

1 THYBERGLAW  
2 GREGORY A. THYBERG SBN102132  
3 3104 O STREET #190  
4 SACRAMENTO, CALIFORNIA 95816  
5 TEL: (916) 204-9173  
6 greg@thyberglaw.com

**FILED**  
Sep 13, 2017  
CLERK, U.S. DISTRICT COURT  
EASTERN DISTRICT OF CALIFORNIA

7 ATTORNEYS FOR RELATOR, BRIAN MARKUS

**SEALED**

8 UNITED STATES DISTRICT COURT

9 FOR THE EASTERN DISTRICT OF CALIFORNIA

10  
11 UNITED STATES OF AMERICA: ) Civil Action No. 2:15-cv-2245 WBS-AC  
12 *ex rel.* )  
13 BRIAN MARKUS ) **FILED UNDER SEAL PURSUANT TO**  
14 ) **31 U.S.C. § 3730(b)(2)**  
15 Plaintiffs, )  
16 vs. )  
17 AEROJET ROCKETDYNE HOLDINGS, )  
18 INC., a corporation and AEROJET )  
19 ROCKETDYNE, INC. a corporation. ) **DO NOT PLACE IN PRESS BOX**  
20 ) **DO NOT ENTER ON PACER**  
21 Defendants )  
22 )  
23 )  
24 )

25 **FIRST AMENDED FALSE CLAIMS ACT COMPLAINT AND DEMAND FOR**  
26 **JURY TRIAL**

27 **I. Introduction**

28 1. Brian Markus (the “relator”) brings this action on behalf of the United States of America against defendants AEROJET ROCKETDYNE HOLDINGS, INC.

1 (“ARH”) and AEROJET ROCKETDYNE INC. (“AR”) for treble damages and civil  
2 penalties arising from defendants’ false statements and false claims in violation of the  
3 Civil False Claims Act, 31 U.S.C. §§ 3729 *et seq.* The violations arise out defendants  
4 fraudulently inducing the federal government to grant them contracts to provide goods  
5 and services to the federal government including, the National Aeronautics and Space  
6 Administration (“NASA”) and the Department of Defense (“DOD”), when they knew  
7 they were not complying with federal acquisition regulations that were required as a  
8 material terms of those contracts.  
9

10  
11 2. As required by the False Claims Act, 31 U.S.C. § 3730(b)(2), the relator  
12 shall serve the Attorney General of the United States and to the United States Attorney  
13 for the Eastern District of California a statement of all material evidence and information  
14 related to the complaint. This disclosure statement is supported by material evidence  
15 known to the relator at his filing establishing the existence of defendants’ false claims.  
16 Because the statement includes attorney-client communications and work product of  
17 relator’s attorneys, and is submitted to the Attorney General and to the United States  
18 Attorney in their capacity as potential co-counsel in the litigation, the relator understands  
19 this disclosure to be confidential.  
20  
21

## 22 **II. Jurisdiction and Venue**

23  
24 3. This action arises under the False Claims Act, 31 U.S.C. §§ 3729 *et seq.*  
25 This Court has jurisdiction over this case pursuant to 31 U.S.C. §§ 3732(a) and 3730(b).  
26 This court also has jurisdiction pursuant to 28 U.S.C. § 1345 and 28 U.S.C. § 1331.  
27



1 are jointly and severally liable for the conduct alleged herein.

2 **III. Facts Common to All Counts**

3 **A. Background**

4  
5 8. United States government contracts are subject to Federal Acquisition  
6 Regulations (“FAR”). There are also agency specific regulations that supplement FAR.  
7 Contracts entered with the DOD are subject to Defense Federal Acquisition Regulations  
8 (“DFARS”) and contracts entered with NASA are subject to NASA Federal Acquisition  
9 Regulations (“NASAFARS”)

10 9. The federal government requires that all companies that enter contracts to  
11 provide good or services to the DOD or NASA meet minimum standards to prevent  
12 unauthorized access and disclosure of unclassified controlled technical information  
13 belonging to NASA or the DOD that will be stored on the company’s computer system in  
14 the course of the company performing the government contract. These minimum  
15 standards are set forth in the DFARS and NASAFARS regulations and apply to all  
16 federal contracts where the contractor will have access to unclassified controlled  
17 technical information belonging to the federal government.

18  
19 10. Prior to November 18, 2013, the federal government ensured compliance  
20 with these regulations by incorporating terms in federal contracts setting minimum levels  
21 of cyber security to make sure that contractors’ information systems were protected from  
22 unauthorized access. Contractors were required to meet the minimum standards for cyber  
23 security set forth in the DFARS and NASAFARS regulations in order to be awarded a  
24 government contract where they would have access to unclassified controlled technical  
25 information belonging to the federal government.

26 11. The DFARS and NASAFARS regulations required that contactors meet  
27 cyber security standards standards specified by the National Institute of Standards and

1 Technology (“NIST”). Contracting officers at NASA and the DOD were required to  
2 review contracts to see if there would be access to unclassified controlled technical  
3 information and to insert terms in the contract to make sure the DFARS and NASAFARS  
4 regulations relating to cyber security were incorporated as a term of the contract. In the  
5 case of the DOD, the agency would prepare a form DD-254 that was incorporated in the  
6 contract

7  
8 12. On November 18, 2013, the DOD issued a regulation, 78 Fed. 69,273,  
9 (“DOD REG”) which intensified the safeguards required by government contractors to  
10 protect their computer systems from cyber attacks that could result in unauthorized access  
11 and disclosure of unclassified controlled technical information belonging to the federal  
12 government.

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

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

22 15. The DOD REG required that all federal contracts going forward  
23 incorporate DFARS Clause 252.704-7012. This clause was required in any contract with  
24 the government where the contractor would have access to unclassified controlled  
25 technical information belonging to the federal government.  
26

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

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

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

10  
11 B. Wrongful Acts by Defendants

12 19. Defendants have entered multiple contracts with the federal government,  
13 and as subcontractors on contracts with the federal government, which required that  
14 defendants meet the cyber security standards set forth in the DOD REG, DFARS, NASA-  
15 FARS, DD-254 forms and DFARS Clause 252.704-7012 even though defendants knew  
16 their information systems did not meet these cyber security requirements.

17  
18 20. Defendants fraudulently entered contracts knowing they did not meet the  
19 minimum standards required to be awarded a contract and they misled the government  
20 concealing their non-compliance with these regulations.

21  
22 21. Defendants also fraudulently entered subcontracts with prime contractors  
23 who were working on federal contracts that required that they comply with the DFARS  
24 and NASAFARS cyber security regulations.  
25  
26  
27  
28

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

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

7           24.     When relator started working for defendants, he was given a budget of only  
8 3.8 million dollars rather than 10 million. Defendants provided an internal staff of two  
9 employees not the five to ten that were promised. Instead of twenty-five contract  
10 employees, defendants provided only seven.

11           25.     Relator found that defendants were understaffed and under budgeted to  
12 provide the level of cyber security that was required by the federal acquisition regulations  
13 for contractors granted access to unclassified controlled technical information belonging  
14 to the federal government.

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

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

21           28.     Defendants were not compliant with the NASAFARS or DFARS cyber  
22 security requirements including the DOD REG or DFARS Clause 252.704-7012 when  
23 relator started his employment June 30, 2014. Based on the state of defendants' computer  
24 systems at the time relator began his employment, relator is informed and believes  
25  
26  
27

1 thereon alleges defendants' computer systems had not been compliant with the DOD  
2 REG, DFARS or NASAFARS cyber security requirements for several years.

3 29. In 2013, ARH purchased Rocketdyne from Pratt & Whitney. At the time of  
4 the purchase Pratt & Whitney represented that its Rocketdyne division was compliant  
5 with the DFARS and NASAFARS regulations related to cyber security. After the  
6 purchase, the computer systems of Rocketdyne were merged with defendants' computer  
7 systems so that after 2013, Rocketdyne was no longer compliant with the DOD REG,  
8 NASAFARS, DFARS or DFARS Clause 252.704-7012 cyber security requirements.  
9

10 30. Defendants' were aware of breaches of their computer system in 2013 and  
11 2014 by nation state sponsored threat actors. Defendants reported those breaches to the  
12 federal government in as required by DFARS regulations and DFARS Clause 252.704-  
13 7012. In reporting those breaches defendants concealed the fact that their computer  
14 system was not compliant with the DOD REG, NASAFARS, DFARS or DFARS Clause  
15 252.704-7012 cyber security requirements.

16 31. When questioned by the government about its cyber security, defendants  
17 gave the government misleading information. For example, they were asked if they had a  
18 certain piece of security equipment, they would say "yes," even though the equipment  
19 was sitting in a box and not connected to their computer system. Defendants represented  
20 they had cyber security software/hardware installed to protect the systems when in reality  
21 the software/hardware in question only covered part of the environment leaving  
22 defendants vulnerable to a cyber attack. In some cases, they claimed compliance only  
23 considering the primary control and not the sub-controls, which were clearly not being  
24 met.  
25  
26  
27  
28



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

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

7           34.     Relator prepared a presentation to be presented to the Board, which showed  
8 that defendants’ computer system was not DFARS or NASAFARS compliant. Relator’s  
9 report to be submitted to the Board indicated that defendants’ computer system was  
10 unpatched, misconfigured, outdated and thus vulnerable to a cyber attack.

11           35.     When AR’S president Warren Boley (“BOLEY”) became aware that relator  
12 intended tell the Board that defendants were not DFARS or NASAFARS compliant, he  
13 took over relator’s presentation and changed it. Relator is informed and believes and  
14 thereon alleges that BOLEY concealed from the Board that defendants were not in  
15 compliance with DFARS and NASAFARS cyber security requirements.

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

24           37.     Defendants’ management was well aware prior to January 2015 that they  
25 were out of compliance with the DFARS and NASAFARS cyber security requirements as  
26

1 relator provided AR and ARH'S top management, including the President, CEO and  
2 Chief Information officer weekly and monthly reports beginning July 2014 advising them  
3 of the state of AR and ARH'S compliance with DFARS and NASAFARS requirements.  
4 There were also a number of presentations made to multiple officers of AR and ARH  
5 prior to January 2015 regarding defendants' lack of compliance the DFARS and  
6 NASAFARS cyber security regulations.

7  
8 38. After the January 2015 board meeting, the Board ordered an audit of AR  
9 and ARH'S cyber security posture using Ernest & Young ("EY"). In addition, the Senior  
10 Leadership tasked Jose Ruiz (CIO) to update the compliance documents as it was a  
11 becoming dated and needed to reflect actual costs and DFARS and NASAFARS  
12 compliance levels.

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

17 40. EMAGINED found defendants were only 23.9% compliant NASA NIST  
18 SP 800 moderate controls, 21.8% compliant with NASA NIST 800-171 controls and  
19 27.8% compliant with the pre August 2015 DFARS controls. In order to participate in  
20 government contracts and bill for their services, defendants were required to be 100%  
21 compliant with these regulatory requirements.

22 41. The EMAGINED report indicated that for defendants to reach 100%  
23 compliance would take a combination of technical solutions, business process  
24 improvements and a fundamental change in defendants' strategic direction. EMAGINED  
25 stated for defendants to achieve compliance "... will require a shift in how the business  
26 addresses contractual and regulatory responsibilities..." The report outlined estimated  
27

1 costs in the amount of \$34,548,866 over a five-year period, which would be required for  
2 defendants' to make their computer systems compliant with the DFARS cyber security  
3 requirements.

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

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

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

21 45. The EY assessment team was also able to compromise the computer system  
22 so they could access physical security files and folders and they were able to remotely  
23 access defendants' security cameras so they could view and listen to security camera  
24 footage. This activity was not detected by defendants and remained undetected for seven  
25 days.  
26  
27



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

1  
2  
3         51. Relator re-alleges and incorporates the allegations of paragraphs 1–50 as if  
4 fully set forth herein.

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

9  
10         53. The federal government set forth these minimum cyber security  
11 requirements in federal acquisition regulations, including DFARS, NASAFARS, DOD  
12 REG and DFARS Clause 252.704-7012. Compliance with these regulations was not only  
13 a prerequisite to payment on these contracts but defendants were required to meet these  
14 requirements to participate in the contracts at all.  
15  
16

17         54. Defendants knowingly made false statements to the government in order to  
18 induce the government to grant them contracts with NASA and the DOD even though  
19 they were not compliant with the DFARS and NASAFARS cyber security regulations.  
20

21         55. Defendants falsely represented that they were compliant with DFARS,  
22 NASAFARS and DFARS Clause 252.704-7012 as well as specific sections of program  
23 DD-254's. These included signing contracts that included DFARS and NASAFARS  
24 cyber security requirements that defendants knew they were not complying with. Not  
25 only did defendants' falsely represent that they were complying with these requirements  
26 but at the time they made those promises they had no intention of complying with these  
27 requirements.

1 cyber security regulations.

2 56. Defendants obtained subcontracts that were subject to federal acquisition  
3 regulations related to cyber security by falsely representing that they were compliant with  
4 those regulations. These prime contractors included Boeing, Lockheed Martin and  
5 Raytheon.  
6

7 57. The federal government was misled by defendants' false statements and  
8 would never have entered these contracts with defendants had the government been  
9 aware that defendants were not complying with the NASAFARS, DFARS or DOD REG  
10 cyber security regulations. These regulations prohibited the federal government from  
11 entering contract with a party that would have access to unclassified controlled technical  
12 information unless that party was complying with these cyber security regulations.  
13  
14

15 58. As a result of defendants false representations the federal government paid  
16 out money on contracts they would have never entered.  
17

18 59. As a result of these false representations the federal government paid out  
19 more money to defendants than they would not have otherwise paid as the government  
20 would have demanded a discount on the money they paid defendants for their goods and  
21 services had they known defendants were not complying with these federal acquisition  
22 regulations.  
23

24 60. The federal government has also been damaged as its unclassified  
25 controlled technical information has been made available to unauthorized parties,  
26 including technical work product information such as engineering designs that the  
27

1 government was paying defendants to create.

2 **COUNT TWO**

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

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

6  
7 62. Defendants’ knowingly made, used, or verified a false record or statement  
8 that was material to the false or fraudulent claim.

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

12  
13 64. Defendants signed contracts after November 18, 2013, indicating that they  
14 were compliant with DFARS Clause 252.704-7012 when they knew they were not.

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

18  
19 66. Defendants represented to the federal government that that had computer  
20 hardware that was required by DFARS and NASAFARS, when the hardware in question  
21 was sitting in a box and was not being used by defendants.

22  
23 67. Defendants submitted invoices and bills to the federal government for  
24 payment when defendants knew that the government would not have awarded defendants  
25 the contract or paid for their services if the federal government was aware that defendants  
26 were not in compliance with NASAFARS, DFARS, DOD REG or DFARS Clause  
27 were not in compliance with NASAFARS, DFARS, DOD REG or DFARS Clause

1 252.704-7012.

2 68. All of these statements were made to get the federal government to make  
3 payments to which defendants were not entitled or would have been substantially  
4 discounted had the government been aware that defendants were not compliant with the  
5 federal acquisition regulations related to cyber security.  
6

7 69. This course of conduct violated the False Claims Act, 31 U.S.C. §§ 3729 *et*  
8  
9 *seq.*

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

12 71. The federal government was damaged as a result of defendants' conduct as  
13 they paid defendants for bills and invoices they would not have otherwise paid.  
14

15 72. The federal government was damaged because they paid defendants more  
16 than their good services were worth given defendants' failure to comply with the federal  
17 acquisition regulations that were required by these contracts. The federal government  
18 would have demanded a discount if it had known defendants were not complying with the  
19 cyber security regulations required by the contracts..  
20

21 73. The federal government has also been damaged as its unclassified  
22 controlled technical information has been made available to unauthorized parties,  
23 including technical work product information such as engineering designs that the  
24 government was paying defendants to create.  
25

26  
27 **COUNT THREE**  
**CONSPIRACY TO SUBMIT FALSE CLAIMS 31. U.S.C.A. §3729(a)(1)(C)**



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

4 75. Defendants combined, conspired, and agreed together to defraud the  
5 United States by knowingly submitting false claims to the United States and to its  
6 grantees for the purpose of getting the false or fraudulent claims paid or allowed and  
7 committed the other overt acts set forth above in furtherance of that conspiracy, all in  
8 violation of 31 U.S.C. § 3729(a)(1)(C), causing damage to the United States.  
9

10  
11 **COUNT FOUR**  
**RETALIATION IN VIOLATION OF 31 U.S.C. § 3730(h)**

12 76. Relator re-alleges and incorporates the allegations of paragraphs 1–75 as if  
13 fully set forth herein.  
14

15 77. On September 14, 2015, *qui tam* plaintiff MARKUS was terminated in his  
16 employment by defendants as a result of his lawful acts done in furtherance of this action,  
17 including complaints to management regarding the false claims described herein and his  
18 refusal to falsely sign a document indicating that defendants were compliant with DFARS  
19 and NASAFARS. MARKUS' termination was in violation of 31 U.S.C. § 3730(h).  
20

21 78. As a direct and proximate result of this unlawful termination, MARKUS  
22 has suffered emotional pain and mental anguish, together with serious economic  
23 hardship, including lost wages and special damages associated with his efforts to obtain  
24 alternative employment, in an amount to be proven at trial.  
25

26  
27 **COUNT FIVE**  
**MISREPRESENTATION IN VIOLATION OF LABOR CODE § 970**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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.

1 84. Defendants falsely promised MARKUS that if he took the job he would  
2 have a staff of 40 employees who were knowledgeable in cyber security. When  
3 MARKUS arrived to start his job he had no employees and was later given two to three  
4 internal employees and seven contract employees. The internal employees were not  
5 knowledgeable in cyber security.  
6

7 85. In order to induce MARKUS to take the AR job, defendant falsely  
8 promised relator that he would have full authority to implement changes to the computer  
9 system that were needed to make the systems compliant with cyber security regulations.  
10 MARKUS was given no authority to make changes but was required to go through a  
11 lengthy justification and process where the changes he attempted to implement were  
12 often vetoed by AR and ARH management.  
13  
14

15 86. Defendants committed these acts alleged herein maliciously, fraudulently,  
16 and oppressively, in bad faith with the wrongful intention of injuring relator, from an  
17 improper and evil motive amounting to malice, and/or in conscious disregard of relator's  
18 rights by reason thereof relator is entitled to an award of punitive damages, the amount of  
19 such damages to be established by proof at trial.  
20

21 87. These misrepresentations entitle relator to a civil penalty for double the  
22 damages resulting from defendants' misrepresentations pursuant to Labor Code § 972.  
23

24 88. Relator is entitled to an award of his reasonable attorneys fees in  
25 connection with the prosecution of this action.  
26

27 **COUNT SIX**  
**WRONGFUL TERMINATION IN VIOLATION OF PUBLIC POLICY**

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28

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.

1           95. Relator is informed and believes, and based thereon alleges, that the  
2 outrageous conduct of defendants, described above, was done with oppression and malice  
3 and was ratified by the other individuals who were managing agents of those directly  
4 responsible. These unlawful acts were further ratified by the defendant employers and  
5 done with a conscious disregard for relator's rights and with the intent, design and  
6 purpose of injuring relator. By reason thereof, relator is entitled to punitive or exemplary  
7 damages against defendants for their acts as described in this cause of action in a sum to  
8 be determined at the time of trial.  
9

10           WHEREFORE, relator respectfully requests this Court to enter judgment against  
11 defendants, as follows:  
12

- 13           (a) That the United States be awarded damages in the amount of three times the  
14 damages sustained by the United States because of the false claims and fraud  
15 alleged within this Complaint, as the Civil False Claims Act, 31 U.S.C. §§ 3729 *et*  
16 *seq.* provides;  
17
- 18           (b) That unjust enrichment damages are awarded to the United States for the money  
19 defendants' were not required to spend to keep their computer systems DFARS and  
20 NASAFARS compliant as required by their contracts with the federal government;  
21
- 22           (c) That civil penalties of \$11,000 are imposed for each and every false claim that  
23 defendants presented to the United States and/or its grantees;  
24
- 25           (d) That pre- and post-judgment interest is awarded, along with reasonable attorneys'  
26 fees, costs, and expenses, which the relator necessarily incurred in bringing and  
27 pressing this case;  
28

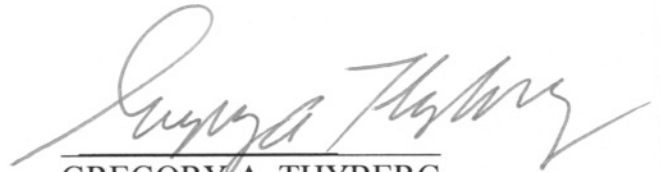
- 1 (e) That the Court grant permanent injunctive relief to prevent any recurrence of the  
2 False Claims Act for which redress is sought in this Complaint;  
3  
4 (f) That the relator be awarded the maximum amount allowed to him pursuant the  
5 False Claims Act; and  
6  
7 (g) For Count four, that relator be granted all relief necessary to make him whole,  
8 including but not limited to two times his back pay and other compensatory  
9 damages sustained as a result of defendants' harassment and retaliation;  
10  
11 (h) Punitive damages; and,  
12  
13 (i) That this Court award such other and further relief as it deems proper

14 **DEMAND FOR JURY TRIAL**

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

17 DATED: September 13, 2017

18 THYBERGLAW

19 

20 GREGORY A. THYBERG  
21 Attorney for Relator  
22 BRIAN MARKUS  
23  
24  
25  
26  
27