UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNDER SEAL,	Plaintiff[s],	Civil Action No.
		JURY TRIAL DEMANDED
v.		
UNDER SEAL,	Defendant[s].	FILED IN CAMERA AND UNDER SEAL PURSUANT TO 31 U.S.C. § 3730

FALSE CLAIMS ACT COMPLAINT

DO NOT ENTER ON PACER

TABLE OF CONTENTS

UNITED STATES DISTRICT COURT
FOR THE DISTRICT OF MASSACHUSETTS

UNITED STATES OF AMERICA *ex rel.* KEVIN BERICH, Plaintiffs, v. MORSECORP, INC. and ANDREAS KALLAS, Defendants.	Civil Action No. JURY TRIAL DEMANDED FILED IN CAMERA AND UNDER SEAL PURSUANT TO 31 U.S.C. § 3730

COMPLAINT FOR VIOLATIONS OF THE FALSE CLAIMS ACT AND DEMAND FOR JURY

I. INTRODUCTION

1. This is an action brought by *qui tam* Plaintiff-Relator Kevin Berich, on behalf of the United States, to recover damages, civil penalties, and other relief from Morsecorp, Inc. d/b/a Morse Corp. ("Morse") and its CEO and primary owner Andreas Kallas (hereafter, collectively, "Defendants") pursuant to the *qui tam* provisions of the Federal False Claims Act, 31 U.S.C. §§ 3729, *et seq.*, ("FCA").

A. The Fraudulent Schemes

2. As is more fully described below, since in or before 2015, Morse has fraudulently induced the federal government to award it tens of millions of dollars in contracts, and to make tens of millions of dollars in contract payments, based on false representations and false submissions concerning Morse's compliance with required cybersecurity measures for safeguarding sensitive government information.

3. Morse describes itself as a "specially selected team of scientists, engineers, and software developers who use asymmetric and unconventional approaches to deploy practical solutions that solve difficult multi-disciplinary problems faced by the US National Security

Ecosystem." Over the past several years, Morse has pursued and been awarded multiple contracts from the U.S. Department of Defense ("DoD") including contracts to develop, analyze, and support several of DoD's most sensitive ongoing programs. The terms of those contracts require that Morse implement and maintain baseline cybersecurity measures to safeguard Controlled Unclassified Information ("CUI") and other sensitive government information belonging to DoD.

4. Morse has made repeated false representations to DoD concerning its compliance with the applicable DoD cybersecurity requirements. As a result of its false representations, Morse has fraudulently induced DoD to award it contracts worth tens of millions of dollars when, in fact, Morse's failure to maintain basic cybersecurity measures made it ineligible to perform the required work. Similarly, Morse has submitted inaccurate and false cybersecurity assessment scores to DoD to qualify for the payment of millions of dollars from the government. In fact, Morse was never in compliance with its contractual cybersecurity obligations, and it received those payments based on its false statements and submissions to DoD.

5. Morse has also made repeated false statements to prime contractors with respect to Morse's internal cybersecurity measures and required DoD assessment and thereby caused the submission of false and fraudulent claims and other records by those prime contractors to the federal government.

6. Morse also failed to develop, implement, or employ software development techniques, architectural designs, or system engineering principles to promote effective information security within the organization. Morse software developers could, and did, incorporate existing software programs gathered from multiple open sources without regard to the security vulnerabilities of those programs. As a result, Morse sold and supplied software to

DoD which failed to meet DoD's requirements for software cybersecurity, in violation of the controlling contract terms.

7. Morse and its senior executives were aware of Morse's chronic failure to comply with DoD's cybersecurity requirements but declined to expend the necessary corporate resources to achieve actual compliance. Morse executives openly discussed the company's disregard of DoD cybersecurity requirements, which placed U.S. national security and the safety of U.S. military personnel in peril, as a "business decision." The same executives described the perceived low probability of having DoD discover its noncompliance as what they considered to be an acceptable "business risk."

8. These schemes allowed Defendants to gain an unfair competitive advantage over competitors who and which expended the necessary resources to comply with the applicable DoD requirements for implementing and maintaining required cybersecurity measures to safeguard CUI and other sensitive government information.

9. Through these schemes Defendants have been unjustly enriched and have generated many millions of dollars in profits, which Defendants have divided among themselves.

B. The Instant Action

10. Based on the operative provisions of the FCA, *qui tam* Plaintiff-Relator seeks, through this action, to recover damages and civil penalties arising from Defendants' knowing fraud against the United States, including fraud against the Department of Defense.

11. The allegations set forth in this Complaint have not been publicly disclosed within the meaning of the FCA, as amended, 31 U.S.C. § 3730(e)(4). In the alternative, if the Court finds that there was a public disclosure of such allegations before the filing of this Complaint, Relator is an "original source" as that term is used in the FCA.

12. Prior to the filing of this Complaint, Relator made substantive disclosures to the United States of facts and evidence underlying the allegations in this Complaint.

13. This action is filed in camera and under seal pursuant to the requirements of the FCA.

II. JURISDICTION AND VENUE

14. This Court has jurisdiction over this action pursuant to 28 U.S.C. §§ 1331, 1345 and 31 U.S.C. § 3732, which confers jurisdiction over actions brought pursuant to 31 U.S.C. §§ 3729 and 3730.

15. This Court has personal jurisdiction over Defendants pursuant to 31 U.S.C. § 3732(a) because one or more Defendants can be found in, resides in, and transacts substantial business in this district, including business related to Defendants' misconduct.

16. Venue is proper in this District pursuant to 31 U.S.C. § 3732(a), 28 U.S.C. § 1391, and 28 U.S.C. § 1395(a), because one or more Defendants reside in and/or transact business in this District.

III. PARTIES

A. Plaintiffs

17. Plaintiff the United States of America is the real party in interest with respect to the Federal False Claims Act *qui tam* claims made herein pursuant to 31 U.S.C. § 3730(b).

18. Plaintiff-Relator Kevin Berich is a citizen of the United States and a resident of the Commonwealth of Massachusetts. Mr. Berich has more than 10 years of experience as a security professional working in the Defense Industrial Base sector. Since January of 2021 Relator has served as the Head of Security and Facility Security Officer for Morse. In that capacity, Mr. Berich is familiar with the information systems and networks Morse uses to

process, store, and transmit CUI and other sensitive government information. Mr. Berich also has first-hand knowledge of Morse's cybersecurity practices and procedures.

B. Defendants

19. Defendant Morsecorp Inc. d/b/a Morse (Mission Oriented Rapid Solution Engineering) Corp. ("Morse") is a privately held corporation created under the laws of the State of Delaware with headquarters located in Cambridge Massachusetts. In its mission statement, Morse describes itself as a "specially selected team of scientists, engineers, and software developers who use asymmetric and unconventional approaches to deploy practical solutions that solve difficult multi-disciplinary problems faced by the U.S. National Security Ecosystem" *See* https://www.morsecorp.com/about.html (last visited 01/09/2023). In practice, Morse derives virtually 100% of its revenues from its federal, mostly DoD, contracts and subcontracts.

20. Defendant Andreas Kellas is one of the three original founders of Morse and currently holds the title of Morse CEO. According to Morse's annual filings with the Commonwealth of Massachusetts, Kellas also holds the positions of President, Treasurer, and Corporate Secretary. While Morse identifies itself as being "employee owned," Kellas owns all shares of Morse voting stock and is the sole member of the Morse corporate board.

IV. LEGAL AND REGULATORY BACKGROUND

A. The Federal False Claims Act

21. The FCA creates liability to the United States for any entity that or individual who "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval," 31 U.S.C. § 3729(a)(1)(A); "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim," 31 U.S.C. § 3729(a)(1)(B); "conspires to commit a violation of" the False Claims Act, 31 U.S.C. § 3729(a)(1)(C); and/or "knowingly makes, uses, or causes 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 conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government," 31 U.S.C. § 3729(a)(1)(G).

22. Any entity that or person who violates the FCA is liable for a civil penalty for each violation, plus three times the amount of the damages sustained by the United States. 31 U.S.C. § 3729(a)(1). The civil penalty shall be not less than $5,000 and not more than $10,000, as adjusted by the Federal Civil Penalties Inflation Adjustment Act of 1990. 31 U.S.C. § 3729(a)(1). The penalty varies depending on the date of the violation. For violations on or after November 2, 2015, when adjusted for inflation as required, the civil penalty amounts range from a minimum of $12,537 to a maximum of $25,076. *See* 87 Fed. Reg. 27513 (May 9, 2022); *see generally* 28 C.F.R. § 85.5.

23. For purposes of the FCA, a person "knows" a claim is false if that person: "(i) has actual knowledge of [the falsity of] the information; (ii) acts in deliberate ignorance of the truth or falsity of the information; or (iii) acts in reckless disregard of the truth or falsity of the information." 31 U.S.C. § 3729(b)(1). The FCA does not require proof that a defendant specifically intended to commit fraud. *Id.* Unless otherwise indicated, whenever the words "know," "learn," "discover" or similar words indicating knowledge are used in this Complaint, they mean "knowingly" as defined in the FCA.

24. The FCA defines "claim" to include "any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property." 31 U.S.C. § 3729(b)(2). A claim can be "presented to an officer, employee, or agent of the United States"; or it can be "made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a

Government program or interest, and if the United States Government— (I) provides or has provided any portion of the money or property requested or demanded; or (II) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded." *Id.*

25. The FCA provides that "the term 'obligation' means an established duty, whether or not fixed, arising from an express or implied contractual, grantor-grantee, or licensor-licensee relationship, from a fee-based or similar relationship, from statute or regulation, or from the retention of any overpayment." 31 U.S.C. § 3729(b)(3).

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

B. Controlling Federal Contracting Law

27. United States government contracts are subject to Federal Acquisition Regulations ("FAR"). There are also agency specific regulations that supplement FAR. For example, contracts entered with the Department of Defense ("DoD") are also subject to Defense Federal Acquisition Regulations ("DFARS").

28. Over the past decade, DoD has made a concerted effort to mandate minimum cybersecurity practices on the part of its contractors and subcontractors in the Defense Industrial Base sector. In pursuit of that goal, DoD has made a series of revisions to the DFARS and issued Interim Rules and Guidance Memoranda which require contractors to meet or exceed cybersecurity standards specified by the National Institute of Standards and Technology ("NIST"), specifically those required under NIST Special Publication 800-171 ("NIST SP 800-171"). NIST SP 800-171 sets out detailed methodologies for developing and maintaining

cybersecurity measures to protect CUI in the possession of contractors, subcontractors and other nonfederal systems and organizations.

29. NIST SP 800-171 divided cybersecurity requirements into fourteen areas, including, for example, access control, configuration, system and information protection, and audit and accountability. NIST SP 800-171 identified both basic security requirements and derived security requirements for each of those fourteen categories, which are designated as "Security Requirement Families." NIST SP 800-171A provided detailed instructions for the assessment of CUI security requirements through examination, interviews, and testing.

30. Since December 30, 2015, all contractors performing services for or providing goods (other than so called commercial off the shelf items) to DoD have been required to meet or exceed the NIST SP 800-171 cybersecurity requirements. DFARS 252.204.7008(c)(1) & (2) and 252.204-7012.

31. Federal Acquisition Regulation ("FAR") 1.602-1(b) provides that: "No contract shall be entered into unless the contracting officer ensures that all of the requirements of law, executive orders, regulations, and all other applicable procedures, including clearances and approvals, have been met." DoD contracting officers have no authority to enter into a contract unless the contractor is complying with DFARS regulations that are legally required to be incorporated in the contract.

32. Compliance with DFARS regulations that are required by law to be incorporated in federal contracts are non-waivable contract terms. According to FAR 1.602-3, the Government can only ratify a change in a contract obligation if the resulting contract "would otherwise have been proper if made by an appropriate contracting officer" and any such

ratification is "in accordance with any other limitations prescribed under agency procedures." FAR 1.602-3(c)(3) & (7).

2015 DoD Interim Rule

33. In August 2015, DoD issued an Interim Rule modifying DFARS Clause 252.204-7012 to align with the cybersecurity requirements of NIST SP 800-171. 80 Fed. Reg. 51739-40 (August 26, 2015). DoD issued the Interim Rule to protect "sensitive information residing in contractor information systems." 80 Fed. Reg 51740.

34. Under the 2015 Interim Rule, contractors were temporarily allowed to implement "alternative but equally effective cybersecurity measures" as an alternative to compliance with NIST SP 800-171. 80 Fed. Reg 51744-45 and DFARS 252.204.7008(c)(1) & (2). However, any contractor who used any such alternative measures was required to notify and obtain written acceptance from DoD for the request to deviate from NIST SP 800-171 "prior to the award" of the relevant DoD contract. 80 Fed. Reg 51745 and DFARS 252.204.7008(d).

35. The 2015 Interim Rule also added new cybersecurity requirements for cloud services used to store CUI and other sensitive government information by adding DFARS 252.239.7009 and modifying DFARS 252.239.7010. The revised DFARS provisions directed that all DoD contractors using cloud computing services "shall implement and maintain administrative, technical, and physical safeguards and controls" in accordance with DoD's Cloud Computing Security Requirements Guide. 80 Fed. Reg. 51747 and DFARS 252.239.7010(b).

36. The DoD 2015 Interim Rule was finalized in December of 2015. 80 Fed. Reg. 81472 (December 30, 2105). In the final version, DoD announced "Contractors will be given until December 31, 2017 for implementation of NIST 800-171 security requirements." 80 Fed. Reg. 81473. The 2015 Interim Rule also amended DFARS 252.204-7008 to provide that the

submission of any offer to DoD constituted a representation by the offeror that "it will implement the security requirements" as specified by NIST SP 800-171 "not later than December 31, 2017." 80 Fed. Reg. 81473 and DFARS 204.7008(c)(1).

2017 DoD Guidance Memorandum

37. On September 21, 2017, the DoD Office of the Under Secretary of Defense (DoD-OUSD) issued a Guidance Memorandum titled "Safeguarding Covered Defense Information and Cyber Incident Reporting" (hereafter, "09/21/2017 Memo") which expressly reconfirmed the December 31, 2017 deadline for compliance with all NIST SP 800-171 measures. (09/21/2017 Memo., pg. 1). The 09/21/2017 Memo stated "[u]ltimately, it is the contractor's responsibility to determine whether it has implemented the NIST 800-171 [measures]…as well as any other security measures necessary to provide adequate security for covered defense information." *Id*, pg. 2.

38. The 09/21/2017 Memo also specified the mechanics by which each contractor was to inform the government of the contractor's implementation of NIST SP 800-171 cybersecurity measures. The 09/21/2017 Memo specifically cited the solicitation provisions of DFARS 252.204-7008, which provided that, by submitting any offer to DoD, the contractor was "representing its compliance" with NIST SP 800-171. (09/21/2017 Memo., pg. 3).

2020 DoD Interim Rule

39. In September 2020, DoD issued an Interim Rule entitled "Assessing Contractor Implementation of Cybersecurity Requirements." 85 Fed. Reg. 61505 (Sept, 29, 2020). (hereafter, "2020 Interim Rule"). The 2020 Interim Rule was issued "to enhance the protection of unclassified information" within the DoD supply chain. In pursuit of that result, the 2020

Interim Rule announced a new assessment methodology and framework "to assess contractor implementation of cybersecurity requirements." 85 Fed. Reg. at 61505.

40. The 2020 Interim Rule amended DFARS 204.7302 to make clear that all DoD contractors and subcontractors required to implement NIST SP 800-171 were further required "at time of award" to have "at least a Basic NIST SP 800-171 DoD Assessment that is not more than three years old." 85 Fed. Reg. 61519 and DFARS 204.7302(a)(2). Going forward, all DoD government contractors were required to meet and maintain the specified cybersecurity rating under DoD's Cybersecurity Maturity Model Certification (CMMC) program. 85 Fed. Reg. 61520 and (DFARS 204.7302(b).

41. The body of the 2020 Interim Rule candidly acknowledged the failure of prior DoD regulations to bring about necessary compliance with applicable cybersecurity requirements. For example, the 2020 Interim Rule cited a 2018 survey of DoD contractors in which 45% of all respondents acknowledged not having read NIST SP 800-171 and cited to the results of on-site assessments by DoD personnel which found that only 36% of contractors "demonstrated implementation of all 110 of the NIST SP 800-171 security requirements." 85 Fed. Reg. 61518. The 2020 Interim Rule starkly observed "[d]efense contractors must begin viewing cybersecurity as part of doing business, in order to protect themselves and to protect national security." *Id.*

42. While prior regulations had allowed DoD contractors to conduct fully internal assessments of cybersecurity compliance, the 2020 Interim Rule announced that contractors would be required to document the results of those assessments in DoD's Supplier Performance Risk System ("SPRS"). 85 Fed. Reg. 61505. The SPRS was created to be DoD's "authoritative source for supplier and product performance information" and to alert DoD to "how many

security requirements have not yet been implemented." 85 Fed. Reg. 61511. The requirement of accurate contractor assessments was identified as necessary for the "urgent need for DoD to immediately begin assessing where vulnerabilities in its supply chain exist" and to "take steps to correct such deficiencies." 85 Fed. Reg. 61518.

43. To achieve the objective of enhancing the protection of CUI within the DoD supply chain, the 2020 Interim Order created three new DFARS provisions identified as DFARS 252.204-7019, 7020 and 7021.

44. The new DFARS 252.204-7019: Notice of NIST SP 800-171 DoD Assessment Requirements created specific requirements for any offeror bidding on DoD contracts. Specifically, DFARS 252.204-7019:

- Required that an offeror possess an assessment for each covered contractor information system that is relevant to the offer, contact, task order, or delivery order to be considered for an award. 85 Fed. Reg. 61520 and DFARS 252.204-7019(b); and
- Required that an offeror verify that summary level scores of a NIST SP 800-171 DoD Assessment (that are not more than 3 years old) are posted into SPRS for all covered contractor information systems relevant to its offer. 85 Fed. Reg. 61520-21 and DFARS 252.204-7019(c)(1).

45. To ensure that each member of DoD's supply chain was in compliance with cybersecurity measures, DoD also issued DFARS clause 252.204-7020. Among other requirements, DFARS clause 252-204-7020:

- Required a contractor to insert DFARS clause 252.204-7020 NIST SP 800-171 DoD Assessment Requirements in all subcontracts and other contractual instruments. 85 Fed. Reg. 61522 and DFARS 252.204-7019(g)(1).
- Required that a contractor not award a subcontract or other contractual instrument unless the subcontractor has completed at least a Basic NIST SP 800-171 DoD Assessment for all covered contractor information systems relevant to the offer within the last 3 years. 85 Fed. Reg. 61522 and DFARS 252.204-7019(g)(2).

46. Finally, the new 2020 Interim Rule included DFARS clause 252.204-7021 with the goal of requiring CMMC compliance from all DoD contractors going forward. Among other requirements, DFARS clause 252-204-7021:

- Required that all DoD contractors possess a current (not more than 3 years old) CMMC certificate at the CMMS level required by the contract. 85 Fed. Reg. 61522 and DFARS 252.204-7021(b).
- Required that all DoD contractors insert the same requirement into all subcontracts or other contractual documents. *Id*, (DFARS 252.204-7021(c)(1).
- Required DoD contractors to confirm that a subcontractor satisfied the CMMC certificate requirement prior to awarding any subcontract. *Id*, (DFARS 252.204-7021(c)(2).

47. To implement a "phased roll out" of the CMMC cybersecurity requirements, the 2020 Interim Order also amended DFARS 204.7502 to provide that, prior to October 1, 2025:

- DoD solicitations, contracts, task orders, and similar documents were to specify the CMMC level required from the DoD contractor. 85 Fed. Reg. 61520 and DFARS 204.7503(a)

- DoD-OUSD could approve a requirement of CMMC level certification for any solicitation of a specific DoD contract, task order, or similar document. *Id.*
- After October 1, 2025, all DoD contracts were to incorporate the above quoted terms from DFARS 252.204-7021. *Id.*

2021 Department of Justice Cyber-Fraud Initiative

48. On October 6, 2021, Deputy Attorney General Lisa O. Monaco announced a new Department of Justice Cyber-Fraud Initiative using the False Claims Act to "pursue cybersecurity related fraud by government contractors." The initiative was announced with the stated goal to "hold accountable entities or individuals that put U.S. information or systems at risk by knowingly providing deficient cybersecurity products or services, knowingly misrepresenting their cybersecurity practices or protocols, or knowingly violating obligations to monitor and report cybersecurity incidents and breaches." *See* https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative (last visited 01/05/2023).

49. In announcing the 2021 DOJ Cyber-Fraud Initiative, Deputy Attorney General Monaco stated, "[f]or too long companies have chosen silence under the mistaken believe that it is less risky to hide a breach than to bring it forward and to report it…Well that changes today." Deputy Attorney General Monaco added "[w]e will use our civil enforcement tools to pursue companies, government contractors who receive federal funds, when they fail to follow required cybersecurity standards – because we know that puts all of us at risk." *Id.*

V. FACTS AND ALLEGATIONS

50. In January of 2021, Relator was hired as Morse's Head of Security and Facility Security Officer for the company's Cambridge, Massachusetts headquarters. Relator's job

responsibilities included supervising daily security activities, enforcing controls, and ensuring that company security policies were strictly followed. In carrying out his official duties, Relator became familiar with the information systems and networks Morse uses to store, process, and transmit CUI and other sensitive government information.

51. Relator also became familiar with Morse's cybersecurity practices and procedures. Relator had regular face-to-face discussions of cybersecurity matters with numerous Morse senior executives, managers, and employees including, but not limited to, Chief Executive Officer Andreas Kellas, Chief Operating Officer Josh Torgerson, Morse co-founder Bobby Cohanim, Chief Technology Officer Eric Nelson, Contractor Program Security Officer Matt DeWitt, Information Systems Security Manager Nicolas Fichera, and Head of IT Christopher Platt.

52. Within weeks of arriving at Morse, Relator witnessed multiple violations of industry standard cybersecurity requirements, including:

- Employees using personal and unregistered devices to access Morse information systems used to store and transmit CUI;
- Failure to implement multi factor authentication for devices and users accessing Morse information systems used to store and transmit CUI;
- Failure to maintain logs to identify instances of unauthorized access to Morse information systems used to store and transmit CUI;
- Failure to install anti-virus software on approximately 90% of software programs or on devices used to access Morse information systems used to store and transmit CUI;
- Use of non-compliant email hosting services for communications that contained CUI;
- Use of non-compliant cloud data storage services for records that contained CUI;
- Use of non-compliant video call hosting services to conduct calls which included discussions of CUI.

53. Relator knew from his prior security positions in the Defense Industrial Base and from his cybersecurity training and experience that each of these practices was in violation of one or more provisions of NIST SP 800-171 and DFARS 252.204-7012. Relator also knew that Morse's failure to implement any meaningful control over access to its information systems rendered the majority of the NIST SP 800-171 security requirements meaningless and unmet.

54. In or about April 2021, Relator learned that Morse had recently posted its cybersecurity self-assessment via DoD's Supplier Performance Risk System ("SPRS"). The Morse SPRS assessment was submitted and certified by Morse COO Torgerson. COO Torgerson told Relator that Morse had claimed to be in compliance with 106 of the 110 cybersecurity requirements set out in NIST SP 800-171. COO Torgerson remarked that the only reason he and CEO Kellas decided not to claim 100% cybersecurity compliance was "to avoid scrutiny" from DoD.

55. When Relator raised concerns that the Morse cybersecurity self-assessment was not accurate, COO Torgerson responded "you can blame me and Andreas" (referring to Morse CEO Kellas). COO Torgerson then related that Morse Head of IT Platt and Morse Information Systems Security Manager Fichera had raised similar concerns over Morse being out of compliance on most NIST SP 800-171 requirements but remarked that the two were "overruled" by himself and CEO Kellas.

56. Relator made repeated efforts in 2021 to convince Morse senior executives that the company needed to bring itself into actual compliance with NIST SP 800-171 and DFARS 252.204-7012. In the summer of 2021, Relator attempted to share authoritative guidance on the application of NIST SP 800-171 terms and requirements with COO Torgerson. COO Torgerson rejected that guidance in favor of the "more aggressive" interpretations he and CEO Kellas

preferred. Relator responded that Morse's "aggressive" interpretations were not good faith disagreements over the meaning of ambiguous terms. Relator also told COO Torgerson that Morse was not in compliance with most of the access control provisions of NIST SP 800-171.

57. In or about the late autumn of 2021, Morse co-founder Cohanim suggested adjusting access to Morse's information systems so that certain Morse applications would be available via the internet to individuals logging in using DoD credentials and access cards. Relator alerted Cohanim, CEO Kellas, and COO Torgerson that doing so would make it obvious to DoD personnel that Morse's information systems failed to comply with the cybersecurity requirements of NIST SP 800-171. In response, Relator was instructed to implement only those cybersecurity measures that would be obvious to DoD personnel who remotely logged into Morse's information systems, but to leave the majority of cybersecurity measures unimplemented.

58. In December 2021, Relator created a "CUI Path Forward" page on Morse's internal wiki site and presented it to COO Torgerson. The wiki page explained the regulatory risks for failure to comply with the applicable DFARS provisions and laid out a path to achieving actual compliance. That CUI Path Forward page included the recommendation that Morse hire an outside firm to audit its cybersecurity policies and practices. COO Torgerson disagreed with that suggestion, telling Relator that he (Torgerson) already knew that Morse failed to comply with the relevant NIST SP 800-171 measures, and asking why the company should hire an outside firm "if we already know what they're going to tell us?"

59. During Relator's 2021 performance review, COO Torgerson instructed Relator to stop putting critical information "in writing" when communicating with himself and other senior

Morse executives. COO Torgerson also told Relator not to bring concerns about Morse's cybersecurity failures directly to CEO Kellas.

60. Notwithstanding COO Torgerson's instructions not to bring concerns about cybersecurity matters directly to the CEO, in February 2022, Relator had a face-to-face discussion with CEO Kellas. During that discussion Relator expressed concern that Morse's chronic non-compliance with DoD's cybersecurity requirements was potentially putting the entire company at risk. Relator also observed that Morse had additional exposure because it had falsely represented that it was in compliance with NIST SP 800-171 in its 2021 SPRS assessment filing with the federal government.

61. In response, CEO Kellas voiced his disagreement over the need to fully comply with DoD's cybersecurity requirements and observed that Morse "never would have gotten off the ground" if it had followed every DFARS provision and every DoD regulation. CEO Kellas characterized Morse's disregard of NIST SP 800-171 cybersecurity requirements as a "business decision."

62. In the weeks following the February 2022 discussion with CEO Kellas, COO Torgerson expressed displeasure that Relator had discussed Morse's cybersecurity failures directly with CEO Kellas. Nevertheless, in the spring of 2022, Relator succeeded in convincing CEO Kellas and COO Torgerson to formally retain an outside auditor to evaluate Morse's cybersecurity policies and practices. Eventually the firm PFK O'Connor Davis (PFKOD) was retained to conduct that assessment. The assessment took place in the late spring and early summer of 2022 and was led by PFKOD Partner Nick DeLena.

63. In the early summer of 2022, Relator received his mid-year review from Morse co-founder Cohanim. Mr. Cohanim told Relator that he (Relator) needed to be "less stringent"

about DoD security requirements. When Relator voiced disagreement about being "less stringent," and shared an experience in which a former colleague at a different company lost his government clearances for failing to enforce all relevant DoD security requirements, Mr. Cohanim responded that the incident only proved that "everybody does it" with respect to non-compliance.

64. At the end of July 2022, PFKOD issued a written summary of its assessment of Morse's cybersecurity policies and practices. The PFKOD assessment confirmed that Morse had failed to implement 78% of cybersecurity measures required by NIST SP 800-171 and DFARS 252.204-7012.

65. The PFKOD assessment included a multipage spreadsheet which addressed each individual NIST SP 800-171 cybersecurity requirement and designated each one as "Implemented" or "Not Implemented." Most of those cybersecurity requirements were identified - in red font - as "Not Implemented."

66. Among other findings, the PFKOD assessment found that Morse had failed to implement eighteen of the twenty-two NIST SP 800-171 access control requirements, including the two basic requirements to limit system access to authorized users and devices and to limit access to types of transactions and functions that authorized users were permitted to execute.

67. The PFKOD assessment also found that Morse had failed to implement:

- Any of the requirements for audit and accountability;
- Any of the requirements for configuration management;
- Any of the requirements for incident response;
- Any of the requirements for security assessment;
- Nine of the eleven requirements for identification and authentication; and

- Nineteen of the twenty-three requirements for system and information integrity.

68. The PFKOD assessment also found that Morse failed to implement thirteen of the sixteen NIST SP 800-171 requirements for system and communications protection. Among other findings, the PFKOD assessment found that Morse had failed to implement the basic security requirement that it employ architectural designs, software development techniques, and systems engineering principles to promote effective information security within Morse.

69. On August 17, 2022, PFKOD Partner DeLena made an in-person presentation on the cybersecurity assessment at the Morse offices. The presentation was attended by COO Torgerson, Morse co-founder Cohanim, Chief Technology Officer Nelson, Relator, and other senior executives. CEO Kellas was invited to the presentation but did not attend. Relator believes CEO Kellas chose not to attend to avoid having PFKOD witness his (Kallas's) receipt and knowledge of the assessment finding Morse's failure to implement 78% of DoD's required cybersecurity measures.

70. None of the Morse executives who were in attendance at the August 17, 2022 presentation disputed or disagreed with any of the PFKOD findings.

71. During the August 17, 2022 presentation, COO Torgerson brought up the Morse self-assessment he had certified and posted with DoD SPRS (which assessment had falsely reported that Morse met 106 out of the 110 NIST SP 800-171 cybersecurity requirements). PFKOD Partner DeLena shared his opinion that Morse's immediate priority should be fixing all cybersecurity failures identified in the assessment.

72. To Relator's knowledge, most of the cybersecurity failures identified in the PKKOD assessment have still not been fixed, and neither COO Torgerson, nor anyone else from Morse, has taken steps to file an accurate Morse cybersecurity assessment with DoD SPRS.

Similarly, Morse made no efforts to adjust or refund any payments received from DoD. Instead, CEO Kellas, COO Torgerson, and other senior Morse executives continued to conceal Morse's noncompliance to avoid Morse's obligation to return payments to DoD for failing to comply with the terms of the underlying contracts.

73. In late August 2022, Morse senior executives held an in-house meeting to further discuss the results of the PFKOD assessment. CEO Kellas did attend the in-house meeting. In discussing the PFKOD assessment, CEO Kellas stated that he could accept the potential "risk" that the government might one day discover Morse's non-compliance with NIST SP 800-171 and the corresponding DFARS provisions. Relator responded that the upcoming DFARS/CMMC rules were going to require third-party audits of all DoD contractors, meaning that DoD's discovery of Morse's noncompliance was not a potential risk, but a certain eventuality.

74. In September 2022, Relator had a face-to-face conversation with CEO Kellas concerning the PFKOD assessment finding Morse out of compliance with 78% of the applicable cybersecurity requirements. During that conversation, Kellas repeated the statement that the noncompliance was simply "a business risk." Kellas also observed that he (Kellas) owned multiple residential rental units in the Cambridge area and stated that he disregarded many rental code requirements, a practice he viewed as a similar type of "business risk."

75. During the months following receipt of the PFKOD assessment, in the process of bidding on and receiving certain DoD subcontracts, Morse executives falsely certified Morse's compliance with DoD cybersecurity requirements to several prime contractors working on DoD matters.

76. In October 2022, COO Torgerson proposed a plan under which Morse would prepare a set of compliant cybersecurity policies but not implement those policies until just

before the next third-party audit, thereby allowing Morse to claim that its policies complied with the law, while not having to actually follow them. Relator advised against this plan.

77. In November 2022, COO Torgerson proposed a similar plan under which Morse would make itself "audit ready," then revert to its noncompliant cybersecurity practices until just prior to the next third-party audit. Relator again advised against that plan and explained to COO Torgerson that certain NIST SP 800-171 controls (such as vulnerability management or change management) required a continually generated body of data, meaning it would be readily apparent to any auditor that Morse was failing to comply with its policies in the time period leading up to the audit.

78. In late November 2022, a Morse employee improperly used a personal device to film what was initially believed to be classified Defense Advanced Research Projects Agency (DARPA) information. A subsequent investigation determined that the information was CUI, not classified.

79. In response to the incident involving mishandling of DARPA CUI, Relator and Contractor Program Security Officer DeWitt made the case that Morse needed to immediately impose a company-wide policy limiting the use of personal devices. CEO Kellas rejected that proposal. Instead, CEO Kellas decided to inform DoD that Morse maintained a company policy limiting use of personal devices, but to enforce the policy only as to the single DARPA program at issue.

80. In December 2022, Relator identified and acquired a mobile device application management system which could be used to secure mobile devices as required by NIST SP 800-171. The system was presented to CEO Kellas who decided to defer implementation until a time "closer to the audit."

A. Morse Made Repeated False Statements Concerning its Cybersecurity Practices and Policies to Obtain Tens of Millions of Dollars in DoD Contracts

81. Since in or before December of 2015, Morse has made repeated false statements to DoD concerning its cybersecurity practices and policies. Morse did so to fraudulently induce DoD to award it contracts worth many tens of millions of dollars when, in fact, Morse's failure to maintain basic cybersecurity measures to protect Controlled Unclassified Information made it ineligible to perform the required work.

82. Attached hereto as Relator's Exhibit 1 is a spreadsheet that identifies 30 separate contracts for which Morse – which has been assigned CAGE code number 78X46 – submitted offers to DoD between 2016 and 2022.[1] Morse was ultimately awarded each of those contracts, which have a combined value of more than $90 million.

83. Since December 30, 2015, the controlling DFARS provisions have clearly provided that whenever a contractor submitted a bid, proposal, or other offer to DoD, "the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 'Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations'…that are in effect at the time the solicitation is issued or as authorized by the contracting officer **not later than December 31, 2017** (emphasis added)." DFARS 204.7008(c)(1).

84. But Morse did not implement the NIST SP 800-171 security requirements by December 31, 2017. And Morse never intended to do so. As of January 2023, Morse still has not implemented most of those security requirements. Morse's willful disregard of those

---

[1] Relator is informed and believes that Morse has been awarded additional federal contracts between 2016 and the date of this complaint which are not included on Exhibit 1.

cybersecurity requirements continues to put highly sensitive Controlled Unclassified Information at risk of exfiltration, misappropriation, or theft.

85. Each bid, proposal, offer and similar submission by Morse to DoD since December 30, 2015 represents a separate false statement and false claim made by Morse to fraudulently obtain contracts with a combined value of more than $90 million.

B. Morse Provided DoD with False Cybersecurity Assessment Information

86. In or about April 2021, Morse posted its required cybersecurity self-assessment via DoD's Supplier Performance Risk System ("SPRS"). The SPRS assessment falsely reported that Morse was in compliance with 106 out of the 110 cybersecurity requirements set out in NIST SP 800-171. Morse COO Torgerson remarked that he and CEO Kellas decided not to claim 100% cybersecurity compliance "to avoid scrutiny" from DoD.

87. As CEO Kellas and COO Toreson knew, the cybersecurity self-assessment which Morse posted on the DoD SPRS was false. Morse was not, is not, and never has been in compliance with 106 out of the 110 cybersecurity requirements set out in NIST SP 800-171.

88. Even after receipt of a detailed report confirming that Morse was out of compliance with 78% of the cybersecurity measures required by NIST SP 800-171, neither CEO Kellas, COO Torgerson, nor any other Morse executive took steps to post an accurate cybersecurity self-assessment with DoD.

89. DoD established the SPRS program to be its "authoritative source" on supplier cybersecurity performance so it could address the "urgent need…to immediately begin assessing where vulnerabilities in its supply chain exist" and to "take steps to correct such deficiencies." Morse was replete with cybersecurity vulnerabilities and deficiencies. Rather than provide DoD with an accurate assessment of its cybersecurity policies and procedures, Morse simply lied and then attempted to justify that lie as a "business risk."

90. At the time the materially false Morse cybersecurity self-assessment was posted Morse was performing multiple sensitive DoD contracts involving significant volumes of CUI. Those contracts included, for example, an engineering services contract to test and evaluate artificial intelligence and machine learning for the U.S. Army with a contract value of $29.9 million.

91. Morse posted the materially false cybersecurity assessment so that the company could fraudulently claim it was entitled to tens of millions of dollars in payments from DoD when, in fact, Morse was in material breach of the terms of each of the underlying contracts.

C. Morse Made Repeated False Statements Concerning its Cybersecurity Practices and Policies to Prime DoD Contractors

92. Since in or before December of 2015, Morse has also made repeated false statements to DoD prime contractors concerning its cybersecurity practices and policies. Morse did so to fraudulently induce DoD prime contractors to award it subcontracts worth many millions of dollars when, in fact, Morse's failure to maintain basic cybersecurity measures to protect Controlled Unclassified Information made it ineligible to perform the required work. Morse further caused numerous prime contractors to file false and fraudulent statements and claims with DoD.

93. Attached hereto as Relator's Exhibit 2 is a spreadsheet that identifies 20 separate DoD subcontracts which Morse was awarded 2016 and 2022.[2] The identified subcontracts awarded to Morse have a combined value of more than $12 million.

---

[2] Relator is informed and believes that Morse has been awarded additional federal subcontracts between 2016 and the date of this complaint which are not included on Exhibit 2.

94. As stated above, since December 2015 the controlling DFARS provisions have clearly provided that whenever a contractor submitted a bid, proposal, or other offer to DoD, "the Offeror represents that it will implement the security requirements specified by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations"... that are in effect at the time the solicitation is issued or as authorized by the contracting officer **not later than December 31, 2017** (emphasis added)." DFARS 204.7008(c)(1).

95. Morse did not implement the NIST SP 800-171 security requirements by December 31, 2017. And Morse never intended to do so. As of January 2023, Morse still has not implemented most of those security requirements. For each DoD subcontract awarded to Morse since December 30, 2015, Morse caused the prime contractor to present one or more false claims, records, and/or statements to DoD.

96. To further ensure that each member of DoD's supply chain was in compliance with required cybersecurity measures, the DFARS were amended in September 2020 with the addition of DFARS clause 252-204-7020. That clause prohibited a DoD contractor from awarding a subcontract or other contractual instrument "unless the subcontractor has completed at least a Basic NIST SP 800-171 DoD Assessment for all covered contractor information systems." DFARS 252.204-7019(g)(2).

97. As is set forth above, the DoD assessment posted by Morse in April 2021 was knowingly false and failed to provide DoD with required information concerning Morse's actual cybersecurity policies and practices. As such, the assessment could not and did not satisfy the requirements of DFARS 252.204-7019(g)(2).

98. Even after receipt of a detailed report in July 2022 confirming that Morse was out of compliance with 78% of cybersecurity measures required by NIST SP 800-171, Morse executives continued to falsely represent to prime contractors that Morse was in compliance with cybersecurity measures required by DoD. Morse did so to fraudulently induce prime contractors to award Morse millions of dollars in subcontracts, which subcontracts were expressly prohibited under the DFARS.

D. Morse Sold and Supplied Vulnerable and Unsecure Software to DoD

99. Since in or before December 2015, Morse has pursued and been awarded multiple contracts to design and deliver highly sophisticated software for DoD. Examples include software to operate the airdrop.mil website developed for the U.S. Army and the "Themis" software developed for the Joint Artificial Intelligence Center (JAIC). Each of the controlling DoD contracts required that Morse perform the software design work in compliance with the cybersecurity requirements of NIST SP 800-171

100. Morse, however, failed to develop, implement, or employ software development techniques, architectural designs, or system engineering principles to promote effective information security within the organization as required by NIST SP 800-171. Morse software developers could, and did, incorporate existing software programs gathered from multiple open sources without regard to the security vulnerabilities of those programs. As a result, Morse sold and supplied vulnerable and unsecure software to DoD.

101. Each resulting Morse invoice or other request for payment submitted under any DoD contract awarded since December 30, 2015 represents a separate false claim.

E. Damages to the Government

102. As summarized above, Morse has been awarded prime DoD contracts with a combined value of more than $90 million. Morse has been awarded additional DoD subcontracts

with a combined value of more than $12 million. Those sums were intended to compensate and support DoD contractors and subcontractors that implemented and maintained required cybersecurity measures. Morse falsely and fraudulently claimed to be such a contractor/subcontractor when, in fact, it willfully and intentionally disregarded DoD's required cybersecurity standards. DoD has been defrauded out of a basic benefit it bargained for in awarding and approving the $90 million in prime contracts and $12 million in subcontracts.

103. DoD has likewise purchased vulnerable and unsecure Morse software costing many millions of dollars which was developed in violation of DoD's cybersecurity requirements. Remediation and/or replacement of Morse's deficient software can be expected to cost the Government many millions of dollars in additional and unnecessary expenses.

104. Morse and its senior executives brazenly disregarded basic cybersecurity measures for information systems used to store, process, and transmit significant volumes of CUI, including CUI relating to some of the country's most sensitive ongoing defense programs and projects. Morse failed to maintain required access logs for those information systems, meaning there may be no way to ever determine how much CUI entrusted to Morse was exfiltrated, misappropriated, or stolen. The final damage to the Government for Morse's cybersecurity failures is unquantifiable.

VI. CLAIMS FOR RELIEF

Count I

Federal False Claims Act – False Claims
31 U.S.C. § 3729(a)(1)(A)

105. Relator realleges and incorporates by reference the allegations contained in the foregoing paragraphs as though fully set forth herein.

106. This is a claim for treble damages and penalties under the False Claims Act, 31 U.S.C. §§ 3729, *et seq*. as amended.

107. The FCA, 31 U.S.C. § 3729(a)(1)(A), creates liability for a person who "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval." Defendants have repeatedly violated this provision of the FCA.

108. The Government, unaware of the falsity of all such claims made or caused to be made by Defendants, has paid, and continues to pay such false or fraudulent claims that would not be paid but for Defendants' illegal conduct.

109. By reason of Defendants' acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

110. Additionally, the United States is entitled to the maximum statutory penalty for each and every violation alleged herein.

Count II

Federal False Claims Act – False Records or Statements
31 U.S.C. § 3729(a)(1)(B)

111. Relator realleges and incorporates by reference the allegations contained in the foregoing paragraphs as though fully set forth herein.

112. This is a claim for treble damages and penalties under the False Claims Act, 31 U.S.C. §§ 3729, *et seq*. as amended.

113. The FCA, 31 U.S.C. § 31 U.S.C. § 3729(a)(1)(B), creates liability for a person who "knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim." Defendants have repeatedly violated this provision of the FCA.

114. The Government, unaware of the falsity of the records, statements, and claims made or caused to be made by Defendants, has paid and continues to pay claims that would not be paid but for Defendants' illegal conduct.

115. By reason of Defendants' acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

116. Additionally, the United States is entitled to the maximum statutory penalty for each and every violation alleged herein.

Count III

Federal False Claims Act – Reverse False Claims
31 U.S.C. § 3729(a)(1)(G)

117. Relator realleges and incorporates by reference the allegations contained in the foregoing paragraphs as though fully set forth herein.

118. This is a claim for treble damages and penalties under the False Claims Act, 31 U.S.C. §§ 3729, *et seq.* as amended.

119. The FCA, 31 U.S.C. § 3729(a)(1)(G), creates liability for any person who "knowingly makes, uses, or causes 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 conceals or knowingly and improperly avoids or decreases, an obligation to pay or transmit money or property to the Government." Defendants have repeatedly violated this provision of the FCA.

120. The Government, unaware of Defendants' violation of this provision, has not made demand for or collected the years of overpayments due from the Defendants.

121. By reason of Defendants' acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

122. Additionally, the United States is entitled to the maximum statutory penalty for each and every violation alleged herein.

Count IV

Federal False Claims Act – Conspiracy
31 U.S.C. § 3729(a)(1)(C)

123. Relator realleges and incorporates by reference the allegations contained in the foregoing paragraphs above as though fully set forth herein.

124. This is a claim for treble damages and penalties under the False Claims Act, 31 U.S.C. §§ 3729, *et seq.*, as amended.

125. By and through the acts described above, Defendants conspired to commit violations of 31 U.S.C. § 3729(a)(1)(A) by agreeing and conspiring among themselves to present and cause to be presented, one or more false or fraudulent claims for payment or approval.

126. By and through the acts described above, Defendants conspired to commit violations of 31 U.S.C. § 3729(a)(1)(B) by agreeing and conspiring among themselves to make, use and cause to be made or used, one or more false records or statements material to a false or fraudulent claim.

127. By and through the acts described above, Defendants conspired to commit violations of 31 U.S.C. § 3729(a)(1)(G) by agreeing and conspiring to make, use and cause to be made or used, one or more false records or statements material to an obligation to pay or transmit money or property to the Government, and by agreeing and conspiring to conceal and to knowingly avoid or decrease and obligation to pay or transmit money or property to the Government.

128. The Government, unaware of the Defendants' conspiracy and fraudulent schemes, has paid and continues to pay claims that would not be paid but for Defendants' illegal conduct and has not made demand for or collected the years of overpayments due from the Defendants.

129. By reason of Defendants' acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

130. Additionally, the United States is entitled to the maximum statutory penalty for each and every violation alleged herein.

VII. PRAYERS FOR RELIEF

WHEREFORE, Relator prays for judgment against Defendants as follows:

A. That Defendants are enjoined from violating the Federal False Claims Act, 31 U.S.C. §§ 3729, *et seq.*;

B. That judgment be entered against Defendants and in favor of the United States and the Relator in an amount equal to three times the amount of damages caused by Defendants' misconduct, as well as a civil penalty for each FCA violation in the maximum statutory amount;

C. That Defendants be ordered to disgorge all sums by which they have been enriched unjustly by its wrongful conduct;

D. That judgment be granted for Relator against Defendants for all costs and expenses, including, but not limited to, court costs, litigation costs, expert fees, and all attorneys' fees permitted under 31 U.S.C. § 3730(d).

E. That Relator be awarded the maximum amount permitted under 31 U.S.C. § 3730(d);

F. That the Court award such other relief as the Court deems proper.

JURY DEMAND

Pursuant to Federal Rule of Civil Procedure 38, Relator requests a jury trial.

January 19, 2023

Respectfully submitted,

/s/ David W. S. Lieberman

David W.S. Lieberman BBO #673803
Bruce C. Judge (CA Bar No. 148805)
Whistleblower Law Collaborative LLC
20 Park Plaza, Suite 438
Boston, MA 02116-4334
(617) 366-2800
Fax: (888) 676-7420
david@whistleblowerllc.com
bruce@whistleblowerllc.com

Counsel for Plaintiff-Relator

Contract No.	Agency	Sub-Agency	Description	Start Date	End Date	Status	Obligated Amount	Potential Amount
47QFNA20F0084	GSA	Federal Acquisition Service	Aerial Delivery SW Development	8/25/20	8/24/25	In progress	$4,982,509	$21,712,423
47QRAA18D00A1	GSA	Federal Acquisition Service	Federal Supply Schedule Contract	5/31/18	5/30/23	In progress	$8,236,870	$29,543,141
FA8656621DA033	DOD	U.S. Air Force	Eglin Wide Agile Acquisitions Contract	9/23/21	9/9/31	In progress	$1,000	$1,000
W15QKN19F0879	DOD	Army	Procurement of JPADS Base Year Services	9/24/19	8/15/23	In progress	$2,604,837	$6,132,445
W15QKN19F0973	DOD	Army	Parachute Navigation System Post Production Software Support	9/25/19	8/31/25	In progress	$649,522	$1,698,272
W911QX19C0029	DOD	Army	Advanced Test and Evaluation (T&E) for the exponential pace of artificial intelligence/Machine Learning (AI/ML) Progress	8/26/22	8/31/23	In progress	$3,195,692	$44,890,536
W911QY19C0042	DOD	Army	Research and Development	6/4/19	6/4/24	In progress	$1,995,067	$4,285,449
W911QY20C0088	DOD	Army	Research and Development	8/24/20	8/23/25	In progress	$9,477,937	$9,750,000
W911QY22PO081	DOD	Army	National Security Covered Action - R&D Effort to Further Determine Capability to Meet Mission	5/20/22	12/31/22	In progress	$248,657	$248,657
FA865019C7915	DOD	U.S. Air Force	Rapid Warfighter Exfiltation	2/8/19	8/31/20	completed	$1,063,287	$1,063,287
FA865621FA027	DOD	U.S. Air Force	Manufacturing ammunition	9/23/21	10/22/21	completed	$1,000	$1,000
HR001116C0086	DOD	Defense Advanced Research Projects Agency	Research and Development: Defense Other	6/17/16	12/14/20	completed	$7,047,945	$7,047,945
HR001119C0093	DOD	Defense Advanced Research Projects Agency	High Agility Terrain Flight Simulation	6/4/19	12/4/19	completed	$483,710	$483,710
HR001122C0046	DOD	Defense Advanced Research Projects Agency	E014042 Rapid Assembly Paramotor for tactical operator relocation (RAPTOR) SBIR Phase II Base	11/24/21	11/30/23	completed	$500,000	$1,500,000
W52P1J21C0014	DOD	Army	Project Gargoyle - JAIC	1/1/21	12/31/21	completed	$2,749,089	$2,749,089
W52P1J21C0034	DOD	Army	Themis Test Harness for AI	8/30/21	8/29/22	completed	$1,498,372	$1,498,372
W911NF19C0101	DOD	Army	Novel Artificial Intellegence (AI)/Machine Learning (ML) Test & Evaluation (T&E) and Ensembling	9/30/19	9/30/22	completed	$29,932,547	$29,932,547
W911QX19C0023	DOD	Army	Base: Test and Evaluation JAIC PMX	9/4/19	7/25/21	completed	$2,500,277	$2,500,277
W911QY16PO268	DOD	Army	Morse Corp SBIR I, IGF: OT:IGF	9/12/16	10/31/18	completed	$149,999	$149,999
W911QY17C0014	DOD	Army	Morse Corp BAA - Base Effort	4/18/17	10/31/22	completed	$5,812,480	$6,353,949
W911QY18C0120	DOD	Army	Obfuscating Film (POOF)	4/27/18	10/31/20	completed	$999,998	$999,998
W911QY18PO288	DOD	Army	Meets requirements of classifed J&A	9/28/18	8/19/19	completed	$49,500	$49,500
W911QY19C0042	DOD	Army	Research and Development	6/4/19	6/4/24	completed	$1,995,067	$4,285,449
W911QY19C0073	DOD	Army	JPADS Mission Planner ATAK Plugin	8/1/19	1/14/22	completed	$2,242,500	$2,242,500
W911QY20C0085	DOD	Army	Obfuscating Film (POOF)	9/11/20	10/31/21	completed	$1,194,053	$1,194,053
W911QY21C0077	DOD	Army	Equipment	5/18/21	12/31/21	completed	$714,600	$714,600
W911QY21C0104	DOD	Army	Equipment	8/16/21	12/31/21	completed	$308,100	$308,100
W911QY22PO011	DOD	Army	Specialized Equipment	12/13/21	1/31/22	completed	$49,600	$49,600
W911QY22PO121	DOD	Army	Cargo Delivery System	7/29/22	9/1/22	completed	$20,329	$20,329
						Totals:	$90,704,544	$181,406,227

EXHIBIT 1

Sub Contract No.	Prime Contract Number	Prime Contractor	Agency	Sub-Agency	Description	Start Date	End Date	Status	Amount
97088	HR0011-21-C-0058	Aerovironment	DOD	DARPA			10/28/2023	In progress	$1,678,814
10P0-3717	FA873021F0066	Tapestry (Boeing)	DOD	U.S. Air Force	Engineering Services	9/30/2022	7/7/2023	In progress	$1,090,343
41-7051515	FA252121F0178	Bae	DOD	U.S. Air Force	SUAST Phase 2	6/4/21	1/31/23	In progress	$90,054
41-7052860	FA252121F0178	Bae	DOD	U.S. Air Force	Subcontractor services ETS1147RT PDPAS phase 3-4	6/4/21	1/31/23	In progress	$150,340
41-7053109	FA252121F0178	Bae	DOD	U.S. Air Force	Subcontractor services-enhanced optical video scoring IAW	6/4/21	1/31/23	In progress	$150,015
41-7058599	FA252122F0041 (child of Award FA252120D005)	BAE	DOD	U.S. Air Force	Unified data management study IAW proposal dated 03-11-2022	4/7/2022	9/30/2025	In progress	$150,127
41-7061809	FA252122F0041 (child of Award FA252120D005)	BAE	DOD	U.S. Air Force	GPS denied RF ranging radio AOA	8/12/2022	9/30/2025	In progress	$152,972
41-7061810	FA252122F0041 (child of Award FA252120D005)	BAE	DOD	U.S. Air Force	Data as a services (DAAS) architecture-consolidation and dev	8/11/2022	9/30/2025	In progress	$300,061
41-7062240	FA252122F0041 (child of Award FA252120D005)	BAE	DOD	U.S. Air Force	Transmission quality metric calculations	8/29/2022	9/30/2025	In progress	$112,420
41-7062240	FA252122F0041 (child of Award FA252120D005)	BAE	DOD	U.S. Air Force	Transmission quality metric calculations	9/8/2022	9/30/2025	In progress	$112,420
41-7062485	FA252122F0041 (child of Award FA252120D005)	BAE	DOD	U.S. Air Force	Sensor fusion architecture design	9/8/2022	9/30/2025	In progress	$100,477
2458-17-0001	FA873017F0095	Tapestry (Boeing)	DOD	Defense Contract Mgmt Agency	Providing software development support and services to tap	4/7/2020	6/6/2021	completed	$421,078
SUB1230010-002	FA873021F0154	Jacobs Tech.	DOD	U.S. Air Force	Mission planning support aircraft agile efforts	9/1/2021	11/1/2022	completed	$1,875,349
SUB1237510-003	FA460006D0003_97000	Alion	DOD	U.S. Air Force	Protype undersea systems	5/2/2016	12/29/2016	completed	$256,800
SUB1237510-004	FA460006D0003_97000	Alion	DOD	U.S. Air Force	The on demand drop task effort will provide a web-based logistics tracking system	6/30/2016	12/29/2016	completed	$196,460
SUB1237510-005	FA460006D0003_97000	Alion	DOD	U.S. Air Force		10/3/2016	12/29/2016	completed	$2,466,629
SUB1244305-001	FA807514D0014_9700	Alion	DOD	U.S. Air Force	Software engineering for guided parafoil systems	6/15/2017	9/20/2021	completed	$1,265,040
19000845	W911QX-18-C-0037	ECS Federal	DOD	Army					$300,000

EXHIBIT 2

SUB1260205-001	FA8075-18-D-002	Alion		U.S. Air Force					$700,779
	FA8730-21-C-0035	Tapestry (Boeing)		U.S. Air Force					$564,134
								Totals:	$12,134,312

EXHIBIT 2