THYBERGLAW
GREGORY A. THYBERG SBN102132
3104 O STREET #190
SACRAMENTO, CALIFORNIA 95816
TEL: (916) 204-9173
greg@thyberglaw.com

ATTORNEYS FOR RELATOR, BRIAN MARKUS

UNITED STATES DISTRICT COURT

FOR THE EASTERN DISTRICT OF CALIFORNIA

UNITED STATES OF AMERICA: *ex rel.* BRIAN MARKUS Plaintiffs, vs. AEROJET ROCKETDYNE HOLDINGS, INC., a corporation and AEROJET ROCKETDYNE, INC. a corporation. Defendants	Civil Action No. 2:15-cv-2245 WBS-AC SECOND AMENDED FALSE CLAIMS ACT COMPLAINT AND DEMAND FOR JURY TRIAL

I. Introduction

1. Brian Markus (the "relator") brings this action on behalf of the United States of America against defendants AEROJET ROCKETDYNE HOLDINGS, INC. ("ARH") and AEROJET ROCKETDYNE INC. ("AR") for treble damages and civil penalties arising from defendants' false statements and false claims in violation of the

Civil False Claims Act, 31 U.S.C. §§ 3729 *et seq.* The violations arise out defendants fraudulently inducing the federal government to grant them contracts to provide goods and services to the federal government including, the National Aeronautics and Space Administration ("NASA") and the Department of Defense ("DOD"), when they knew they were not complying with federal acquisition regulations that were required as a material terms of those contracts.

2. As required by the False Claims Act, 31 U.S.C. § 3730(b)(2), the relator served the Attorney General of the United States and to the United States Attorney for the Eastern District of California a statement of all material evidence and information related to the complaint. This disclosure statement is supported by material evidence known to the relator at his filing establishing the existence of defendants' false claims. Because the statement includes attorney-client communications and work product of relator's attorneys, and is submitted to the Attorney General and to the United States Attorney in their capacity as potential co-counsel in the litigation, the relator understands this disclosure to be confidential.

3. On June 6, 2018, the United States Government filed a Notice indicating it was declining to intervene in this action. Relator continues this action on behalf of himself and the United States Government.

II. Jurisdiction and Venue

4. This action arises under the False Claims Act, 31 U.S.C. §§ 3729 *et seq.* This Court has jurisdiction over this case pursuant to 31 U.S.C. §§ 3732(a) and 3730(b).

This court also has jurisdiction pursuant to 28 U.S.C. § 1345 and 28 U.S.C. § 1331.

5. Venue is proper in this District pursuant to 31 U.S.C. § 3732(a), because the acts proscribed by 31 U.S.C. §§ 3729 *et seq.* and complained of herein took place in this district, and is also proper pursuant to 28 U.S.C. § 1391(b) and (c), because at all times material and relevant, defendants transact and transacted business in this District.

Parties

6. Relator Brian Markus ("MARKUS") is a citizen of the United States and a resident of the State of California. From to June 30, 2014 to September 14, 2015, relator worked for defendants as the senior director of Cyber Security, Compliance & Controls. The relator brings this action based on his direct, independent, and personal knowledge and also on information and belief.

7. Defendants AEROJET ROCKETDYNE HOLDINGS, INC. ("ARH") and AEROJET ROCKETDYNE, INC. ("AR") are in the business of developing and manufacturing products for the aerospace and defense industry including aerospace propulsion systems, precision tactical weapons systems, and armament systems including warhead and munitions applications. Defendants' primary customers for these products are the United States government who purchases these products pursuant to contracts defendants entered with the federal government including the Department of Defense ("DOD") and the National Aeronautics and Space Administration ("NASA").

8. Defendant AR is a wholly owned subsidiary of ARH. ARH uses AR to perform its contact obligations. AR and ARH share computer systems, and have common

corporate officers that oversee the management of both corporations in performing the federal contracts which are the subject of this false claims action as such both defendants are jointly and severally liable for the conduct alleged herein.

III. Facts Common to All Counts

A. Background

9. United States government contracts are subject to Federal Acquisition Regulations ("FAR"). There are also agency specific regulations that supplement FAR. Contracts entered with the Department of Defense ("DOD") are subject to Defense Federal Acquisition Regulations ("DFARS") and contracts entered with the National Aeronautics and Space Administration ("NASA") are subject to NASA Federal Acquisition Regulations ("NASA FARS")

10. The federal government requires that all companies that enter contracts to provide good or services to the DOD or NASA meet minimum standards to prevent unauthorized access and disclosure of unclassified controlled technical information ("UCTI") or sensitive but unclassified information ("SBU") belonging to NASA or the DOD that will be stored on the company's computer system in the course of the company performing the government contract. These minimum standards are set forth in the DFARS and NASA FARS regulations and apply to all federal contracts where the contractor will have access to UCTI or SBU belonging to the federal government.

11. Prior to November 18, 2013, the federal government ensured compliance with these regulations by incorporating terms in federal contracts setting minimum levels of cyber security to make sure that contractors' information systems were protected from unauthorized access. Contractors were required to meet the minimum standards for cyber security set forth in the DFARS and NASA FARS regulations in order to be awarded a

government contract where they would have access to UCTI or SBU belonging to the federal government.

12. The DFARS and NASAFARS regulations required that contactors meet cyber security standards standards specified by the National Institute of Standards and Technology ("NIST"). Contracting officers at NASA and the DOD were required to review contracts to see if there would be access to UCTI or SBU and to insert terms in the contract to make sure the DFARS and NASA FARS regulations relating to cyber security were incorporated as a term of the contract. In the case of the DOD, the agency would prepare a form DD-254 that was incorporated in the contract

13. On November 18, 2013, the DOD issued a regulation, 78 Fed. 69,273, ("DOD REG") which intensified the safeguards required by government defense contractors to protect their computer systems from cyber attacks that could result in unauthorized access and disclosure of UCTI belonging to the federal government.

14. UCTI according to the DOD REG, included computer software as defined by DFARS Clause 252.227-7013 with a military or space application that is subject to DOD access controls. Technical information included engineering data, drawings, specifications, standards and technical reports.

15. The DOD REG, which was effective immediately imposed two requirements: (1) that contractors provide adequate security for information systems that contain unclassified controlled technical information; and (2) that they report cyber incidents or any compromise of information systems.

16. The DOD REG required that all federal contracts with the DOD going forward incorporate DFARS Clause 252.704-7012. This clause was required in any contract with the government where the contractor would have access to UCTI belonging to the federal government.

17. The DOD REG required that contractors and subcontractors working on these federal DOD contracts meet the minimum cyber security safeguards set forth in DFARS Clause 252.704-7012.

18. DFARS Clause 252.704-7012 required that contactors meet the standards specified by the NIST Special Publication 800-53. The rule required that contractors implement 51 controls covering 14 areas of cyber security.

19. In the event a contractor was deficient in meeting the NIST 800-53 standards in any respect, they were required to contact the government-contracting officer and advise them of the deficiency and explain to the contracting officer how they would be able to meet the standard through alternative means.

20. The NIST SP 800-53 standards were originally implemented to apply to contractors operating computer systems on behalf of the federal government. In June of 2015 the DOD and NIST published a new set of rules specifically tailored to defense contractors storing controlled unclassified technical information on defense contractor computer systems, NIST 800-171. NIST 800-171 incorporated 109 cyber security controls from the NIST 800-53 standard.

21. In August 2015 the DOD issued an interim rule modifying DFARS Clause 252.704-7012. Under the modified rule defense contractors were only required to meet the NIST 800-171 cyber security standards, which were less stringent than the requirements of NIST 800-53. When the NIST 800-171 standards were not met the clause required that defense contactors provide: "Alternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection approved in writing by an authorized representative of the Department of Defense Chief Information Officer ("DoD CIO") prior to contract award."

22. The DOD amended the interim DFARS Clause 252.704-7012 effective December 31, 2015. The new rule required contractors be fully compliant with the NIST 800-171 standards as soon as practical but not later than December 31, 2017. For all contracts awarded prior to October 1, 2017, the contractor was required to notify the DoD CIO via email within 30 days of the contract award, of any security requirements specified by NIST SP 800-171 not implemented at the time of contract award.

23. The contractor was required to submit requests to vary from the NIST SP 800-171 standards in writing to the DoD CIO. The contractor was only excused from a security control if it was "adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place."

24. Every operative version of DFARS Clause 252.704-7012 required that contractors provide "Adequate Security" to protect UCTI on their system from unauthorized disclosure. The clause stated "Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."

25. Contractors awarded contracts from NASA must comply with NASA FAR regulations. NASA FARS 1852.204-76 requires that 264 of the NIST SP 800-53 moderate control be incorporated in NASA contracts where the contractor would store sensitive but unclassified information (SBU) belonging to the federal government on their computer system while performing a contract for NASA. This regulation makes no provision for the contractor use alternative controls or protective measures.

26. NASA FARS 1804.470-4(a) requires that this clause incorporated in every NASA contract where the contractor has access to or stores SBU belonging to the federal

government on its computer system. NASA FARS 1852.204-76 states in pertinent part: " (a) The contractor shall protect the confidentiality, integrity, and availability of NASA Electronic Information and IT resources and protect NASA Electronic Information from unauthorized disclosure. (b) This clause is applicable to all NASA contractors and sub-contractors that process, manage, access, or store unclassified electronic information, to include Sensitive But Unclassified (SBU) information, for NASA in support of NASA's missions, programs, projects and/or institutional requirements."

27. Government contracting officers have no authority to enter a contract unless the contractor is complying with DFARS and NASA FARS regulations that are legally required to be incorporated in the contract. 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."

28. Compliance with DFARS and NASA FARS regulations that are that are required by law to be incorporated in a federal contracts are non-waiverable contract terms. According to FAR 1.602-3 (c) (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."

B. Wrongful Acts by Defendants

29. Defendants have entered multiple contracts with the federal government, and as subcontractors on contracts with the federal government, which required that defendants meet the cyber security standards set forth in the DFARS Clause 252.704-7012 and NASA FARS Clause 1852.204-76 even though defendants knew their information systems did not meet these cyber security requirements.

30. Defendants fraudulently entered contracts knowing they did not meet the minimum standards required to be awarded a contract and they misled the government concealing their non-compliance with these regulations.

31. Defendants also fraudulently entered subcontracts with prime contractors who were working on federal contracts that required that they comply with the DFARS and NASA FARS cyber security regulations.

32. MARKUS started working for defendants on June 30, 2014 as the senior director of Cyber Security, Compliance & Controls. He was hired by AR to improve the cyber security of defendants' computer systems.

33. Relator was promised a budget of 10 to 15 million dollars to improve the security of defendants' computer systems. He was promised an internal staff of 5 to 10 employees and external staff of up to 25 contract employees.

34. When relator started working for defendants, he was given a budget of only 3.8 million dollars rather than 10 million. Defendants provided an internal staff of two employees not the five to ten that were promised. Instead of twenty-five contract employees, defendants provided only seven.

35. Relator found that defendants were understaffed and under budgeted to provide the level of cyber security that was required by the federal acquisition regulations for contractors granted access to UCTI or SBU belonging to the federal government.

36. When relator started working for defendants, he found that their computer systems failed to meet the minimum cyber security requirements required by the federal government to be awarded contracts funded by the DOD or NASA.

37. Relator had previously worked in the area of cyber security for other defense contractors and so he was familiar the federal acquisitions regulations related cyber security.

38. Defendants were not compliant with the NASA FARS or DFARS cyber security requirements including DFARS Clause 252.704-7012 and NASA FARS Clause 1852.204-76 when relator started his employment June 30, 2014. Based on the state of defendants' computer systems at the time relator began his employment, relator is informed and believes thereon alleges defendants' computer systems had not been compliant with the DFARS or NASA FARS cyber security requirements for several years.

39. In 2013, ARH purchased Rocketdyne from Pratt & Whitney. At the time of the purchase Pratt & Whitney represented that its Rocketdyne division was compliant with the DFARS and NASA FARS regulations related to cyber security. After the purchase, the computer systems of Rocketdyne were merged with defendants' computer systems so that after 2013, Rocketdyne was no longer compliant with the NASA FARS 1852.204-76 or DFARS Clause 252.704-7012 cyber security requirements.

40. Defendants' were aware of breaches of their computer system in 2013 and 2014 by nation state sponsored threat actors. Defendants reported those breaches to the federal government in as required by DFARS regulations and DFARS Clause 252.704-

7012. In reporting those breaches defendants concealed the fact that their computer system was not compliant with the NASAFARS 1852.204-76 or DFARS Clause 252.704-7012 cyber security requirements.

41. When questioned by the government about its cyber security, defendants gave the government misleading information. For example, they were asked if they had a certain piece of security equipment, they would say "yes," even though the equipment was sitting in a box and not connected to their computer system. Defendants represented they had cyber security software/hardware installed to protect the systems when in reality the software/hardware in question only covered part of the environment leaving defendants vulnerable to a cyber attack. In some cases, they claimed compliance only considering the primary control and not the sub-controls, which were clearly not being met.

42. At the time of the 2014 cyber security breach of its computer system, AR was working was working on a DOD contract through the prime contractor Lockheed Martin to supply the booster motor technology for the Terminal High Altitude Area Defense System ("THAAD"). The THAAD system is used to defend the United States and deployed forces and allies against ballistic missiles during all phases of flight. UCTI related to THAAD system was exposed to disclosure as a result of this computer breach.

43. In early 2014, Emagined Security Inc. ("EMAGINED"), an outside consulting firm, performed an audit to determine NASA FARS and DFARS compliance and determine costs to obtain compliances. It was found that defendants were less than 25% compliant.

44. In January 2015, relator was requested to prepare a report for ARH board of directors meeting regarding AR'S and ARH'S computer systems compliance with the DFARS and NASAFARS cyber security requirements.

45. Relator prepared a presentation to be presented to the Board, which showed that defendants' computer system was not DFARS or NASA FARS compliant. Relator's report to be submitted to the Board indicated that defendants' computer system was unpatched, misconfigured, outdated and thus vulnerable to a cyber attack.

46. When AR'S president Warren Boley ("BOLEY") became aware that relator intended tell the Board that defendants were not DFARS or NASA FARS compliant, he took over relator's presentation and changed it. Relator is informed and believes and thereon alleges that BOLEY concealed from the Board that defendants were not in compliance with DFARS and NASA FARS cyber security requirements.

47. Defendants' federal contracts required that they be 100% compliant with the NASA FARS and DFARS cyber security requirements. Relator's team prepared a slide to be presented to the Board, which showed defendants' compliance related to four key areas for which DFARS required 100% compliance, WINDOWS, DMZ, UNIX and NETWORK. Defendants' compliance values in these areas ranged from 6% to 20%. This slide was removed from the Board presentation along with other slides that demonstrated the extent of defendants' failure to comply with federal regulations related to cyber security that were required by defendants' contracts with the federal government.

48. Defendants' management was well aware prior to January 2015 that they were out of compliance with the DFARS and NASA FARS cyber security requirements as relator provided AR and ARH'S top management, including the President, CEO and Chief Information officer weekly and monthly reports beginning July 2014 advising them of the state of AR and ARH'S compliance with DFARS and NASA FARS requirements. There were also a number of presentations made to multiple officers of AR and ARH prior to January 2015 regarding defendants' lack of compliance the DFARS and NASA FARS cyber security regulations.

49. After the January 2015 board meeting, the Board ordered an audit of AR and ARH'S cyber security posture using Ernest & Young ("EY"). In addition, the Senior Leadership tasked Jose Ruiz (CIO) to update the compliance documents as it was a becoming dated and needed to reflect actual costs and DFARS and NASA FARS compliance levels.

50. Incremental updates to the DFARS/NASA FARS compliance documents were created and provided regularly to defendants' leadership. EMAGINED conducted a second formal audit in July 2015 and submitted their report in September 2015. EMAGINED identified numerous security gaps in defendants' computer systems.

51. EMAGINED found defendants were only 23.9% compliant NASA NIST SP 800-53 moderate controls, 21.8% compliant with NASA NIST SP 800-171 controls and 27.8% compliant with the pre August 2015 DFARS controls. In order to participate in government contracts and bill for their services, defendants were required to be 100% compliant with these regulatory requirements.

52. The EMAGINED report indicated that for defendants to reach 100% compliance would take a combination of technical solutions, business process improvements and a fundamental change in defendants' strategic direction. EMAGINED stated for defendants to achieve compliance "… will require a shift in how the business addresses contractual and regulatory responsibilities…" The report outlined estimated costs in the amount of $34,548,866 over a five-year period, which would be required for defendants' to make their computer systems compliant with the DFARS cyber security requirements. AR was considering outsourcing its IT department but the EMAGINED report indicated that this would only clear up 10% of the compliance deficiencies.

53. The EMAGINED report was so critical of defendants' failure to meet federal regulatory cyber security requirements that defendants forced EMAGINED to rewrite their final report to omit much of the critical language in its initial report.

54. In April 2015, Ernest & Young ("EY") did an assessment of the vulnerabilities of defendants' computer systems to hackers. Within four hours the EY team was able to utilize vulnerabilities in defendants' computer system to fully compromise the windows network and retrieve all defendants' user accounts and passwords. Information accessed included the CEO and CFO'S inbox and network files that included board strategy documents and merger and acquisition files and technical documents. Employee personal information was accessed including social security numbers and salary.

55. The EY assessment team was able to access legal documents including access to "eCase viewer" which allowed access to attorney client information. With regard to the federal contracts defendants were working on the assessment team was able to get access to emails and files for engineering documents, which contained design documents for rockets and other unclassified controlled technical information belonging to the federal government.

56. The EY assessment team was also able to compromise the computer system so they could access physical security files and folders and they were able to remotely access defendants' security cameras so they could view and listen to security camera footage. This activity was not detected by defendants and remained undetected for seven days.

57. The EY assessment team identified five unique pathways to compromise defendants' system. Defendants' systems contained publically known information system vulnerabilities, which are typically patched as part of an organization's threat and

vulnerability management program. Defendants ignored the Senor Director of Cyber Security's recommendations to patch and secure the systems.

58. In order to secure new contracts, defendants' contracts department had to represent to the federal government that they were compliant with NASA FARS, DFARS, requirements.

59. AR sent a letter dated September 18, 2014 to government contract negotiator Patrisha Conroy regarding its compliance with DFARS Clause 252.204-7012 as part of its proposal to secure contract award FA8650-14-C-7424 a contract with the Air Force valued at $8,326,290.

60. AR advised the government that they were compliant with the majority of the DFARS Clause 252.204-7012 requirements when they were only 24% compliant with the NIST SP 800-53 moderate controls they were required to have in place. AR just reported their 60 of the top controls to make it appear they were close to compliant but did not report its status on the full 264 controls that would have revealed they were 75% non-compliant.

61. AR told the government it had 43 controls that it described in the letter as "Controls in Place Enhancements and Refinement on-On-going." In its letter AR advised the government "AR has implemented the control(s) but needs to implement enhancements to strengthen the controls as necessary." This statement was false and misleading because none of the 43 controls listed was compliant with the NIST SP 800-53 controls that were required by DFARS Clause 252.204-7012.

62. At the time this statement was made, AR was representing a control was in place when it was only in place at one facility. AR was representing the firewalls were installed but they were installed at only one location, or the firewall in place was not working because it was misconfigured.

63. AR was represented that 6 controls had partial a controls in place. AR referred to these controls as 'Partial Controls in place Strengthening, Enhancements and Refinement On-going/needed" for which AR stated: "AR had implemented the control(s) to a degree but needs to investigate further on how to satisfy the full intent of the controls in the environment." As to these controls AR had no control place. AR claimed partial compliance for having equipment or software that it had not installed. Relator continually challenged AR on the use of these types of false and misleading statements AR was making to the government regarding its DFARS compliance.

64. In the letter AR wrote: " It is important to note that AR is compliant with the majority of the clauses requirements. Please be assured that AR will make every effort to prevent a data breach while we work aggressively to strengthen the controls and implement additional protection measures". AR made this statement when it knew if was 75% non-compliant with the NIST SP 800-53 requirements and AR's computer system had already been breached by foreign nation states and AR had not taken effective measures to prevent a future breach.

65. AR was awarded this contract following these false and misleading statements on September 29, 2014. The contract required that AR comply with DFARS Clause 252.204-7012, which was incorporated by reference in Schedule K of the contract. At the time AR signed the contract it was 75% non-complaint with the DFARS cyber security requirements.

66. In May 2015, AR sought a waiver of some of the DFARS Clause 252.704-7012 cyber security requirements in seeking a contract from the DOD.

67. Federal contracting officer, Laurie Hewitt ("HEWITT"), contacted Vicki Michetti ("MICHETTI") of the DoD CIO office via email to seek a waiver for an urgent contract, W31P4Q-15-C-0016. MICHETTI advised HEWITT that the DoD CIO's could

not waive the DFARS requirements and that the DoD CIO'S role was limited to adjudicating a contractor's use of an alternative to a required security control or whether a particular control is applicable to the situation. MICHETTI told HEWITT that compliance with DFARS was not required prior to her awarding the contract to AR but that the DFARS controls had to be in place by the time AR would have UCTI on its system.

68. Relator is informed and believes and thereon alleges that AR was told by the government that the DFARS requirements were non-waivable and that AR was awarded contract W31P4Q-15-C-0016 and that it stored UCTI information related to this contract on its system even though it was not fully compliant with DFARS Clause 252.704-7012.

69. In connection with trying to obtain contract award W31P4Q-15-C-0016, AR provided information to the DOD that was false and misleading and omitted information regarding the DFARS Clause 252.704-7012 requirements it was not complying with.

70. MICHETTI sent an email to HEWITT on May 21, 2015 describing the information AR had provided to the DoD CIO about its DFARS compliance. The information provided by AR was confusing and misleading.

71. AR provided the DOD with a table of controls that was truncated to omit the controls it was not complying with. AR advised the DoD CIO it had seven DFARS controls that were "in place and compliant." But for most of the controls AR indicated "controls in place/ enhancements and refinements ongoing." AR also indicated it had five controls listed partial controls in place.

72. AR's representation that it controls in place or was partially compliant was intentionally misleading. MICHETTI was misled by AR'S statements causing her to

erroneously conclude that AR was possibly compliant when AR was 75% non-compliant with the DFARS requirements. In her email to HEWITT of May 21, 2015, MICHETTI stated: "Based on the documentation provided by the contractor, we determined that they are not compliant with the DFARS Clause 252.204-7012. However, it may be a relatively simple matter for the contractor to become compliant…. It is possible that they are compliant but they are either not fully describing what they are doing, or are misinterpreting the requirements."

73. AR engaged in a pattern of providing false and misleading information to the government regarding its DFARS and NASA FARS cyber security compliance. AR would report it was partially compliant with a DFARS control it was compliant at one of its locations even though compliance at one location was worthless as it provided no protection because its other locations were vulnerable to cyber attack giving a hacker access it entire computer system.

74. One of the cyber security controls required that AR monitor its email accounts to make sure employees were not sending UCTI or SBU out of its system. Compliance required that all emails be monitored to make sure employees were not sending an email with UCTI or SBU information. AR only monitored emails going out to a couple major domains like Gmail or Yahoo and then advised the government that it was compliant with that control.

75. DFARS controls prohibited AR from sending information between its locations over the Internet when it was not encrypted. AR took the position that it could send the information unencrypted because it was going to a site that was encrypted even though EMAGINED showed AR a white paper that showed how this information could be intercepted.

76. In 2015, AR was working on a DOD contract related to ground based strategic defense ("GBSD"), the United States intercontinental missile defense system. DFARS required that there be two levels of security to access the computer system. AR was required to have the employee use not only a user name and password to access the system but also to use a magnetic card but AR had no card reader. AR installed a card reader and told the government that they were compliant with this DFARS requirement and then removed the card reader a few months later.

77. AR also provided false and misleading information to the prime contractors for which it was working on contracts that required DFARS and NASA FARS compliance.

78. After DFARS Clause 252.204-7012 became effective in November 2013, prime contractors including Raytheon started to submit questions to AR to make sure they were DFARS compliant.

79. AR submitted these questions to EMAGINED to prepare a response. EMAGINED provided AR with a response that indicated they were not DFARS or NASA FARS compliant and not eligible to work on DOD contracts that required DFARS 252.204-7012 compliance.

80. Based on the fact that AR continued to get work from these defense contractors, relator is informed and believes and thereon alleges that AR provided false information to these prime contractors by changing the response they received from EMAGINED.

81. In July 2015, ARH, VP and COO, Mark Tucker approached relator and VP & CIO Jose Ruiz requesting that they sign a documents that they could send to defendants' contracts department indicating that defendants' computer system was now complaint with the NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012.

82. When relator told defendants he could not sign the document until defendants were compliant with these cyber security requirements, Mr. Tucker brushed his comment off stating that it was not really a big deal and that all that would happen if they were not compliant with these federal acquisition regulations is they might get audited. He also stated that the government has never shutdown one of their programs for being out of compliance in the past. Relator refused to sign the documents and he advised defendants that by signing these documents he would be committing a fraud on the government and he could lose his national security clearance. Relator contacted the companies Ethics hotline and filed a formal report.

83. On September 14, 2015, MARKUS' employment with defendants was terminated.

DOD Contracts

84. AR signed at least six contracts with the DOD between February 23, 2014 and April 8, 2015 that incorporated the November 2013 version of DFARS Clause 252.704-7012. The clause was incorporated in schedule K of each of these contracts.

85. AR signed a contract to provide services to the Department of the Army on February 24, 2014, Award ID # W31P4Q14C0075 (Department of the Army, Office W6QK ACC RSA) which was valued at $ 33,070,971.

86. AR signed a contract to provide services to the Department of the Navy on April 22, 2014, Award ID #N0001414COO35 (Department of the Navy, Office of Naval Research) valued at $879,303

87. AR signed a contract to provide services to the Department of the Air Force on September 29, 2014, Parent Award ID #FA865013D2335, Award Id. 0002 (Department of the Air Force, Office FA8650 USAF AFMC AFRL/RQK) valued at $8,326,290.

88. AR signed a contract to provide services to the Department of the Navy on September 30, 2014, Award ID # N6893614C0035 (Department of the Navy, Office Naval Air warfare Center) valued at $843,421.

89. AR signed a contract to provide services to Department of the Air Force on September 30,2014, Award ID # FA865014C7424 (Department of the Air Force, Office FA8650 USAF AFMC AFRL/RQK) valued at $467,018

90. AR signed a contract to provide services to Department of the Air Force on April 8, 2015, Parent Award ID #FA865013D2335, Award Id. 0003 (Department of the Air Force, Office FA8650 USAF AFMC AFRL/RQK) valued at $6,467,965.

91. AR signed two contracts that required it comply with August 2015 interim rule modifying DFARS Clause 252.704-7012 so as to require it comply with the NIST SP 800-171 cyber security standards.

92. AR signed a contract to provide services to the Defense Advanced Research Projects Agency on September 15, 2015, Award ID # HR001115C0132 (Defense Advanced Research Projects Agency, Office DEF Advanced Research Projects Agency) valued at $320,284

93. AR signed a contract to provide services to the Department of the Air Force on October 8, 2015, Parent Award ID #FA865013D2335, Award Id. 0004 (Department of the Air Force, Office FA8650 USAF AFMC AFRL/RQK) valued at $955,818.

94. AR entered these contracts when it knew it was less than 25% with the required NIST SP 800-53 controls.

95. AR not only fraudulently entered these contracts but it did not comply with the law when the DFARS requirements were relaxed.

96. AR was compliant with only 41 of the relaxed 188 NIST SP 800-171 controls at the time it solicited these contracts.

97. Although DFARS 252.704-7012 was relaxed to allow AR to until December 31, 2017 reach full DFARS 252.704-7012 compliance, AR compliance with the NIST 800-171 standards was not excused.

98. AR was required to submit requests to vary from the NIST SP 800-171 standards in writing to the DoD CIO. The AR was only excused from a security control if it was "adjudicated by an authorized representative of the DoD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place."

99. AR did not submit requests in writing to deviate from all of the NIST SP 800-171 standards where it was not compliant.

100. When the standard was relaxed AR was also required to notify the DoD CIO within 30 days of all its contracts entered before October 1, 2017 that were not fully compliant with the NIST SP 800-171 controls and relator is informed and believes and thereon alleges that AR failed to do this.

101. Every version of DFARS 252.704-7012 required that AR provide "Adequate Security" to protect UCTI from unauthorized disclosure.

102. The clause stated "Adequate security means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."

103. AR entered these contracts knowing it was not providing "Adequate Security" because its system had already been breached by foreign nation states in 2013 and 2014 and it knew it was no more than 25% compliant with the NIST controls required to protect UCTI.

104. AR concealed information from the government the extent of its failure to comply with the NIST SP 800-53 and NIST SP 800-171 controls when it entered these contracts and represented to the government that it was more compliant than it was.

NASA Contracts

105. AR signed at least nine contracts with the NASA between March 11, 2014 and April 1, 2016 that incorporated NASA FARS Clause 1852.204-76

106. AR through its wholly owned subsidiary Pratt & Whitney signed a contract to provide services to NASA on March 11, 2014, Parent Award ID # NNC10BA13B, Award ID #NN13TA66T (NASA Glenn Research Center) valued at $12,226,270.

107. AR signed a contract to provide services to NASA on December 11, 2014, Parent Award ID# NNC10BA02B, Award ID # NNC15TA07T (NASA Glenn Research Center) valued at $1,099,916.

108. AR signed a contract to provide services to NASA on February 14, 2015, Award ID # NNM16AB21P (NASA Marshall Space Flight Center) valued at $187,682.

109. AR signed a contract to provide services to NASA on March 31, 2015, Award ID# NNC15CA07C (NASA Glenn Research Center) valued at $28,851,720.

110. AR signed a contract to provide services to NASA on July 27,2015, Award ID # NNC15VD08P (NASA Glenn Research Center) valued at $99,782.

111. AR signed a contract to provide services to NASA on November 1, 2015, Award ID # NNM16AA02C (NASA Marshall Space Flight Center) valued at $1,672,701,512.

112. AR signed a contract to provide services to NASA on November 17, 2015, Award ID # NNM16AB22P (NASA Marshall Space Flight Center) valued at $8,213.

113. AR signed a contract to provide services to NASA on January 15, 2016, Award ID # NNH16CP17C (NASA Headquarters) valued at $6,509,484.

114. AR signed a contract to provide services to NASA on April 1, 2016, Award ID # NNM16AA12C (NASA Marshall Space Flight Center) valued at $195,610,838.

115. These NASA contracts all incorporated NASA FARS Clause 1852.204-76 as was required by NASA FAR Reg. NASA FAR 1804.470-4(a) because AR was required to process, manage, access, or store unclassified electronic information, to include Sensitive But Unclassified (SBU) information belonging to NASA in the course of performing the contract. This clause required that AR protect NASA'S SBU information adhering to 264 of the NIST SP 800-53 moderate cyber security controls.

116. At the time AR solicited these contracts AR was not compliant with the NIST SP 800-53 moderate cyber security controls. As of October 2015 AR was only compliant with 63 of the 264 required controls. As of the end of November 2015 AR was only compliant with 78 of the 264 controls.

117. NASA FARS Clause 1852.204-76 required that AR submit an IT Security Management Plan within 30 days of being awarded these contracts. AR submitted IT Security Management Plans pursuant to these contracts that represented that it was complying with the NIST SP 800-53 moderate cyber security controls when it was not.

118. AR was also required to submit monthly reports to NASA certifying that it was complying with the IT Security Management Plan and the NIST SP 800 -53 controls. Relator was requested to sign these monthly reports but refused to do so because they represented that AR was compliant with the NIST SP 800-53 Controls when it was not.

119. AR tried to get other IT personnel including Jens Landreth and David Chamberlin to sign these NASA reports but they refused. AR kept circulating the report until they could find someone to sign it.

COUNT ONE
PROMISSORY FRAUD IN VIOLATION OF 31 U.S.C. §3729(a)(1)(A)

120. Relator re-alleges and incorporates the allegations of paragraphs 1–119 as if fully set forth herein.

121. Defendants entered multiple contracts with the federal government wherein they had access to and stored UCTI and SBU belonging to the government on their computer system, which required defendants to meet minimum cyber security requirements to protect that information set forth in DFARS Clause 252.704-7012 or NASA FARS Clause1852.204-76

122. The federal government set forth these minimum cyber security requirements in federal acquisition regulations, including NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012. Compliance with these regulations was not only a prerequisite to payment on these contracts but defendants were required to meet these requirements to participate in the contracts at all.

123. Defendants knowingly made false statements to the government in order to induce the government to grant them contracts with NASA and the DOD even though they were not compliant with the DFARS and NASAFARS cyber security regulations.

124. Defendants falsely represented that they were compliant with NASA FARS Clause1852.204-76 and DFARS Clause 252.704-7012. These included signing contracts that included DFARS and NASA FARS cyber security requirements that defendants knew they were not complying with. Not only did defendants' falsely represent that they were complying with these requirements but at the time they made those promises they had no intention of complying with these cyber security regulations.

125. Defendants also concealed information from the government regarding the state of its compliance with NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012 because they knew they were not eligible to participate in these contracts and that if they disclosed this information they would not get the contract award.

126. Defendants obtained subcontracts that were subject to federal acquisition regulations, NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012, related to cyber security by falsely representing that they were compliant with those regulations. These prime contractors included Boeing, Lockheed Martin and Raytheon.

127. The federal government was misled by defendants' false statements and would never have entered these contracts with defendants had the government been aware that defendants were not complying with the NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012 cyber security regulations. These regulations prohibited the federal government from entering contract with a party that would have access to UCTI or SBU belonging to the federal government unless that party was complying with these cyber security regulations.

128. Compliance with these regulations was material to the federal government's decision to enter these contracts as no federal contracting officer has authority to enter a contact where the contractor is not complying with the law. 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."

129. As a result of defendants' false representations and material omissions the federal government paid out money on contracts they would have never entered.

130. As a result of these false representations and material omissions the federal government paid out more money to defendants than they would not have otherwise paid as the government would have demanded a discount on the money they paid defendants for their goods and services had they known defendants were not complying with these federal acquisition regulations.

131. The federal government has also been damaged as UCTI and SBU belonging to the federal government has been made available to unauthorized parties, including technical work product information such as engineering designs that the government was paying defendants to create.

COUNT TWO
FALSE OR FRAUDULENT STATEMENT OR RECORD 31 U.S.C. §3729(a)(1)(B)

132. Relator re-alleges and incorporates the allegations of paragraphs 1–131 as if fully set forth herein.

133. Defendants' knowingly made, used, or verified a false record or statement that was material to the false or fraudulent claim.

134. Defendants signed contracts with the DOD and NASA representing to the government that they were DFARS and NASA FARS compliant when they knew they were not. They submitted IT Security Management Plans indicating that that were

complying with NASA FARS Clause 1852.204-76 when they were not. AR also sent monthly reports for its NASA contracts certifying it was complying with NASA FARS Clause 1852.204-76 when it was not.

135. FAR 52.246-15 required that every invoice AR submitted to the government for payment have a certification certifying that the supplies or services were in accordance with all applicable requirements and the supplies or services are of the quality specified and conform in all respects with the contract requirements.

136. Relator is informed and believes and thereon alleges that AR submitted invoices to the government for payment for the services on the contracts alleged herein and that AR falsely certified in those invoice that the services conformed in all respects with the contract requirements when it knew it was not complying with NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012 including providing "Adequate Security" to protect UCTI belonging to the federal government.

137. All of these statements were made to get the federal government to make payments to which defendants were not entitled or would have been substantially discounted had the government been aware that defendants were not compliant with the federal acquisition regulations related to cyber security, NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012.

138. This course of conduct violated the False Claims Act, 31 U.S.C. §§ 3729 *et seq.*

139. The federal government was unaware of the falsity of the claims and/or

statements, and acted in reliance on the accuracy thereof.

140. The federal government was damaged as a result of defendants' conduct as they paid defendants for bills and invoices they would not have otherwise paid.

141. The federal government was damaged because they paid defendants more than their good services were worth given defendants' failure to comply with the federal acquisition regulations that were required by these contracts. The federal government would have demanded a discount if it had known defendants were not complying with the cyber security regulations required by the contracts..

142. The federal government has also been damaged as its UCTI and SBU has been made available to unauthorized parties, including technical work product information such as engineering designs that the government was paying defendants to create.

COUNT THREE
CONSPIRACY TO SUBMIT FALSE CLAIMS 31. U.S.C.A. §3729(a)(1)(C)

143. Relator re-alleges and incorporates the allegations of paragraphs 1–142 as if fully set forth herein.

144. Defendants and their officers and managing agents combined, conspired, and agreed together to defraud the United States by knowingly submitting false claims to the United States and to its grantees for the purpose of getting the false or fraudulent claims paid or allowed and committed the other overt acts set forth above in furtherance of that conspiracy, all in violation of 31 U.S.C. § 3729(a)(1)(C), causing damage to the United States.

COUNT FOUR
RETALIATION IN VIOLATION OF 31 U.S.C. § 3730(h)

145. Relator re-alleges and incorporates the allegations of paragraphs 1–144 as if fully set forth herein.

146. On September 14, 2015, *qui tam* plaintiff MARKUS was terminated in his employment by defendants as a result of his lawful acts done in furtherance of this action, including complaints to management regarding the false claims described herein and his refusal to falsely sign a document indicating that defendants were compliant with DFARS and NASA FARS. MARKUS' termination was in violation of 31 U.S.C. § 3730(h).

147. As a direct and proximate result of this unlawful termination, MARKUS has suffered emotional pain and mental anguish, together with serious economic hardship, including lost wages and special damages associated with his efforts to obtain alternative employment, in an amount to be proven at trial.

COUNT FIVE
MISREPRESENTATION IN VIOLATION OF LABOR CODE § 970

148. Relator re-alleges the information set forth in paragraphs 1-147 above and hereby incorporate these paragraphs as though fully set forth and alleged herein.

149. Defendant made false promises to MARKUS in order to induce him to move from the southern California where he was working for Raytheon to Northern California to work for AR.

150. Defendant made false statements to MARKUS regarding the kind and character of the work he would be doing at AR and the length of time his employment would last.

151. As set forth above, defendant misled MARKUS regarding its commitment to complying with NASA FARS and DFARS cyber security regulations. Defendant recruited relator by representing that he was being hired to improve the cyber security of defendants computer systems in order to make those systems fully compliant with NASA FARS and DFARS cyber security requirements. At the time defendant hired MARKUS they had no intention devoting the resources necessary to make their computer system fully compliant with these regulations.

152. In order to induce MARKUS to take the job, defendant made false promises to MARKUS concerning the resources he would have available in order to make defendant's computer system fully compliant with NASAFARS and DFARS regulations. Defendant promised MARKUS a budget of 15 million dollars when they had no intention giving MARKUS a budget this large. Defendant gave MARKUS a budget of less than four million.

153. Defendants falsely promised MARKUS that if he took the job he would have a staff of 40 employees who were knowledgeable in cyber security. When MARKUS arrived to start his job he had no employees and was later given two to three internal employees and seven contract employees. The internal employees were not knowledgeable in cyber security.

154. In order to induce MARKUS to take the AR job, defendant falsely promised relator that he would have full authority to implement changes to the computer system that were needed to make the systems compliant with cyber security regulations. MARKUS was given no authority to make changes but was required to go through a lengthy justification and process where the changes he attempted to implement were often vetoed by AR and ARH management.

155. Defendants committed these acts alleged herein maliciously, fraudulently, and oppressively, in bad faith with the wrongful intention of injuring relator, from an improper and evil motive amounting to malice, and/or in conscious disregard of relator's rights by reason thereof relator is entitled to an award of punitive damages, the amount of such damages to be established by proof at trial.

156. These misrepresentations entitle relator to a civil penalty for double the damages resulting from defendants' misrepresentations pursuant to Labor Code § 972.

157. Relator is entitled to an award of his reasonable attorneys fees in connection with the prosecution of this action.

COUNT SIX
WRONGFUL TERMINATION IN VIOLATION OF PUBLIC POLICY

158. Relator re-alleges the information set forth in Paragraphs 1-157 above, and incorporates these paragraphs into this cause of action as if they were fully alleged herein.

159. Under California law, no employee, whether they are an at-will employee, or an employee under a written or other employment contract, can be terminated for a reason that is in violation of a fundamental public policy.

160. Relator is informed and believes, and based thereon alleges, that defendants terminated his employment in violation of public policy of the State of California and the United States, as a motivating reason for his termination was opposing defendants' conduct in violation of the federal false claims act 31 U.S.C. §§ 3729 et seq. and DFARS and NASA FARS regulations

161. Relator alleges that defendants violated articulated, fundamental public policies, affecting society at large, by violating the statutes described above.

162. As a direct, foreseeable, and proximate result of the actions of defendants as described above, relator has suffered, and continues to suffer severe emotional distress, substantial losses in salary, bonuses, job benefits, and other employment benefits he would have received from defendants, all to the relator's damage, in an amount unknown at this time but to be established at the time of trial.

163. Based on the grossly reckless and/or intentional, malicious, and bad faith manner in which defendants conducted themselves as described herein, by willfully violating those statutes enumerated above, relator prays for punitive damages against defendants in an amount to be determined at the time of trial, that is sufficiently high to punish defendants, deter them from engaging in such conduct in the future, and to make an example of them to others.

164. Relator is informed and believes, and based thereon alleges, that the outrageous conduct of defendants, described above, was done with oppression and malice and was ratified by the other individuals who were managing agents of those directly responsible. These unlawful acts were further ratified by the defendant employers and done with a conscious disregard for relator's rights and with the intent, design and purpose of injuring realtor. By reason thereof, relator is entitled to punitive or exemplary damages against defendants for their acts as described in this cause of action in a sum to be determined at the time of trial.

WHEREFORE, relator respectfully requests this Court to enter judgment against defendants, as follows:

(a) That the United States be awarded damages in the amount of three times the damages sustained by the United States because of the false claims and fraud alleged within this Complaint, as the Civil False Claims Act, 31 U.S.C. §§ 3729 *et seq.* provides;

(b) That unjust enrichment damages are awarded to the United States for the money defendants' were not required to spend to keep their computer systems DFARS and NASAFARS compliant as required by their contracts with the federal government;

(c) That civil penalties of $11,000 are imposed for each and every false claim that defendants presented to the United States and/or its grantees;

(d) That pre- and post-judgment interest is awarded, along with reasonable attorneys' fees, costs, and expenses, which the relator necessarily incurred in bringing and pressing this case;

(e) That the Court grant permanent injunctive relief to prevent any recurrence of the False Claims Act for which redress is sought in this Complaint;

(f) That the relator be awarded the maximum amount allowed to him pursuant the False Claims Act; and

(g) For Count four, that relator be granted all relief necessary to make him whole, including but not limited to two times his back pay and other compensatory damages sustained as a result of defendants' harassment and retaliation;

(h) Punitive damages; and,

(i) That this Court award such other and further relief as it deems proper

DEMAND FOR JURY TRIAL

Relator, on behalf of himself and the United States, demands a jury trial on all claims alleged herein.

DATED: January 4, 2019

THYBERGLAW

/s/ Gregory A. Thyberg
GREGORY A. THYBERG
Attorney for Relator
BRIAN MARKUS