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 **FILED UNDER SEAL PURSUANT TO 31 U.S.C. § 3730(b)(2)** **DO NOT PLACE IN PRESS BOX** **DO NOT ENTER ON PACER**

FIRST 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 shall serve 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.

II. Jurisdiction and Venue

3. 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.

4. 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

5. 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.

6. 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 DOD and NASA.

7. 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

8. United States government contracts are subject to Federal Acquisition Regulations ("FAR"). There are also agency specific regulations that supplement FAR. Contracts entered with the DOD are subject to Defense Federal Acquisition Regulations ("DFARS") and contracts entered with NASA are subject to NASA Federal Acquisition Regulations ("NASAFARS")

9. 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 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 NASAFARS regulations and apply to all federal contracts where the contractor will have access to unclassified controlled technical information belonging to the federal government.

10. 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 NASAFARS regulations in order to be awarded a government contract where they would have access to unclassified controlled technical information belonging to the federal government.

11. 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 unclassified controlled technical information and to insert terms in the contract to make sure the DFARS and NASAFARS 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

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

13. The unclassified controlled technical information 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.

14. 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.

15. The DOD REG required that all federal contracts 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 unclassified controlled technical information belonging to the federal government.

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

17. DFARS Clause 252.704-7012 required that contactors meet the standards specified by the NIST Special Publication 800-53.

18. 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.

B. Wrongful Acts by Defendants

19. 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 DOD REG, DFARS, NASA-FARS, DD-254 forms and DFARS Clause 252.704-7012 even though defendants knew their information systems did not meet these cyber security requirements.

20. 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.

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

22. 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.

23. 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.

24. 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.

25. 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 unclassified controlled technical information belonging to the federal government.

26. 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.

27. 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.

28. Defendants were not compliant with the NASAFARS or DFARS cyber security requirements including the DOD REG or DFARS Clause 252.704-7012 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 DOD REG, DFARS or NASAFARS cyber security requirements for several years.

29. 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 NASAFARS 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 DOD REG, NASAFARS, DFARS or DFARS Clause 252.704-7012 cyber security requirements.

30. 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 DOD REG, NASAFARS, DFARS or DFARS Clause 252.704-7012 cyber security requirements.

31. 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.

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

33. 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.

34. Relator prepared a presentation to be presented to the Board, which showed that defendants' computer system was not DFARS or NASAFARS 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.

35. When AR'S president Warren Boley ("BOLEY") became aware that relator intended tell the Board that defendants were not DFARS or NASAFARS 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 NASAFARS cyber security requirements.

36. Defendants' federal contracts required that they be 100% compliant with the 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.

37. Defendants' management was well aware prior to January 2015 that they were out of compliance with the DFARS and NASAFARS 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 NASAFARS 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 NASAFARS cyber security regulations.

38. 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 NASAFARS compliance levels.

39. 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.

40. EMAGINED found defendants were only 23.9% compliant NASA NIST SP 800 moderate controls, 21.8% compliant with NASA NIST 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.

41. 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.

42. 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.

43. 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.

44. 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.

45. 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.

46. 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.

47. In order secure new contracts, defendants' contracts department had to represent to the federal government that they were compliant with NASAFARS, DFARS, and DOD REG requirements. Moreover, defendants had to sign contracts, which included DFARS Clause 252.704-7012 relating to cyber security.

48. 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 NASAFARS, DFARS, DOD REG and DFARS Clause 252.704-7012.

49. 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.

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

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

51. Relator re-alleges and incorporates the allegations of paragraphs 1–50 as if fully set forth herein.

52. Defendants entered multiple contracts with the federal government wherein they had access to unclassified controlled technical information and were required to meet minimum cyber security requirements to protect that information through either the DFARS Clause 252.704-7012 or specifically called out in a program DD-254.

53. The federal government set forth these minimum cyber security requirements in federal acquisition regulations, including DFARS, NASAFARS, DOD REG 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.

54. 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.

55. Defendants falsely represented that they were compliant with DFARS, NASAFARS and DFARS Clause 252.704-7012 as well as specific sections of program DD-254's. These included signing contracts that included DFARS and NASAFARS 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.

56. Defendants obtained subcontracts that were subject to federal acquisition regulations related to cyber security by falsely representing that they were compliant with those regulations. These prime contractors included Boeing, Lockheed Martin and Raytheon.

57. 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 NASAFARS, DFARS or DOD REG cyber security regulations. These regulations prohibited the federal government from entering contract with a party that would have access to unclassified controlled technical information unless that party was complying with these cyber security regulations.

58. As a result of defendants false representations the federal government paid out money on contracts they would have never entered.

59. As a result of these false representations 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.

60. The federal government has also been damaged as its unclassified controlled technical information 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)

61. Relator re-alleges and incorporates the allegations of paragraphs 1–60 as if fully set forth herein.

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

63. Defendants signed contracts prior to November 18, 2013 representing to the government that they were DFARS and NASAFARS compliant when they knew they were not.

64. Defendants signed contracts after November 18, 2013, indicating that they were compliant with DFARS Clause 252.704-7012 when they knew they were not.

65. Defendants told the federal government that they had cyber security software that was required by DFARS when that software covered only part of their system, while DFARS required 100% coverage.

66. Defendants represented to the federal government that that had computer hardware that was required by DFARS and NASAFARS, when the hardware in question was sitting in a box and was not being used by defendants.

67. Defendants submitted invoices and bills to the federal government for payment when defendants knew that the government would not have awarded defendants the contract or paid for their services if the federal government was aware that defendants were not in compliance with NASAFARS, DFARS, DOD REG or DFARS Clause

252.704-7012.

68. 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.

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

70. The federal government was unaware of the falsity of the claims and/or statements, and acted in reliance on the accuracy thereof.

71. 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.

72. 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..

73. The federal government has also been damaged as its unclassified controlled technical information 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)

74. Relator re-alleges and incorporates the allegations of paragraphs 1–73 as if fully set forth herein.

75. Defendants 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)

76. Relator re-alleges and incorporates the allegations of paragraphs 1–75 as if fully set forth herein.

77. 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 NASAFARS. MARKUS' termination was in violation of 31 U.S.C. § 3730(h).

78. 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

79. Relator re-alleges the information set forth in paragraphs 1-78 above and hereby incorporate these paragraphs as though fully set forth and alleged herein.

80. 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.

81. 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.

82. As set forth above, defendant misled MARKUS regarding its commitment to complying with NASAFARS 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 NASAFARS 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.

83. 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.

84. 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.

85. 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.

86. 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.

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

88. 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

89. Relator re-alleges the information set forth in Paragraphs 1-88 above, and incorporates these paragraphs into this cause of action as if they were fully alleged herein.

90. 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.

91. 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 NASAFARS regulations

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

93. 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.

94. 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.

95. 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: September 13, 2017

THYBERGLAW

GREGORY A. THYBERG
Attorney for Relator
BRIAN MARKUS