creation of a system security plan ("SSP"). *See id.* And although the initial version identified several controls related to malicious code protection, *see* Sec. Reqs. 3.14.2, 3.14.4, and 3.14.5, that version never required or even recommended the installation of antivirus software, *see id.*

In December 2016, NIST published Revision 1 to NIST SP 800-171, which introduced the SSP requirement (resulting in 110 total controls). Ex. 10, NIST SP 800-171 Rev. 1 (2016). And in February 2020, NIST published Revision 2, which added "discussion" sections to "provid[e] additional information to facilitate the implementation and assessment" of the controls. Ex. 11, NIST SP 800-171 Rev. 2 at 8 (2020). For the controls related to malicious code, the discussions added, for the first time, "anti-virus signature definitions and reputation-based technologies"—i.e., antivirus software—as a recommended solution, *see* Sec. Reqs. 3.14.1, 3.14.2, 3.14.4, 3.14.5, but did not mandate its use, *see, e.g.*, *id.* 3.14.2 ("malicious code protection mechanisms *include* anti-virus signature definitions" (emphasis added)).

The substantive requirements of DFARS 7012 have a companion clause, 48 C.F.R. §252.204-7008 ("DFARS 7008"), that can be inserted in DoD contract *solicitations* to alert proposed bidders that the contract may require compliance with DFARS 7012. DFARS 7008(c)(1); 48 C.F.R. §204.7304. When included in a solicitation, DFARS 7008 provides that proposals in response to the solicitation will

be understood as a representation to implement DFARS 7012, if it applies.[3]

**Assessment of Compliance with NIST SP 800-171 (DFARS 7019).**

Effective as of December 2020, DFARS 7019 requires that bidding contractors self-assess their system's compliance with NIST SP 800-171's 110 controls and post the resulting score in DoD's Supplier Performance Risk System ("SPRS"). Such assessments are necessary only for information systems "required to implement NIST SP 800-171"—i.e., systems that handle CDI. DFARS 7019(b); DFARS 7012(a)-(b). DoD has deemed these assessments "[l]ow" confidence because they are "self-generated." Ex. 13, NIST SP 800-171 Assessment Methodology, Version 1.2.1 at 4 (June 24, 2020). And although DoD contracting officers are supposed to verify the existence of a SPRS score before awarding a contract, no minimum score is required. *See* 48 C.F.R. §204.7303(b). When included in a solicitation, DFARS 7019 provides that proposals in response to the solicitation will be understood as a representation to have a SPRS score less than three years old. DFARS 7019(b).[4]

---

[3] The Complaint also alleges that GTRC violated FAR 52.204-21, which concerns a different category of information—federal contract information ("FCI"). "Fundamental research … is not, by definition, FCI." Ex. 12, 88 Fed. Reg. 89058, 89068. Given that the Astrolavos Lab performed only fundamental research under the contracts, the lab's research had no FCI and was not subject to FAR 52.204-21.

[4] The government's claim that GTRC violated 48 C.F.R. §204.7302, which indicates it is DoD "policy" for contractors to implement DFARS 7012 and 7019, is duplicative of the government's claim that GTRC violated those underlying DFARS provisions and thus fails for the same reasons as those claims.

## B. Factual Background

These facts are drawn from the allegations in the Complaint and documents attached to this Motion, which, as set forth more fully in the accompanying Motion for Judicial Notice, can be considered in ruling on this Motion under the Court's authority to either judicially notice governmental records, F.R.E. 201, or to consider documents under the doctrine of incorporation by reference that are "central to the plaintiff's claims" and "undisputed," *Johnson v. City of Atlanta*, 107 F.4th 1292, 1300 (11th Cir. 2024). When such documents "contradict the general and conclusory allegations of the pleading, the exhibits govern." *Griffin Indus., Inc. v. Irvin*, 496 F.3d 1189, 1206 (11th Cir. 2007).

### 1. GTRC Entered into DoD Contracts to Perform Fundamental Research

Georgia Tech is a leading public research university. Compl. ¶25. The Astrolavos Lab is a group of faculty and students on Georgia Tech's campus that performs cybersecurity research. *See id.* ¶12. Defendant GTRC is the non-profit contracting arm for Georgia Tech's on-campus research. *Id.* ¶¶26-29. Non-party Georgia Tech Research Institute ("GTRI") is the applied research arm of Georgia Tech that maintains separate operations and often conducts classified research.

The Complaint identifies two contracts under which DoD paid GTRC for research to be conducted on campus in the Astrolavos Lab. *Id.* ¶¶97-101. The November 2016 contract, Enhanced Attribution ("EA"), was part of a Defense

Advanced Research Projects Agency ("DARPA") effort to create methods for revealing malicious cyber actors using unclassified information. Ex. 14, EA Statement of Work ("EA SOW") at 3-4. DARPA oversaw the project while the Air Force Research Lab ("AFRL") handled contracting duties. *See* Ex. 15, EA Contract. The October 2022 contract, "Signature Management using Operational Knowledge and Environments" ("SMOKE"), was part of a DARPA program to investigate methods for tracing cyber threats. Compl. ¶¶122-23; Ex. 16, SMOKE Contract.

**The EA Contract Was for Fundamental Research.** GTRC and AFRL executed the EA contract on November 17, 2016. Compl. ¶102. The contract provided for multiple performers—GTRC (in the Astrolavos Lab), University of North Carolina, University of Georgia Research Foundation, *see* Ex. 14, EA SOW at 12, and GTRI, *see* Ex. 17, EA Subcontracting Plan at 1. DFARS 7012 (which was scheduled to become effective a year later) was among the dozens of FAR and DFARS provisions included in the contract. *See* Ex. 15, EA Contract.

The EA contract was awarded in response to an April 2016 DARPA solicitation, which, as relevant here, never provided that contractors would handle, or be required to handle, CDI. Ex. 18, EA Solicitation at 38. The EA solicitation *did not include* a DFARS 7008 clause, under which any proposal submitted by a contractor would have constituted a representation to implement (if applicable) DFARS 7012. The first mention of DFARS 7008 came *after* GTRC submitted its

proposal and *after* DoD had selected GTRC as an award winner, when the clause was inserted into the award letter. *See* Ex. 19, EA Award Notice at 2.

The EA contract included several documents describing information associated with the research—a security classification guide ("SCG"), a DD Form 254, and a contract data requirements list ("CDRL"). *None of the contract documents identified any CDI that would be involved in the Astrolavos Lab's research*, as would be required if CDI were involved. *See* Ex. 1, DFARS PGI 204.7303-1(b)(1)-(2) (rev. Nov. 18, 2015). The SCG identified no CDI related to GTRC's performance of the contract and instead listed three categories of information as "FOUO." Ex. 20, EA SCG at 6-7. The DD Form 254 likewise indicated only that the contractor would "require access to" FOUO information. Ex. 21, EA DD 254 at 1. *Nor did the contract documents instruct GTRC how to mark any purported CDI*, which also would be required if CDI were involved. *See* Ex. 1, DFARS PGI 204.7303-1(b)(2) (rev. Nov. 18, 2015). Contrary to the government's allegations, Compl. ¶113, the CDRL identified as "TBD" the distribution statements applicable to all work product delivered under the contract, and DoD never updated the CDRL during the life of the contract to provide GTRC any further instruction. Ex. 22, EA CDRL. For one such "TBD" item, the associated "remarks" box noted "Distribution Statement F," but explained—in text the Complaint omits—that the "distribution statement is

preliminary only [and that the] final distribution statement shall be determined by the government during the review process." *Id.* at 14.

Moreover, in written statements that were exchanged between the parties contemporaneously with the contract's execution (but which are omitted from the Complaint), *both DARPA and AFRL separately confirmed that the Astrolavos Lab's EA work was fundamental research* not subject to any distribution controls. Specifically, on November 16, 2016, the day before GTRC signed the EA contract, the principal researcher for the Astrolavos Lab emailed DARPA to request confirmation that "the unclassified work [Georgia Tech] is planning to do is not subject of a pre pub[lication] rule" controlling distribution of its research findings. Ex. 5, DARPA Statement. In response to the inquiry, DARPA confirmed that "**all subs under GTRC (Georgia Tech (Not GTRI), UNC, UGA) are considered fundamental research**." *Id.* (emphasis added). Two days later, on November 18, 2016, a GTRC contracting officer emailed a contract specialist for AFRL, requesting "clarification to the contract DD 254 making it clear that [the Astrolavos Lab's] part of the work effort is fundamental research and excluded from publication restrictions" (a type of distribution control). Ex. 23, AFRL Statement. AFRL responded, after consulting with DARPA, that "a revised DD 254 is not necessary" because as "[**f]undamental [r]esearch**," the Astrolavos Lab's work was already exempted from any "prepublication review requirements." *Id.* Accordingly, both

DARPA and AFRL informed GTRC and Georgia Tech in writing in November 2016, contemporaneously to GTRC's signing of the contract, that the work of the Astrolavos Lab was fundamental research, which by definition does not include CDI and thus is not covered by DoD's cybersecurity rules.

**The SMOKE Contract Was for Fundamental Research.** SMOKE was executed on October 5, 2022, after GTRC won an award under a December 2021 DARPA solicitation. The solicitation incorporated DFARS clauses 7008 and 7012, but explicitly noted that "[f]or awards where the work is considered fundamental research, the contractor will not have to implement [DFARS 7008 and 7012]." Ex. 24, SMOKE Solicitation at 29. In connection with its proposal, GTRC represented that it would implement DFARS 7019 to the extent that provision was operative. *See* Compl. ¶125. DFARS 7012 was among the more than one hundred FAR and DFARS provisions incorporated in the contract. *See* Ex. 16, SMOKE Contract.

The SMOKE contract contemplated multiple performers across two contract line-item numbers ("CLINs"): CLIN 0001 and CLIN 0002. *Id.* at 2. The contract made clear that GTRC's research would be fundamental research, and that one subcontracted performer would perform non-fundamental research. As the contract explicitly detailed, **"DARPA expects the work performed by the Georgia Tech Research Corporation and it[s] subcontractor, the University of Georgia, under this contract to be fundamental research and it is, therefore, not subject to**

**publication restrictions."** Ex. 25, SMOKE Contract Attachment 1A at 5 (emphasis added). Consistent with this designation, the contract provided that GTRC's "reports and other deliverables" would be marked as "Distribution Statement A," meaning that they would be "[a]pproved for public release." *Id.* at 1.

In November 2022, GTRC and DARPA modified the contract to "add[] [a] Non-Fundamental Research CLIN 0003" and to "incorporate" a Form DD 254 and "Non-Fundamental Research FAR and DFARS clauses." Ex. 26, SMOKE Modification at 1. The modification made clear (in a provision the Complaint omits) that any non-fundamental research would be performed "**on Government facilities and/or GTRI facilities**"—not in the Astrolavos Lab at Georgia Tech. Ex. 27, SMOKE Modification Attachment 1A at 1 (emphasis added). It also provided that the non-fundamental research would not begin until 36 months after the contract award (i.e., October 2025), *id.*, and would be allocated just $20,000 in funding (out of a total contract value of over $22 million), Ex. 26, SMOKE Modification at 3.

The modification reaffirmed (in other provisions the Complaint omits) that the original CLINs were "[f]undamental [r]esearch," *id.* at 2, and repeated the contract's determination that "**DARPA expects the work performed by the Georgia Tech Research Corporation and it[s] subcontractor, the University of Georgia, under this contract to be fundamental research and it is, therefore, not subject to publication restrictions**," Ex. 27, SMOKE Modification Attachment 1A at 6

(emphasis added). The DD Form 254 accompanying the modification provided that the "contractor" would require access to CUI and receive, store, or generate CUI, Ex. 28, SMOKE Modification DD 254 at 2, which the modification clarified applied to "Non-Fundamental Research CLINs" (i.e., CLIN 0003), while for the "other CLINs," persons should "follow the procedures in … [the] Public Release or Dissemination of Information [section]," Ex. 26, SMOKE Modification at 3, which stated that GTRC's research was fundamental research not subject to distribution restrictions, Ex. 27, SMOKE Modification Attachment 1A at 5-6.

### 2. Astrolavos Lab Performed Fundamental Research under the DoD Contracts and GTRC Requested Payment for this Work

Following contract execution, the Astrolavos Lab "perform[ed] work" under the contracts, as contemplated. *See* Compl. ¶¶121, 133. The EA research was completed by August 2021. *See id.* ¶¶285-86. SMOKE's research began in October 2022 and is ongoing. *See id.* ¶¶122, 289. The Complaint does not contest the excellence of the research performed in any way. *See generally id.*

For both contracts, GTRC submitted invoices on Standard Form 1034, which indicated the "date of delivery of service," total "amount" sought, and, on an attachment, amounts sought for various cost elements, including "Salaries and Wages," and "Materials and Supplies." Ex. 29, EA Invoice; Ex. 30, SMOKE Invoice. The EA invoices 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." Ex. 29, EA Invoice. The SMOKE invoices included that certification or a comparable one: "I certify the amounts herein claimed are in accordance with the application and award documents and have not been previously claimed." Ex. 30, SMOKE Invoice; Compl. ¶288. The invoices do not mention cybersecurity rules nor certify compliance with them.

### 3. The Relators' and Government's Complaints Allege Purported Violations but No Harm

Relators are, respectively, a current and a former Georgia Tech employee in Georgia Tech's IT department. Neither had any role in the Astrolavos Lab nor any idea whether the at-issue contracts involved CDI or were for fundamental research. The relators filed a qui tam complaint on July 8, 2022. *See* Dkt. 1. Twenty months later, following its investigation, the government intervened. *See* Dkt. 17.

The Complaint alleges that, with respect to the EA and SMOKE contracts, GTRC (but not Georgia Tech) violated DFARS 7012 by not satisfying the SSP or malicious code requirements of an unspecified version of NIST SP 800-171. The Complaint further alleges, with respect to SMOKE, that GTRC and Georgia Tech violated DFARS 7019 by submitting an allegedly false SPRS score several years before the SMOKE proposal (though the Complaint pleads no facts purporting to show that Georgia Tech submitted a SPRS score). The government does not allege that any information related to the contracts was compromised by any purported failure to comply with the cyber requirements. And similarly, the government does

not allege that GTRC's invoices were inaccurate, apart from its (flawed) theory that GTRC supposedly failed to disclose its purported noncompliance with the cybersecurity regulations on the invoices.

The Complaint asserts FCA claims against GTRC alone for presenting a false claim in violation of 31 U.S.C. §3729(a)(1)(A) and for creating a false statement or record in violation of 31 U.S.C. §3729(a)(1)(B), as well as common law claims against GTRC and Georgia Tech for fraud, negligent misrepresentation, unjust enrichment, payment by mistake, and (as to GTRC alone) breach of contract.

## LEGAL STANDARD

"[O]nly a complaint that states a plausible claim for relief survives a motion to dismiss." *Ashcroft v. Iqbal*, 556 U.S. 662, 679 (2009). A claim is not plausible if the plaintiff's factual allegations—stripped of bald assertions, bare legal conclusions, and other conclusory statements—do not support a "reasonable inference that the defendant is liable for the misconduct alleged." *Id.* at 678. In addition, because the Complaint either asserts fraud directly or sounds in fraud, the government must satisfy the heightened pleading standard of Rule 9(b) for all claims. *See U.S. ex rel. Atkins v. McInteer*, 470 F.3d 1350, 1357 (11th Cir. 2006); *Robinson v. Adtalem Global Educ., Inc.*, 2019 U.S. Dist. LEXIS 242263, at *13-15 (N.D. Ga. 2019).

Under that standard, a plaintiff must plead "facts as to time, place, and substance of the defendant's alleged fraud." *Atkins*, 470 F.3d at 1357.[5]

## ARGUMENT

### I. THE COMPLAINT DOES NOT PLEAD VIABLE FCA CLAIMS

Despite its length and its irrelevant, unjustified attacks on Georgia Tech's employees, the Complaint is most notable for its lack of particularized facts showing a regulatory violation, false promises to comply with the regulations, false certifications of compliance, or any indication that compliance was material to DoD.[6]

#### A. The Government's FCA Presentment Claim Against GTRC Fails As A Matter Of Law (Count I)

In Count I, the government asserts that GTRC violated 31 U.S.C. §3729(a)(1)(A) by (1) submitting invoices that falsely certified compliance with DoD cybersecurity regulations and (2) fraudulently inducing DoD to award GTRC the EA and SMOKE contracts. To state a "presentment" claim under that subsection, the government must allege facts to show, with particularity, that the defendant made a claim that was (a) false (b) with scienter (c) that was material. *U.S. ex rel. Bibby v.*

---

[5] Defendants believe all issues can be decided now on this motion to dismiss. However, if the Court concludes that any issue in this motion should be converted to a motion for summary judgment, Defendants respectfully request that the Court defer ruling on that issue so that the parties can more fully develop the record in discovery.

[6] Defendants also preserve the argument that the qui tam provisions of the FCA—under which this case was filed—are unconstitutional, as set forth in *U.S. ex rel. Zafirov v. Fla. Med. Assocs., LLC*, 2024 WL 4349242 (M.D. Fla. 2024). In the event that holding is affirmed by the Eleventh Circuit during the pendency of this litigation, Defendants reserve their right to seek appropriate relief in this case.

*Mortg. Invs. Corp. ("MIC")*, 987 F.3d 1340, 1346-47 (11th Cir. 2021). In this context, to plead falsity, the government must first allege a "regulatory violation," *U.S. ex rel. Willard v. Humana Health Plan of Texas Inc.*, 336 F.3d 375, 383 (5th Cir. 2003); *Carrel v. AIDS Healthcare Found., Inc.*, 898 F.3d 1267, 1272-75 (11th Cir. 2018), and either GTRC's false certification of compliance with that regulation (legal falsity) or a false promise to comply with the regulation that caused DoD to enter a contract (fraudulent inducement). In other words, the government must allege both that GTRC broke the law and lied to DoD about it.

**1. The Complaint Does Not Plead Violations of the DoD Cybersecurity Requirements**

The Complaint fails to plead falsity for two overarching reasons: First, it does not (and cannot) allege a regulatory violation because DoD's cybersecurity rules did not apply to the systems used to perform fundamental research in the Astrolavos Lab. Second, as discussed *infra* §I(A)(2), the Complaint does not (and cannot) plausibly allege that GTRC either falsely certified compliance with the DoD rules or fraudulently induced DoD to award the contracts based on false promises to comply.

With respect to a regulatory violation, the Complaint assumes—but does not plead facts to plausibly establish—that DoD's cybersecurity requirements applied to the systems performing research under the EA and SMOKE contracts. To guard that assumption, the Complaint intentionally omits the governing contractual provisions and undisputedly authentic DoD documents fatal to its case. And even if

(counterfactually) those requirements did apply, the Complaint does not plead facts showing they were violated because it either relies on the wrong versions of those requirements or invokes standards that are too ambiguous to support FCA liability.

*a. The Astrolavos Lab's fundamental research was not subject to DFARS 7012 or 7019*

**DoD Confirmed that EA Was for Fundamental Research.** The government does not properly allege that the EA contract was subject to DoD cybersecurity regulations. The contract unambiguously shows that no CDI was contemplated for EA, because it does not "identif[y]" *any* CDI related to the contract, as DoD regulations require. Ex. 1, PGI 204.7303-1(b)(1) (rev. Nov. 18, 2015). Moreover, contemporaneously with the contract's execution, both DARPA and AFRL confirmed in writing that Georgia Tech's work was "fundamental research" not subject to distribution controls. *See* Ex. 5, DARPA Statement; Ex. 23, AFRL Statement. These DoD statements conclusively demonstrate that DoD did not identify any CDI that the Astrolavos Lab was required to safeguard under the contract; to the contrary, DoD instructed the lab that there were no restrictions on publishing its EA research. The government's entire case rides on a legal conclusion—that the cybersecurity regulations applied to the lab—that deserves no deference on a motion to dismiss. *Kwok v. Delta Air Lines Inc.*, 994 F. Supp. 2d 1290, 1295 (N.D. Ga. 2014). The governing legal documents demonstrate that, because DoD identified no CDI, the government's foundational legal conclusion is wrong.

The government attempts to infer the existence of CDI based on misleading snippets from documents and alleged statements of Georgia Tech personnel.[7] For example, the Complaint cites the April 2016 EA solicitation that would-be contractors would need to protect "DARPA CUI," Compl. ¶¶106-07, but that language was neither included nor referenced in the EA contract that was signed by the parties. *See* Ex. 15, EA Contract. Similarly, the Complaint's assertion that the CDRL applied Distribution Statement "F" to one contract deliverable mischaracterizes that document, which said that the applicable distribution statement was "TBD." *See* Ex. 22, EA CDRL at 14. Nor does the Complaint allege—as it could not—that the CDRL or any other contract document was ever amended to provide that Distribution Statement F applied, and for good reason: Distribution Statement "F" cannot be applied to on-campus research. *See supra* n.2. The Complaint's suggestion that CDI was present because the DD Form 254 and SCG identify "FOUO" is incorrect, because DoD's own directive states that "[i]nformation that is identified as [FOUO] alone does not indicate that it is covered defense

[7] The misleading nature of the government's selective soundbites is illustrated by its colorful accusation that Georgia Tech researchers are treated like "star quarterbacks." Compl. ¶¶11, 189. These words, which the Complaint suggests came from a Georgia Tech IT employee, *id.* ¶189, never came out of the employee's mouth. They were spoken *to* the employee during a deposition by government counsel, who then parroted his own words in the Complaint to attack Georgia Tech.

information," Ex. 2, DFARS FAQ Q25, and therefore cannot trigger the DoD cybersecurity requirements.

The handful of alleged statements from the Astrolavos Lab staff about whether they handled CUI are likewise irrelevant, *see* Compl. ¶¶137-38, 140, 142-47, because the staff's "subjective interpretation of [GTRC's] contractual duties" cannot create FCA liability, *U.S. ex rel. Wilson v. Kellogg Brown & Root, Inc.*, 525 F.3d 370, 377 (4th Cir. 2008); those interpretations conflict with the EA contract; and of course Georgia Tech's staff could not designate information as CDI, an authority held only by DoD. *See* Ex. 1, DFARS PGI 204.7303-1(b)(1)-(2) (rev. Nov. 18, 2015). And the allegation that some unnamed DARPA employee at some unspecified time in some oral conversation "effectively ask[ed]" the principal researcher to mark some presentations as Distribution Statement "F"—which DoD is prohibited from applying to on-campus research—cannot suffice in the absence of pleading specific facts about a single contract document from DoD identifying CDI. *See* Compl. ¶139.

**Contract Documents Show SMOKE Was for Fundamental Research.** Contract documents incorporated into the Complaint demonstrate that the Astrolavos Lab performed only fundamental research on the SMOKE contract. The contract and its modification were crystal clear: "DARPA expects the work performed by [GTRC] … under this contract to be fundamental research." Ex. 25, SMOKE Contract Attachment 1A at 5; Ex. 27, SMOKE Modification Attachment 1A at 6.

In an effort to plead around reality, the Complaint ignores that both the contract and its modification included this dispositive language, *see* Compl. ¶¶128-32, and disregards the express language that any non-fundamental research would be performed only "on Government facilities and/or GTRI facilities"—i.e., not on GTRC systems, Ex. 27, SMOKE Modification Attachment 1A at 1. Even more, the Complaint ignores the contractual terms dictating that any non-fundamental research would not begin until October 2025, *id.*, and that the fundamental research CLINs—GTRC's research—were not subject to the DD Form 254 or any prepublication restrictions, *id.* The government's cherry-picking violates the basic principle that a contract "should be read to give effect to all its provisions and to render them consistent with each other." *Davis v. Valsamis, Inc.*, 752 F. App'x 688, 692 (11th Cir. 2018). Reading the whole thing—not just the excerpts in the Complaint—clearly provides that GTRC contracted to perform only fundamental research. Moreover, for the reasons just discussed, the existence of CDI cannot be inferred from the speculation of lab staff, who (for obvious reasons) had no authority to decide what is CDI. *See* Compl. ¶¶148-50.

*b. The Complaint does not allege with particularity violations of the cybersecurity regulations*

Even if DoD's cybersecurity regulations could apply to the Astrolavos Lab systems, the Complaint does not plead particularized facts showing violations of the SSP or malicious-code requirements. The government repeatedly and incorrectly

tries to hold GTRC responsible for failing to comply with the wrong version of the NIST controls: those that went into effect *after* the parties executed the contracts.

**EA Was Not Subject to Cybersecurity Requirements.** The Complaint's confused assertions that GTRC violated NIST SP 800-171 by not creating an SSP or installing antivirus software fail because *those requirements were not in NIST SP 800-171 when the EA contract was solicited, awarded, and executed*. Under DFARS 7012, only "the security requirements in [NIST SP 800-171]" "in effect at the time the solicitation is issued" should be implemented. DFARS 7012(b)(2)(i). The EA contract was subject to the first version of NIST SP 800-171, the one in effect when DoD solicited EA in April 2016. Ex. 18, EA Solicitation. The SSP requirement at issue was not added until Revision 1, which was published in December 2016—after the contract was executed. *See* Ex. 10, NIST SP 800-171 Rev. 1, Sec. Req. 3.12.4. Indeed, the initial publication *expressly rejected* inclusion of an SSP requirement. *See* Ex. 9, NIST SP 800-171 (2015), App. E Tbl. E-12 (noting SSP requirement in a different NIST publication but excluding it from NIST SP 800-171).[8] The confusion of Georgia Tech employees about which rules applied, *see, e.g.*, Compl. ¶159, cannot *create* obligations that do not exist in the contract.

[8] The government asserts, in a single conclusory paragraph, that the lack of an SSP means GTRC violated two other NIST requirements related to implementation of the NIST security requirements and plans of action to address deficiencies. *See* Compl. ¶158. But the Complaint fails to state a claim because it pleads no facts showing why the lack of an SSP violated these other requirements.

Similarly, the allegation that Georgia Tech failed to install antivirus software on certain computers does not establish a regulatory violation because the recommendation to install that software did not appear in NIST SP 800-171 until December 2020 (in the "discussion" section), more than four years after the EA solicitation. The 2020 references are the government's *only* support for its assertion that the Astrolavos Lab was required to install antivirus software in connection with the EA contract. *See id.* ¶87 ("The discussions to NIST Controls 3.14.2, 3.14.4, and 3.14.5 specifically refer to antivirus software…"); *see also id.* ¶88 (similar); *id.* ¶89 (similar). Moreover, the government never alleges that the protections that the lab did have in place, *see id.* ¶188, fell short of the malicious code requirements included in the operative version of NIST SP 800-171.[9]

**The Rules for SMOKE Either Did Not Apply or Were Too Vague.** The Complaint's SMOKE allegations fail on their own terms. The Complaint cannot plead that the Astrolavos Lab failed to implement antivirus software because, as it concedes, the lab "install[ed] … antivirus software" in December 2021, *id.* ¶¶192-93, almost a year before execution of the SMOKE contract, *id.* ¶127.

[9] The government's claim under FAR 52.204-21 fails for the same reason: because the FAR clause also imposes the vague malicious code protections from the initial version of NIST SP 800-171. *See* Ex. 9, NIST SP 800-171 (2015), Sec. Reqs. 3.14.2, 3.14.4, 3.14.5; FAR 52.204-21(b)(1)(xiii)-(xv).

Other alleged SMOKE violations rely on "imprecise statements or differences in interpretation" that the FCA does not punish. *U.S. ex rel. Lamers v. City of Green Bay*, 168 F.3d 1013, 1018 (7th Cir. 1999). The Complaint asserts liability based on an alleged failure to "periodically" update the lab's SSP, Compl. ¶¶165-67, but NIST previously confirmed that there is no "minimum" frequency required, Ex. 2, DFARS FAQ Q87, and, as part of an effort to "remove ambiguity," NIST deleted that language from the latest version of NIST SP 800-171. Ex. 8, NIST SP 800-171 Rev. 3, Sec. Req. 3.12.4; Ex. 31, FAQs for NIST SP 800-171r3 at 1, bit.ly/4hdZAlE. And contrary to the Complaint's suggestion, Compl. ¶¶165-67, Georgia Tech's internal policy cannot create binding obligations regarding the frequency of SSP updates. *See, e.g.*, *Hagood v. Sonoma Cnty. Water Agency*, 81 F.3d 1465, 1477 (9th Cir. 1996) (action that was inconsistent with entity's policy was not false under FCA).

Similarly, the Complaint's assertion that the Astrolavos Lab inaccurately scoped its SSP, Compl. ¶161, ignores that NIST SP 800-171 allows entities to "limit the scope of the security requirements" to those "specific system components" handling CUI. Ex. 11, NIST SP 800-171 Rev. 2 at 2 (2020). That two Georgia Tech employees allegedly disagreed with the plan's scope does not amount to a regulatory or FCA violation. Compl. ¶¶162-63; *see Wilson*, 525 F.3d at 377.

In sum, the government cannot allege that GTRC violated the DoD cybersecurity requirements. Contract language and undisputedly authentic DoD

documents show that the Astrolavos Lab performed fundamental research, which does not involve CDI and is not subject to DoD cybersecurity requirements. And even if the requirements did apply, the Complaint's allegations still fail because the government seeks to hold GTRC liable for requirements that were either enacted after the at-issue contracts or are too imprecise to support FCA liability.

### 2. The Complaint Does Not Allege False Certifications of Compliance or False Promises to Comply

The Complaint also fails to plead falsity because it does not allege particular facts showing that GTRC expressly or impliedly certified its compliance with DoD cybersecurity requirements. Nor does it plead facts that GTRC fraudulently induced DoD to award it contracts based on false promises to comply with those requirements. These omissions are fatal.

#### *a. The Complaint fails to plead that any certification related to the EA or SMOKE contracts was false*

To plead legal falsity, the government must allege with particularity a false certification of compliance with a statute or regulation, which can be either express or implied. *See Universal Health Servs., Inc. v. U.S. ex rel. Escobar*, 579 U.S. 176, 187 (2016). An express certification requires explicit certification of compliance with a law or regulation "in connection with a claim submitted" for payment. *U.S. ex rel. Keeler v. Eisai, Inc.*, 568 F. App'x 783, 798-99 (11th Cir. 2014). An implied false certification requires (1) a claim that "makes specific representations about the

goods or services provided" but (2) "fail[s] to disclose noncompliance with material statutory, regulatory, or contractual requirements [that] makes those representations misleading half-truths." *Escobar*, 579 U.S. at 190.[10]

The government does not allege—nor could it—that GTRC expressly certified compliance with DFARS 7012 or DFARS 7019 in connection with claims for payment. GTRC's invoices certified only the appropriateness of "payments" or "amounts," which speak to "the propriety of fiscal data" and not compliance with dozens of fine-print terms concerning regulatory compliance. *Barko*, 241 F. Supp. 3d at 58-59; *see also U.S. ex rel. Jackson v. Ventavia Rsch. Grp., LLC*, 667 F. Supp. 3d 332, 354 (E.D. Tex. 2023) (certification of "amounts invoiced … for costs incurred in accordance with the agreement" related to pricing, not compliance with terms). The "general sweeping language" of GTRC's certifications is far too imprecise to support an express claim. *McLain v. KBR, Inc.*, 2014 WL 3101818, at *5 (E.D. Va. 2014).

The government's implied certification theory also fails. Contrary to the Complaint's conclusions, Compl. ¶¶284, 288, GTRC's invoices never made "specific representations about the goods or services provided." *Escobar*, 579 U.S. at 190.

[10] The government does not appear to assert a factual falsity claim, which in any event would fail because the Complaint does not plead that the description of goods and services in GTRC's invoices was false, as would be required for factual falsity. *U.S. ex rel. Barko v. Halliburton Co.*, 241 F. Supp. 3d 37, 58-59 (D.D.C. 2017).

Instead, just like the invoices in *U.S. ex rel. Kelly v. Serco, Inc.*, 846 F.3d 325, 332 (9th Cir. 2017), which were held legally insufficient to support implied certification, GTRC's invoices "provided the period of performance, total costs incurred during that period," and "list[ed] the dollar amounts for [GTRC's] costs for labor, travel, [subcontracts], and materials." And GTRC's certifications cannot be read to "identify any 'specific representation' that," by not mentioning cybersecurity compliance, "rendered a given claim a 'misleading half-truth by the omission of material facts.'" *United States v. Walgreen Co.*, 417 F. Supp. 3d 1068, 1086-87 (N.D. Ill. 2019). Thus, the government cannot allege an implied certification claim.

*b. The Complaint fails to plead that GTRC fraudulently induced DoD to enter into contracts*

To plead fraudulent inducement, the Complaint must allege particular facts showing that GTRC (1) made a knowingly false statement that (2) was the but-for cause of DoD's decision to award the contract. *U.S. ex rel. Cimino v. IBM*, 3 F.4th 412, 418-20 (D.C. Cir. 2021); *U.S. ex rel. Marsteller v. Tilton*, 556 F. Supp. 3d 1291, 1302 (N.D. Ala. 2021). The Complaint fails to plead that GTRC fraudulently induced DoD to enter the contracts through promises to comply with DFARS 7012 (EA and SMOKE) or through a false SPRS score (SMOKE).

**DoD Was Not Fraudulently Induced into Awarding the EA Contract.**

GTRC never promised to comply with DFARS 7012 when seeking the EA award. The government never suggests that GTRC did so expressly. Instead, it alleges that

GTRC so promised by operation of DFARS 7008, which (when included in a solicitation) provides that "by submi[tting] … [an] offer, the Offeror represents that it will implement" NIST SP 800-171. DFARS 7008(c)(1). But *DoD did not include DFARS 7008 in the EA solicitation*, so GTRC made no representation by submitting a proposal in response. *See* Ex. 18, EA Solicitation. DoD did not insert DFARS 7008 until *after* GTRC was awarded the contract, Ex. 19, EA Award Notice at 2, and thus could not have been fraudulently induced into entering the contract by that alleged promise. These facts are nearly identical to *Wilson*, where the Fourth Circuit held, in dismissing a fraudulent inducement claim, that "it would be dubious at best" that a DoD form the contractor signed after it began performance could have "influenced the [DoD's] decision to initially award" the contract. 525 F.3d at 378.

Moreover, even if the Complaint adequately alleged a promise to comply with DFARS 7012, the claim would still fail because it does not plead causation. The government pleads no facts showing that DoD was induced to "award[] the contract" by GTRC's alleged representations about compliance. *Marsteller*, 556 F. Supp. 3d at 1302. It is wholly implausible that DoD would not have awarded GTRC a contract to perform fundamental research, but for GTRC's representation that it would comply with rules not applicable to that type of research. It is therefore unsurprising that the Complaint pleads *no facts* alleging that DoD considered compliance with DFARS 7012 in awarding the EA contract, much less alleges *who* considered it, *when*

they did so, and *how* that influenced DoD's decision to contract. *Cf. Cimino*, 3 F.4th at 419 (the government must allege facts showing that "fraud in fact caused the government to enter into a contract"). DoD's belated invocation of DFARS 7008 cannot fill that gap given that the clause appeared in the award letter sent *after* DoD's decision to "enter into [the] contract." *Marsteller*, 556 F. Supp. 3d at 1302.

**DoD Was Not Fraudulently Induced into Awarding the SMOKE Contract.** The claim that the SMOKE contract was fraudulently induced also fails for lack of causation. Again, it strains credulity that compliance with requirements that apply only to non-fundamental research would be the but-for cause of an award to perform fundamental research. The Complaint never alleges that DoD considered compliance with DFARS 7012 or 7019 or, in awarding the SMOKE contract, *even looked up* the Astrolavos Lab's self-assessment score. The Complaint's only causation allegation— "DARPA relied on [GTRC's] representations and certifications," Compl. ¶126—fails even under Rule 8. *Iqbal*, 556 U.S. at 678.

### 3. The Complaint Fails to Plead Scienter

While the Complaint alleges that some Georgia Tech employees believed the Astrolavos Lab had inadequate cybersecurity controls, it fails to allege facts showing what matters: that GTRC knowingly made false claims to DoD. The scienter standard under the FCA is "whether the defendant knew the claim was false." *U.S. ex rel. Schutte v. SuperValu Inc.*, 598 U.S. 739, 743 (2023). To show scienter in

fraudulent inducement, the Complaint must plead that a false promise of compliance was "known to be a lie" when made. *Marsteller*, 556 F. Supp. 3d at 1302. "Generally, there is no inference of fraudulent intent not to perform from the mere fact that a promise made is subsequently not performed." *Willard*, 336 F.3d at 386; *Marsteller*, 556 F. Supp. 3d at 1305 (same). The Complaint fails to plausibly allege scienter on the EA fraudulent inducement claim or the SMOKE false certification and fraudulent inducement claims.

**No Facts Alleged to Show GTRC's Scienter in 2016 Under EA Contract.** As explained above, GTRC's submission of its June 2016 EA proposal included no promise that it would comply with DFARS 7012. But such a promise, had one been made, could not amount to fraudulent inducement because there are no facts alleged that GTRC—at the time it sought the contract—knew it would not comply with DFARS 7012 and falsely promised that it would. Pleading such a claim would require alleging that GTRC knew in June 2016 that (a) the cybersecurity rules applied to the EA contract, (b) the rules required an SSP and antivirus software for the relevant lab, (c) the lab would not have an SSP or antivirus software 18 months later when the rules kicked in, and (d) these requirements would be material to DoD.

The government cannot sidestep its obligation to plead facts with sweeping conclusions that Defendants supposedly "knew Georgia Tech was not and would not by December 31, 2017 be compliant." Compl. ¶238; *see id*. ¶240 (similar). This

broad allegation (which appears to apply to the whole institution rather than any specific lab) does not address any of the factual allegations just discussed. The same is true of the vague allegation that for "multiple years" there was "no enforcement" of the SSP requirement, *id.* ¶¶160, 237, which the Complaint never pins to any specific time period, much less to June 2016 when the contract was signed (and before the rules even required SSPs or antivirus software). The Complaint casts aspersions on a Georgia Tech policy about SSPs that was "adopted during the time" a particular Chief Information Security Officer was in charge, *id.* ¶236, but that CISO did not even hold the role until 2017, *id.* ¶39, so the later-adopted policy has no bearing on GTRC's scienter in 2016. Likewise, the Complaint's references to emails in 2019 and 2021, *id.* ¶¶159, 244, shed no light on GTRC's intent in 2016. GTRC's alleged nonperformance in January 2018—18 months after the allegedly false promise—is far from the "short time … between the making of the promise and the refusal to perform it" necessary to infer intent from nonperformance. *Marsteller*, 556 F. Supp. 3d at 1305. The Complaint is thus deficient for the same reasons as in *Willard*, where the relator could not plead intent to fraudulently induce. There, as here, the complaint failed to allege a "single fact" about "who was involved in the [contract] negotiations, or where or when the negotiations took place" or "what was said before, during, or after the contract negotiations to indicate that the contract was entered with no intent" to perform. 336 F.3d at 385.

**No Facts Alleged to Show GTRC's Scienter in 2022 for SMOKE Contract.**

The Complaint fails to plausibly allege scienter for either the false certification or fraudulent inducement claims regarding SMOKE. The Complaint pleads no facts suggesting that anyone knew SMOKE would require implementation of NIST SP 800-171, let alone that someone knew it in 2022 when GTRC submitted its offer and executed the contract (as required to plead fraudulent inducement). This is unsurprising, because (as the Complaint concedes), the SMOKE contract "called for the Astrolavos Lab to only perform fundamental research" that is not subject to the DoD cybersecurity requirements. Compl. ¶127; *see* Ex. 27, SMOKE Modification Attachment 1A at 6 ("DARPA expects the work performed by [GTRC] … under this contract to be fundamental research."). And, in recognition that SMOKE was for fundamental research, the Astrolavos Lab implemented a "fundamental research exception" SSP. Compl. ¶168. The Complaint does not (and cannot) plead facts that, notwithstanding the SMOKE contractual language, GTRC (a) knew that DoD cybersecurity requirements (which by definition do not apply to fundamental research) nonetheless applied *and* (b) intended to violate those requirements.

### 4. The Complaint Fails to Plead that Strict Compliance with Cybersecurity Controls Was Material to DoD's Payment Decision

The Complaint does not plausibly allege materiality because cybersecurity requirements were not the "essence" of GTRC's contract with DoD. There is no

allegation that DoD asked GTRC about cybersecurity in the Astrolavos Lab generally or about any of the 110 controls in NIST SP 800-171. And despite knowledge of GTRC's alleged noncompliance, DoD has done virtually nothing—much less halt or seek to recoup payment—in response.[11]

Materiality is a "demanding" standard that seeks to limit the scope of liability under the FCA to claims for which the government "would [have] attach[ed] importance to" the violation "in determining [whether to pay the claim]." *Escobar*, 579 U.S. at 193-94. It focuses on "the effect on the likely or actual behavior of the recipient of the alleged misrepresentation." *Id.* at 193. "[N]oncompliance [that] is minor or insubstantial," such as "garden-variety breaches of contract or regulatory violations," "will not satisfy the FCA's materiality requirement." *MIC*, 987 F.3d at 1347 (quoting *Escobar*, 579 U.S. at 194).

In this circuit, the factors relevant to materiality are: (1) "whether the misrepresentations went to the essence of the bargain with the government;" (2) "to the extent the government had actual knowledge of the misrepresentations, the effect on the government's behavior;" and (3) "whether the requirement is a condition of the government's payment." *Id*. No factor is dispositive. *Id.*

[11] The Complaint does not plead facts showing that compliance with FAR 52.204-21 was material or, with respect to falsity, that GTRC ever certified compliance with FAR 52.204-21 or that GTRC's invoices made representations about services that were rendered half-truths by the alleged failure to comply with that FAR clause.

**Cybersecurity Rules Did Not Go to the Essence of the Bargain.** The allegations and incorporated documents show that DoD's cybersecurity controls were far from essential to these contracts—and were in fact irrelevant—because DoD deemed the Astrolavos Lab's work to be fundamental research. This explains why DoD did not include the DFARS 7008 clause in the EA solicitation or identify any CDI in the EA contract documents. If DoD viewed cybersecurity compliance as the "essence" of these contracts, the government would be able to describe when DoD asked GTRC about its cybersecurity controls, when DoD identified relevant CDI to GTRC, and when DoD explained how CDI should be handled.

Despite years of investigation, days of testimony, and thousands of documents produced, the government has not pled a single fact alleging that a contracting officer *ever* considered, much less relied on, GTRC's compliance with the DFARS clauses, or that GTRC *knew* compliance was material to the government. *Escobar*, 579 U.S. at 195-96. The absence of such an allegation is particularly striking for DFARS 7019, where DoD rules require the contracting officer to "verify" the SPRS score. 48 C.F.R. §204.7303(b). The government never pleads that anyone actually did so, a shortcoming that illustrates how unimportant this issue was to DoD.

The regulations themselves support the inference of immateriality. DFARS 7012 does not even require implementation of the NIST SP 800-171 controls—simply having a plan to do so in the future suffices. Compl. ¶63; Ex. 32, DoD,

Memo. re Implementation of DFARS Clause 252.204-7012, 2-5 (Sept. 21, 2017). And here the government has, at most, alleged violations of a handful of the 110 controls, which is the definition of "minor or insubstantial" noncompliance. *See FDIC v. Fifth Third Bank, N.A.*, 2023 WL 7130553, at *4 (2d Cir. 2023) (minor noncompliance not material); *see also Escobar*, 579 U.S. at 194. With respect to DFARS 7019, there is no SPRS score—no matter how low—that makes a contractor ineligible for award, and DoD expressly attributes "[l]ow" confidence to such scores because they are "self-generated." 48 C.F.R. §252.204-7020(a)(3) ("DFARS 7020").

The Complaint's allegations purporting to show that DoD cybersecurity requirements are material—presidential proclamations about cybersecurity, *see* Compl. ¶¶259-62, and the creation of Department of Justice "initiatives," *id.* ¶¶271-72—are irrelevant, as they are not particularized facts concerning the behavior of the "*recipient[s]* of the alleged misrepresentation," *Escobar*, 579 U.S. at 193 (emphasis added)—here DoD (and more specifically DARPA and AFRL). And given the dearth of DoD action to counter noncompliance with DFARS 7012 and 7019, statements from the interim final rules *creating* those two regulations do not support the inference that DoD considers noncompliance to be material. *See* Compl. ¶¶264-70. In short, the government cannot plead that the DoD cybersecurity requirements "went to the essence of the bargain" with GTRC.

**DoD Knew About Alleged Noncompliance and Still Paid Claims.** The government's knowledge of alleged noncompliance with DoD cybersecurity regulations, and its conduct in response, also cuts against materiality. *Escobar*, 579 U.S. at 194-95. For example, the government knew about GTRC's supposed noncompliance no later than July 2022, when the relators' complaint was filed and the government launched its wide-ranging investigation. *See* Dkt. 17. After the relators had claimed the Astrolavos Lab had inadequate cybersecurity controls, DoD awarded GTRC the SMOKE contract, *see* Compl. ¶127, and paid many SMOKE invoices—including *after* the government's intervention here—totaling $10 million, *id.* ¶¶287-89; *see U.S. ex rel. Janssen v. Lawrence Mem'l Hosp.*, 949 F.3d 533, 542 (10th Cir. 2020) (inaction in the face of "detailed allegations from a former employee suggests immateriality"). If, as the government alleges, GTRC has not complied with the cybersecurity rules, then DoD has clearly "pa[id] a particular claim in full despite its actual knowledge that certain requirements were violated," which is "*very strong evidence* that those requirements are not material." *MIC*, 987 F.3d at 1348 (quoting *Escobar*, 579 U.S. at 195).[12]

[12] The immateriality of GTRC's alleged noncompliance is consistent with DoD's general approach to contractor cybersecurity. In report after report, the DoD Inspector General has described widespread non-compliance by DoD contractors, including researchers specifically. *See, e.g.*, Ex. 33, Report No. DODIG-2022-061 at 6-7; Ex. 34, Report No. DODIG-2024-031 at 4, 9-10. And in report after report, the Inspector General has criticized DoD contracting components because they do not

**Cybersecurity Rules Are Not a Payment Condition.** Finally, the government cannot plead facts showing that the cybersecurity requirements were conditions of payment, which is "relevant" but not "dispositive" to the materiality analysis." *MIC*, 987 F.3d at 1347 (citing *Escobar*, 579 U.S. at 194). At most, the Complaint alleges that the DoD cybersecurity rules were conditions of *contract*, but this factor applies only to conditions of payment, which *Escobar* made clear are different than conditions of contract or eligibility. *See* 579 U.S. at 192.

### B. The Government's False Record Or Statement Claim Under Section 3729(a)(1)(B) Against GTRC Fails As A Matter Of Law (Count II)

The Complaint alleges that GTRC violated section 3729(a)(1)(B) by making false statements relating to its promises to comply with DFARS 7012, its certification of compliance with DFARS 7019, and in its invoices for payment. To plead a false statement claim, a complaint must plead with particularity "(1) the defendant made,

---

assess or enforce DoD's cybersecurity requirements. *See, e.g.*, Ex. 33, Report No. DODIG-2022-061 at 17; Ex. 34, Report No. DODIG-2024-031 at 5-6. Unsurprisingly, the Complaint fails to identify a single instance where DoD withheld payment or terminated a contract because a researcher did not comply with cybersecurity regulations. Nor does it plead facts showing the DoD has opened its "toolbox" to pursue other remedies. *MIC*, 987 F.3d at 1352. In fact, the only step the Complaint identifies is a DoD memorandum reminding contracting officers of "contractual remedies to ensure contractor compliance with" DFARS 7012. Compl. ¶263. That pales in comparison to the government's actions in *MIC*, where, to combat noncompliance with lender-fee regulations, the agency "implemented more frequent and more rigorous audits," "consistently required lenders to refund any improperly charged fees that they discovered," and issued a circular "warning of the consequences of noncompliance." 987 F.3d at 1351.

or caused to be made, a false statement"; (2) scienter; and (3) materiality. *U.S. ex rel. 84Partners, LLC v. Nuflo, Inc.*, 79 F.4th 1353, 1359 (11th Cir. 2023). "A false claim is essential … under §3729(a)(1)(B)." *Id*; John T. Boese, *Civil False Claims and* Qui Tam *Actions*, (5th ed. 2020) ("Section 3729(a)(1)(B) is dependent upon a violation of Section 3729(a)(1)(A) because the provision requires a false claim").

As the government's false statement claim is premised on the same alleged false certifications and promises to implement DoD cybersecurity requirements as its presentment claim, *see* Compl. ¶¶298-305, the Complaint's failure to plead with particularity that GTRC made either false certifications or false promises dooms the false statement claim. *See Jackson*, 667 F. Supp. 3d at 357 (dismissing 3729(a)(1)(B) claim for failure to plead a false claim); *U.S. ex rel. Brooks v. Stevens-Henager College, Inc.*, 359 F. Supp. 3d 1088, 1109 (D. Utah 2019) (same).

The Complaint also fails to plead the independent elements of this claim. GTRC made no false statements about purported compliance with DFARS 7012 and 7019 because those provisions did not apply to the fundamental research performed under the EA and SMOKE contracts. And the government cannot assert that GTRC's invoice certifications were false because it never alleges that the fiscal data they cover were incorrect. Nor does the Complaint plead facts showing GTRC knew the alleged statements were, in fact, false. There is no allegation that GTRC knew it needed to but would not implement DFARS 7012 in either 2016 (EA contract) or in

2022 (SMOKE contract); or that the individual certifying compliance with DFARS 7019 in connection with the SMOKE contract knew that certification was false, *see* Compl. ¶125; or that GTRC knew its certifications about fiscal data were false. For all these reasons, the false statement claim fails.

## II. THE COMPLAINT DOES NOT PLEAD VIABLE COMMON-LAW CLAIMS

The Complaint's common-law claims recycle the same allegations as the FCA claims, and for many claims the Complaint attempts to bring in Georgia Tech as a defendant despite the fact that it never contracted with DoD and never made any representations to DoD. The common-law claims fail for the same reasons as the FCA claims and for the additional reasons below.

### A. The Complaint Does Not Adequately Plead Fraud Against GTRC Or Georgia Tech (Count III)

The government's common-law fraud claim is limited to its theory that GTRC and Georgia Tech submitted a false SPRS score in December 2020. To state a fraud claim, the government must plead with particularity allegations showing, among other elements: (1) a false representation of a material fact; (2) justifiable reliance that induces the recipient to act, and (3) economic injury resulting from reliance on the misrepresentation. *U.S. ex rel. Badr v. Triple Canopy, Inc.*, 950 F. Supp. 2d 888, 904 (E.D. Va. 2013), *aff'd in relevant part*, 775 F.3d 628 (4th Cir. 2015).

At the outset, the Complaint does not plead facts with particularity supporting its claim that *Georgia Tech* made any misrepresentation at all. GTRC, not Georgia

Tech, submitted the SPRS score. Compl. ¶¶201-02. The Complaint pleads no facts showing that Georgia Tech made its own submission to DoD or that the Georgia Tech employees who submitted the SPRS score spoke for Georgia Tech (as opposed to GTRC). Relatedly, the Complaint alleges that a GTRC employee—and no Georgia Tech employee—certified that there was a compliant SPRS score in connection with the SMOKE contract. *Id.* ¶125. And the Complaint's other allegations "lump[ing]" Georgia Tech and GTRC together, *U.S. ex rel. Heller v. Guardian Pharm. LLC*, 521 F. Supp. 3d 1254, 1280 (N.D. Ga. 2021), cannot satisfy Rule 9(b), *see* Compl. ¶¶215, 218-21. In short, the Complaint fails to allege that Georgia Tech made any representation, much less a misleading one, to DoD.

In any event, as to either defendant, the claim fails. The SPRS-based claim cannot apply to the EA contract, which was executed in 2016—four years before DFARS 7019 became effective—and was never amended to incorporate that clause. And it cannot apply to the SMOKE contract, which, with respect to the Astrolavos Lab, was expressly for fundamental research not subject to DFARS 7019. *See supra* §I(A)(1)(a). And even if it did apply to SMOKE, the fact that DoD has continued to pay SMOKE invoices notwithstanding knowing about alleged noncompliance with DFARS 7019 defeats materiality. *MIC*, 987 F.3d at 1348.

The Complaint also fails to plead facts showing the government's justifiable reliance on any alleged misrepresentation. *Next Century Commc'ns Corp. v. Ellis*,

214 F. Supp. 2d 1366, 1370-71 (N.D. Ga. 2002), *aff'd*, 318 F.3d 1023 (11th Cir. 2003). It does not "allege with particularity" "who" reviewed the SPRS score, "when" it was reviewed, and "how the review of [the SPRS score] on a specific date influenced" the decision to enter the SMOKE contract. *Badr*, 950 F. Supp. 2d at 904; *see also Epple v. Reich*, 2024 WL 2745330, at *8-9 (N.D. Ga. Feb. 20, 2024) (similar). In fact, there is no allegation that anyone in the government ever looked at the SPRS score. The government's conclusory allegation that DoD "relied on these representations and certifications" falls well short under *Iqbal* and Rule 9(b) and should be disregarded. Compl. ¶¶126, 312-13.

Finally, the government has not pleaded facts showing an injury, let alone an "economic injury," from the alleged fraud. *Keil v. Lagroon*, 2022 WL 4542116, at *7 (S.D. Ga. Sept. 28, 2022). There is no allegation the government did not receive the research GTRC was contracted to perform or that information related to the SMOKE contract was compromised. Nor does the Complaint allege the government would have acted any differently had it known of the allegedly inaccurate SPRS score. *See Lucas Ent. Grp., LLC v. Robert W. Woodruff Arts Ctr., Inc.*, 720 F. App'x 512, 517 (11th Cir. 2017). At most, according to the Complaint, "technology … [was] stored in an environment that was not secure from unauthorized disclosure." Compl. ¶291. But because the government never alleges it was economically harmed as a result, this alleged injury cannot support a common-law fraud claim.

### B. The Complaint Does Not Adequately Plead Negligent Misrepresentation Against GTRC Or Georgia Tech (Counts IV, V)

The government asserts two claims for negligent misrepresentation. In Count IV, the Complaint asserts a claim based on GTRC and Georgia Tech's submission of an allegedly false SPRS score in December 2020. *See* Compl. ¶¶315-23. In Count V, it asserts a claim against GTRC alone based on its alleged promise to comply with DFARS 7012 by 2018 and on the certifications on GTRC's invoices for payment. *Id.* ¶325. "[N]egligent misrepresentation is similar to fraud and requires the same elements of proof, the only difference being whether the defendant knowingly or negligently made the misrepresentations." *VC Macon, GA LLC v. Virginia Coll. LLC*, 2021 WL 723979, at *9 (M.D. Ga. Feb. 24, 2021).

Because the allegations and elements substantially overlap, the SPRS-score negligent misrepresentation claim against GTRC and Georgia Tech (Count IV) fails for the same reasons as the common-law fraud count (Count III).

The claims related to implementation of NIST SP 800-171 and invoice certifications brought against GTRC in Count V likewise fail. With respect to the EA contract, GTRC's work was for fundamental research not subject to NIST SP 800-171, and its alleged promise in 2016 to implement NIST SP 800-171 by 2018, *see* Compl. ¶325, is, at most, a "promise about future conduct [that] cannot be the basis for a … negligent misrepresentation claim" where, as here, the Complaint pleads no facts that the promisor "knows that the future event will not take place."

*FDIC v. Watkins*, 2013 WL 12249504, at *3 (N.D. Ga. Oct. 16, 2013). As to the SMOKE contract, the work that DoD contracted to be performed at Georgia Tech was also expressly for fundamental research. *See supra* §I(A)(1)(a). And the assertion that GTRC made misrepresentations related to its invoice certifications is unavailing, because those certifications concern cost data and there is no allegation that the data were inaccurate. *See supra* §I(A)(2)(a).

The Complaint also fails to allege materiality, actual and justifiable reliance, and injury. The materiality analysis for negligent misrepresentation and the FCA are the same, *see U.S. v. Pub. Warehousing Co.*, 2017 WL 1021745, at *5 (N.D. Ga. Mar. 16, 2017), and thus materiality is lacking for the reasons previously discussed, *see* §I(A)(4). The Complaint's reliance allegations are either conclusory—e.g., DoD relied on representations about DFARS 7012 and 7019, Compl. ¶¶126, 327—or nonexistent—i.e., DoD relied on GTRC's invoice certifications. Finally, because the misrepresentation counts rely on the same deficient injury allegations as the fraud count, *see id*. ¶¶290-91, 328, the government has failed to plead this element too.

### C. The Complaint Does Not Adequately Plead Unjust Enrichment And Payment By Mistake Against Either Defendant (Counts VI and VII)

The government's claims that GTRC and Georgia Tech were unjustly enriched and that DoD paid by mistake, *id*. ¶¶330, 332-34, fail both because (1) neither of these equitable claims can coexist with the written contracts that governed the

Astrolavos Lab's research; and (2) DoD received, and GTRC and Georgia Tech were appropriately compensated for, the research performed under the contracts.

Unjust enrichment and payment-by-mistake claims will not lie where the subject matter of the claim is governed by contract. *See Public Warehousing*, 2017 WL 1021745, at *10; *U.S. ex rel. Reeves v. Mercer Transp. Co.*, 253 F. Supp. 3d 1242, 1255-56 (M.D. Ga. 2017). That is true where a claim is asserted against a contractual party or against a defendant not a party but who received a financial benefit from the contract. *Public Warehousing*, 2017 WL 1021745, at *10 (unjust enrichment and payment by mistake claims dismissed against contract non-party); *Peterson v. Aaron's, Inc.*, 2015 WL 5479877, at *1-2 (N.D. Ga. Sept. 16, 2015).

Here, the government must concede the validity of the EA and SMOKE contracts, which are the entire basis for its case. Those contracts are also the heart of its unjust enrichment and payment-by-mistake claims. *See id.* ¶¶102, 127. These claims must therefore be dismissed as to GTRC, which was a party to the contracts, and Georgia Tech, which according to the Complaint, received a portion of the funds the government paid under those contracts. *Id.* ¶¶330, 333-34.

These claims should also be dismissed because there is no allegation that DoD did not receive the research it contracted for. *See U.S. ex rel. Dustman v. Advoc. Health & Hosps. Corp.*, 2023 WL 2799699, at *11 (C.D. Ill. Apr. 5, 2023)

(dismissing unjust enrichment and payment by mistake claims for failure to adequately allege that claims "should not have been paid").

### D. The Government's Breach Of Contract Claim Against GTRC Fails As A Matter Of Law (Count VIII)

The government claims that GTRC breached the EA and SMOKE contracts by violating DFARS 7302, 7008, 7012, 7019, 7020, and FAR 52.204-21 and by falsely certifying compliance with DFARS 7012, 7019, and 7020. Compl. ¶337.

This claim fails because, as discussed above, both contracts were for fundamental research, such that the cybersecurity requirements did not apply. Also, like the other common-law claims, the government's assertion that it has been injured by inadequate storage of technology fails to show any "harm[]." *Northrop Grumman Computing Sys., Inc. v. U.S.*, 823 F.3d 1364, 1368 (Fed. Cir. 2016).

Moreover, only a few of these provisions were even incorporated in the EA and SMOKE contracts. *See Northrop Grumman Info. Tech., Inc. v. U.S.*, 535 F.3d 1339, 1346-47 (Fed. Cir. 2008). In fact, the EA contract incorporated only DFARS 7012 and FAR 52.204-21, *see* Ex. 15, EA Contract at 13, 17; Compl. ¶¶108, 120. The SMOKE contract incorporated only DFARS 7012, 7019, and 7020 and FAR 52.204-21, *see* Ex. 16, SMOKE Contract at 13, 15; Compl. ¶¶128-29. Because the other provisions were not "identif[ied] with detailed particularity" in the contracts, they were not incorporated and cannot support the contract claim. *See Northrop Grumman*, 535 F.3d at 1344. Nor can the remaining provisions support a contract

claim, because they are operative only for systems that handle CDI or FCI, which GTRC never did on these contracts.

In any event, even assuming the incorporated provisions did apply, the Complaint does not plausibly allege a material breach, which requires factual allegations showing a "fundamental" breach. *Unibright Ventures GmBH v. Provide Techs. Inc.*, 2023 WL 6214885, at *3 (N.D. Ga. July 20, 2023); *see Hotelecopy, Inc. v. U.S.*, 1993 WL 309623, at *1 (Fed. Cir. Aug. 17, 1993). With respect to DFARS 7012, none of the at-issue NIST requirements applied to the EA contract and the Astrolavos Lab implemented an SSP and antivirus software for SMOKE. *See supra* §I(A)(1)(b). And even if GTRC breached the SSP requirement by not "periodically" updating the plan (it did not), that minor breach was not material. The claim that GTRC breached DFARS 7020 also fails, because that clause just requires a contractor to allow "[government] access to its facilities" for security assessments, and there is no allegation that GTRC failed to do so here. *See* DFARS 7020(c).

## CONCLUSION

For the reasons stated above, the Complaint should be dismissed in full.

Dated: October 21, 2024

Respectfully submitted,

*/s/Douglas W. Gilfillan*
Douglas W. Gilfillan
Georgia Bar No. 294713
Gilfillan Law LLC
One Atlantic Center
1201 West Peachtree Street
Suite 2300
Atlanta, GA 30309
Telephone: (404) 795-5016
Doug@gilfillanlawllc.com
*Counsel for Georgia Tech Research Corp. and Georgia Institute of Technology*

*/s/Ronald Machen*
Ronald Machen*
DC Bar No. 447889
Matthew Jones*
DC Bar No. 502943
Wilmer Cutler Pickering
Hale and Dorr, LLP
2100 Pennsylvania Avenue
NW Washington, D.C. 20037
Telephone: (202) 663-6000
Fax: (202) 663-6363
Ronald.Machen@wilmerhale.com
Matt.Jones@wilmerhale.com

George P. Varghese*
Massachusetts Bar No. 706861
Wilmer Cutler Pickering
Hale and Dorr, LLP
60 State Street
Boston, MA 02109
Telephone: (617) 526-6000
Fax: (617) 526-5000
George.Varghese@wilmerhale.com

Peter Kurtz*
Colorado Bar No. 54305
Wilmer Cutler Pickering
Hale and Dorr, LLP
1225 17th Street, Suite 2600
Denver, CO 80202
Telephone: (720) 274-3135
Fax: (720) 274-3133
Peter.Kurtz@wilmerhale.com

*Counsel for Georgia Tech Research Corp.*

*Admitted *pro hac vice*

**CERTIFICATE OF COMPLIANCE WITH LOCAL RULE 5.1**

The undersigned hereby certifies that the foregoing document has been prepared in accordance with the font type and margin requirements of Local Rule 5.1 of the Northern District of Georgia, using a font type of Times New Roman and a point size of 14.

*/s/ Ronald Machen*
Ronald Machen

**CERTIFICATE OF SERVICE**

**I hereby certify** that on October 21, 2024, I electronically filed the foregoing Brief in Support of Defendants' Motion to Dismiss with the Clerk of the Court using the CM/ECF system, which will send Notices of Electronic Filing to all counsel of record.

*/s/ Ronald Machen*
Ronald Machen