

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

7
8 ATTORNEYS FOR RELATOR, BRIAN MARKUS

9 UNITED STATES DISTRICT COURT
10 FOR THE EASTERN DISTRICT OF CALIFORNIA

11 UNITED STATES OF AMERICA:) Civil Action No. 2:15-cv-2245 WBS-AC
12 *ex rel.*)
13 BRIAN MARKUS)
14 Plaintiffs,) SECOND AMENDED FALSE CLAIMS
15 vs.) ACT COMPLAINT AND DEMAND FOR
16 AEROJET ROCKETDYNE HOLDINGS,) JURY TRIAL
17 INC., a corporation and AEROJET)
18 ROCKETDYNE, INC. a corporation.)
19 Defendants)
20)
21)

22 **I. Introduction**

23 1. Brian Markus (the “relator”) brings this action on behalf of the United
24 States of America against defendants AEROJET ROCKETDYNE HOLDINGS, INC.
25 (“ARH”) and AEROJET ROCKETDYNE INC. (“AR”) for treble damages and civil
26 penalties arising from defendants’ false statements and false claims in violation of the
27

1 Civil False Claims Act, 31 U.S.C. §§ 3729 *et seq.* The violations arise out defendants
2 fraudulently inducing the federal government to grant them contracts to provide goods
3 and services to the federal government including, the National Aeronautics and Space
4 Administration (“NASA”) and the Department of Defense (“DOD”), when they knew
5 they were not complying with federal acquisition regulations that were required as a
6 material terms of those contracts.
7

8
9 2. As required by the False Claims Act, 31 U.S.C. § 3730(b)(2), the relator
10 served the Attorney General of the United States and to the United States Attorney for the
11 Eastern District of California a statement of all material evidence and information related
12 to the complaint. This disclosure statement is supported by material evidence known to
13 the relator at his filing establishing the existence of defendants’ false claims. Because the
14 statement includes attorney-client communications and work product of relator’s
15 attorneys, and is submitted to the Attorney General and to the United States Attorney in
16 their capacity as potential co-counsel in the litigation, the relator understands this
17 disclosure to be confidential.
18
19

20 3. On June 6, 2018, the United States Government filed a Notice indicating it
21 was declining to intervene in this action. Relator continues this action on behalf of
22 himself and the United States Government.
23

24 **II. Jurisdiction and Venue**

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

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

2 5. Venue is proper in this District pursuant to 31 U.S.C. § 3732(a), because
3 the acts proscribed by 31 U.S.C. §§ 3729 *et seq.* and complained of herein took place in
4 this district, and is also proper pursuant to 28 U.S.C. § 1391(b) and (c), because at all
5 times material and relevant, defendants transact and transacted business in this District.
6

7 **Parties**

8 6. Relator Brian Markus (“MARKUS”) is a citizen of the United States and a
9 resident of the State of California. From to June 30, 2014 to September 14, 2015, relator
10 worked for defendants as the senior director of Cyber Security, Compliance & Controls.
11 The relator brings this action based on his direct, independent, and personal knowledge
12 and also on information and belief.
13
14

15 7. Defendants AEROJET ROCKETDYNE HOLDINGS, INC. (“ARH”) and
16 AEROJET ROCKETDYNE, INC. (“AR”) are in the business of developing and
17 manufacturing products for the aerospace and defense industry including aerospace
18 propulsion systems, precision tactical weapons systems, and armament systems including
19 warhead and munitions applications. Defendants’ primary customers for these products
20 are the United States government who purchases these products pursuant to contracts
21 defendants entered with the federal government including the Department of Defense
22 (“DOD”) and the National Aeronautics and Space Administration (“NASA”).
23
24

25 8. Defendant AR is a wholly owned subsidiary of ARH. ARH uses AR to
26 perform its contract obligations. AR and ARH share computer systems, and have common
27

1 corporate officers that oversee the management of both corporations in performing the
2 federal contracts which are the subject of this false claims action as such both defendants
3 are jointly and severally liable for the conduct alleged herein.
4

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

6 **A. Background**

7 9. United States government contracts are subject to Federal Acquisition
8 Regulations (“FAR”). There are also agency specific regulations that supplement FAR.
9 Contracts entered with the Department of Defense (“DOD”) are subject to Defense
10 Federal Acquisition Regulations (“DFARS”) and contracts entered with the National
11 Aeronautics and Space Administration (“NASA”) are subject to NASA Federal
12 Acquisition Regulations (“NASA FARS”)
13

14 10. The federal government requires that all companies that enter contracts to
15 provide good or services to the DOD or NASA meet minimum standards to prevent
16 unauthorized access and disclosure of unclassified controlled technical information
17 (“UCTI”) or sensitive but unclassified information (“SBU”) belonging to NASA or the
18 DOD that will be stored on the company’s computer system in the course of the company
19 performing the government contract. These minimum standards are set forth in the
20 DFARS and NASA FARS regulations and apply to all federal contracts where the
21 contractor will have access to UCTI or SBU belonging to the federal government.
22

23 11. Prior to November 18, 2013, the federal government ensured compliance
24 with these regulations by incorporating terms in federal contracts setting minimum levels
25 of cyber security to make sure that contractors’ information systems were protected from
26 unauthorized access. Contractors were required to meet the minimum standards for cyber
27 security set forth in the DFARS and NASA FARS regulations in order to be awarded a
28

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

3 12. The DFARS and NASAFARS regulations required that contactors meet
4 cyber security standards standards specified by the National Institute of Standards and
5 Technology (“NIST”). Contracting officers at NASA and the DOD were required to
6 review contracts to see if there would be access to UCTI or SBU and to insert terms in
7 the contract to make sure the DFARS and NASA FARS regulations relating to cyber
8 security were incorporated as a term of the contract. In the case of the DOD, the agency
9 would prepare a form DD-254 that was incorporated in the contract
10

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

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

19 15. The DOD REG, which was effective immediately imposed two
20 requirements: (1) that contractors provide adequate security for information systems that
21 contain unclassified controlled technical information; and (2) that they report cyber
22 incidents or any compromise of information systems.
23

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

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

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

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

11 20. The NIST SP 800-53 standards were originally implemented to apply to
12 contractors operating computer systems on behalf of the federal government. In June of
13 2015 the DOD and NIST published a new set of rules specifically tailored to defense
14 contractors storing controlled unclassified technical information on defense contractor
15 computer systems, NIST 800-171. NIST 800-171 incorporated 109 cyber security
16 controls from the NIST 800-53 standard.

17 21. In August 2015 the DOD issued an interim rule modifying DFARS Clause
18 252.704-7012. Under the modified rule defense contractors were only required to meet
19 the NIST 800-171 cyber security standards, which were less stringent than the
20 requirements of NIST 800-53. When the NIST 800-171 standards were not met the clause
21 required that defense contactors provide: “Alternative but equally effective security
22 measures used to compensate for the inability to satisfy a particular requirement and
23 achieve equivalent protection approved in writing by an authorized representative of the
24 Department of Defense Chief Information Officer (“DoD CIO”) prior to contract award.”
25
26
27
28

1 22. The DOD amended the interim DFARS Clause 252.704-7012 effective
2 December 31, 2015. The new rule required contractors be fully compliant with the NIST
3 800-171 standards as soon as practical but not later than December 31, 2017. For all
4 contracts awarded prior to October 1, 2017, the contractor was required to notify the DoD
5 CIO via email within 30 days of the contract award, of any security requirements specified
6 by NIST SP 800-171 not implemented at the time of contract award.

7
8 23. The contractor was required to submit requests to vary from the NIST SP 800-
9 171 standards in writing to the DoD CIO. The contractor was only excused from a security
10 control if it was “adjudicated by an authorized representative of the DoD CIO to be
11 nonapplicable or to have an alternative, but equally effective, security measure that may be
12 implemented in its place.”

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

18 25. Contractors awarded contracts from NASA must comply with NASA FAR
19 regulations. NASA FAR 1852.204-76 requires that 264 of the NIST SP 800-53 moderate
20 control be incorporated in NASA contracts where the contractor would store sensitive but
21 unclassified information (SBU) belonging to the federal government on their computer
22 system while performing a contract for NASA. This regulation makes no provision for the
23 contractor use alternative controls or protective measures.
24
25

26 26. NASA FAR 1804.470-4(a) requires that this clause incorporated in every
27 NASA contract where the contractor has access to or stores SBU belonging to the federal
28

1 government on its computer system. NASA FARS 1852.204-76 states in pertinent part: “ (a)
2 The contractor shall protect the confidentiality, integrity, and availability of NASA
3 Electronic Information and IT resources and protect NASA Electronic Information from
4 unauthorized disclosure. (b) This clause is applicable to all NASA contractors and sub-
5 contractors that process, manage, access, or store unclassified electronic information, to
6 include Sensitive But Unclassified (SBU) information, for NASA in support of NASA's
7 missions, programs, projects and/or institutional requirements.”
8
9

10 27. Government contracting officers have no authority to enter a contract
11 unless the contractor is complying with DFARS and NASA FARS regulations that are
12 legally required to be incorporated in the contract. Federal Acquisition Regulation
13 (“FAR”) 1.602-1(b) provides that: “No contract shall be entered into unless the
14 contracting officer ensures that all of the requirements of law, executive orders,
15 regulations, and all other applicable procedures, including clearances and approvals, have
16 been met.”
17
18

19 28. Compliance with DFARS and NASA FARS regulations that are that are
20 required by law to be incorporated in a federal contracts are non-waiverable contract
21 terms. According to FAR 1.602-3 (c) (3), the Government can only ratify a change in a
22 contract obligation if “The resulting contract would otherwise have been proper if made
23 by an appropriate contracting officer.”
24
25

26 B. Wrongful Acts by Defendants
27
28

1 29. Defendants have entered multiple contracts with the federal government,
2 and as subcontractors on contracts with the federal government, which required that
3 defendants meet the cyber security standards set forth in the DFARS Clause 252.704-
4 7012 and NASA FARS Clause 1852.204-76 even though defendants knew their
5 information systems did not meet these cyber security requirements.
6

7 30. Defendants fraudulently entered contracts knowing they did not meet the
8 minimum standards required to be awarded a contract and they misled the government
9 concealing their non-compliance with these regulations.
10

11 31. Defendants also fraudulently entered subcontracts with prime contractors
12 who were working on federal contracts that required that they comply with the DFARS
13 and NASA FARS cyber security regulations.
14

15 32. MARKUS started working for defendants on June 30, 2014 as the senior
16 director of Cyber Security, Compliance & Controls. He was hired by AR to improve the
17 cyber security of defendants' computer systems.
18

19 33. Relator was promised a budget of 10 to 15 million dollars to improve the
20 security of defendants' computer systems. He was promised an internal staff of 5 to 10
21 employees and external staff of up to 25 contract employees.
22

23 34. When relator started working for defendants, he was given a budget of only
24 3.8 million dollars rather than 10 million. Defendants provided an internal staff of two
25 employees not the five to ten that were promised. Instead of twenty-five contract
26 employees, defendants provided only seven.
27
28

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

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

7 37. Relator had previously worked in the area of cyber security for other
8 defense contractors and so he was familiar the federal acquisitions regulations related
9 cyber security.
10

11 38. Defendants were not compliant with the NASA FARS or DFARS cyber
12 security requirements including DFARS Clause 252.704-7012 and NASA FARS Clause
13 1852.204-76 when relator started his employment June 30, 2014. Based on the state of
14 defendants' computer systems at the time relator began his employment, relator is
15 informed and believes thereon alleges defendants' computer systems had not been
16 compliant with the DFARS or NASA FARS cyber security requirements for several
17 years.

18 39. In 2013, ARH purchased Rocketdyne from Pratt & Whitney. At the time of
19 the purchase Pratt & Whitney represented that its Rocketdyne division was compliant
20 with the DFARS and NASA FARS regulations related to cyber security. After the
21 purchase, the computer systems of Rocketdyne were merged with defendants' computer
22 systems so that after 2013, Rocketdyne was no longer compliant with the NASA FARS
23 1852.204-76 or DFARS Clause 252.704-7012 cyber security requirements.
24

25 40. Defendants' were aware of breaches of their computer system in 2013 and
26 2014 by nation state sponsored threat actors. Defendants reported those breaches to the
27 federal government in as required by DFARS regulations and DFARS Clause 252.704-

1 7012. In reporting those breaches defendants concealed the fact that their computer
2 system was not compliant with the NASAFARS 1852.204-76 or DFARS Clause 252.704-
3 7012 cyber security requirements.

4 41. When questioned by the government about its cyber security, defendants
5 gave the government misleading information. For example, they were asked if they had a
6 certain piece of security equipment, they would say “yes,” even though the equipment
7 was sitting in a box and not connected to their computer system. Defendants represented
8 they had cyber security software/hardware installed to protect the systems when in reality
9 the software/hardware in question only covered part of the environment leaving
10 defendants vulnerable to a cyber attack. In some cases, they claimed compliance only
11 considering the primary control and not the sub-controls, which were clearly not being
12 met.
13

14 42. At the time of the 2014 cyber security breach of its computer system, AR
15 was working was working on a DOD contract through the prime contractor Lockheed
16 Martin to supply the booster motor technology for the Terminal High Altitude Area
17 Defense System (“THAAD”). The THAAD system is used to defend the United States
18 and deployed forces and allies against ballistic missiles during all phases of flight. UCTI
19 related to THAAD system was exposed to disclosure as a result of this computer breach.
20

21 43. In early 2014, Emagined Security Inc. (“EMAGINED”), an outside
22 consulting firm, performed an audit to determine NASA FARS and DFARS compliance
23 and determine costs to obtain compliances. It was found that defendants were less than
24 25% compliant.

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

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

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

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

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

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

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

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

15 52. The EMAGINED report indicated that for defendants to reach 100%
16 compliance would take a combination of technical solutions, business process
17 improvements and a fundamental change in defendants' strategic direction. EMAGINED
18 stated for defendants to achieve compliance "... will require a shift in how the business
19 addresses contractual and regulatory responsibilities..." The report outlined estimated
20 costs in the amount of \$34,548,866 over a five-year period, which would be required for
21 defendants' to make their computer systems compliant with the DFARS cyber security
22 requirements. AR was considering outsourcing its IT department but the EMAGINED
23 report indicated that this would only clear up 10% of the compliance deficiencies.
24
25
26
27
28

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

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

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

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

23 57. The EY assessment team identified five unique pathways to compromise
24 defendants' system. Defendants' systems contained publically known information system
25 vulnerabilities, which are typically patched as part of an organization's threat and
26

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

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

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

10 60. AR advised the government that they were compliant with the majority of
11 the DFARS Clause 252.204-7012 requirements when they were only 24% compliant with
12 the NIST SP 800-53 moderate controls they were required to have in place. AR just
13 reported their 60 of the top controls to make it appear they were close to compliant but
14 did not report its status on the full 264 controls that would have revealed they were 75%
15 non-compliant.
16

17 61. AR told the government it had 43 controls that it described in the letter as
18 "Controls in Place Enhancements and Refinement on-Going." In its letter AR advised
19 the government "AR has implemented the control(s) but needs to implement
20 enhancements to strengthen the controls as necessary." This statement was false and
21 misleading because none of the 43 controls listed was compliant with the NIST SP 800-
22 53 controls that were required by DFARS Clause 252.204-7012.
23

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

1 63. AR was represented that 6 controls had partial a controls in place. AR
2 referred to these controls as ‘Partial Controls in place Strengthening, Enhancements and
3 Refinement On-going/needed’ for which AR stated: “AR had implemented the control(s)
4 to a degree but needs to investigate further on how to satisfy the full intent of the controls
5 in the environment.” As to these controls AR had no control place. AR claimed partial
6 compliance for having equipment or software that it had not installed. Relator continually
7 challenged AR on the use of these types of false and misleading statements AR was
8 making to the government regarding its DFARS compliance.
9

10 64. In the letter AR wrote: “ It is important to note that AR is compliant with
11 the majority of the clauses requirements. Please be assured that AR will make every
12 effort to prevent a data breach while we work aggressively to strengthen the controls and
13 implement additional protection measures”. AR made this statement when it knew if was
14 75% non-compliant with the NIST SP 800-53 requirements and AR’s computer system
15 had already been breached by foreign nation states and AR had not taken effective
16 measures to prevent a future breach.

17 65. AR was awarded this contract following these false and misleading
18 statements on September 29, 2014. The contract required that AR comply with DFARS
19 Clause 252.204-7012, which was incorporated by reference in Schedule K of the
20 contract. At the time AR signed the contract it was 75% non-complaint with the DFARS
21 cyber security requirements.
22

23 66. In May 2015, AR sought a waiver of some of the DFARS Clause 252.704-
24 7012 cyber security requirements in seeking a contract from the DOD.

25 67. Federal contracting officer, Laurie Hewitt (“HEWITT”), contacted Vicki
26 Michetti (“MICHETTI”) of the DoD CIO office via email to seek a waiver for an urgent
27 contract, W31P4Q-15-C-0016. MICHETTI advised HEWITT that the DoD CIO’s could
28

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

7
8 68. Relator is informed and believes and thereon alleges that AR was told by
9 the government that the DFARS requirements were non-waivable and that AR was
10 awarded contract W31P4Q-15-C-0016 and that it stored UCTI information related to this
11 contract on its system even though it was not fully compliant with DFARS Clause
12 252.704-7012.

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

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

20
21 71. AR provided the DOD with a table of controls that was truncated to omit
22 the controls it was not complying with. AR advised the DoD CIO it had seven DFARS
23 controls that were "in place and compliant." But for most of the controls AR indicated
24 "controls in place/ enhancements and refinements ongoing." AR also indicated it had five
25 controls listed partial controls in place.

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

1 erroneously conclude that AR was possibly compliant when AR was 75% non-compliant
2 with the DFARS requirements. In her email to HEWITT of May 21, 2015, MICHETTI
3 stated: “Based on the documentation provided by the contractor, we determined that they
4 are not compliant with the DFARS Clause 252.204-7012. However, it may be a relatively
5 simple matter for the contractor to become compliant.... It is possible that they are
6 compliant but they are either not fully describing what they are doing, or are
7 misinterpreting the requirements.”
8

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

15 74. One of the cyber security controls required that AR monitor its email
16 accounts to make sure employees were not sending UCTI or SBU out of its system.
17 Compliance required that all emails be monitored to make sure employees were not
18 sending an email with UCTI or SBU information. AR only monitored emails going out
19 to a couple major domains like Gmail or Yahoo and then advised the government that it
20 was compliant with that control.
21

22 75. DFARS controls prohibited AR from sending information between its
23 locations over the Internet when it was not encrypted. AR took the position that it could
24 send the information unencrypted because it was going to a site that was encrypted even
25 though EMAGINED showed AR a white paper that showed how this information could
26 be intercepted.
27

1 76. In 2015, AR was working on a DOD contract related to ground based
2 strategic defense (“GBSD”), the United States intercontinental missile defense system.
3 DFARS required that there be two levels of security to access the computer system. AR
4 was required to have the employee use not only a user name and password to access the
5 system but also to use a magnetic card but AR had no card reader. AR installed a card
6 reader and told the government that they were compliant with this DFARS requirement
7 and then removed the card reader a few months later.
8

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

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

15 79. AR submitted these questions to EMAGINED to prepare a response.
16 EMAGINED provided AR with a response that indicated they were not DFARS or
17 NASA FARS compliant and not eligible to work on DOD contracts that required DFARS
18 252.204-7012 compliance.

19 80. Based on the fact that AR continued to get work from these defense
20 contractors, relator is informed and believes and thereon alleges that AR provided false
21 information to these prime contractors by changing the response they received from
22 EMAGINED.
23

24 81. In July 2015, ARH, VP and COO, Mark Tucker approached relator and VP
25 & CIO Jose Ruiz requesting that they sign a documents that they could send to
26 defendants’ contracts department indicating that defendants’ computer system was now
27 compliant with the NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012.
28

1 82. When relator told defendants he could not sign the document until
2 defendants were compliant with these cyber security requirements, Mr. Tucker brushed
3 his comment off stating that it was not really a big deal and that all that would happen if
4 they were not compliant with these federal acquisition regulations is they might get
5 audited. He also stated that the government has never shutdown one of their programs for
6 being out of compliance in the past. Relator refused to sign the documents and he
7 advised defendants that by signing these documents he would be committing a fraud on
8 the government and he could lose his national security clearance. Relator contacted the
9 companies Ethics hotline and filed a formal report.
10

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

13 **DOD Contracts**

14 84. AR signed at least six contracts with the DOD between February 23, 2014
15 and April 8, 2015 that incorporated the November 2013 version of DFARS Clause
16 252.704-7012. The clause was incorporated in schedule K of each of these contracts.

17 85. AR signed a contract to provide services to the Department of the Army on
18 February 24, 2014, Award ID # W31P4Q14C0075 (Department of the Army, Office
19 W6QK ACC RSA) which was valued at \$ 33,070,971.
20

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

24 87. AR signed a contract to provide services to the Department of the Air Force
25 on September 29, 2014, Parent Award ID #FA865013D2335, Award Id. 0002
26 (Department of the Air Force, Office FA8650 USAF AFMC AFRL/RQK) valued at
27 \$8,326,290.
28

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

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

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

10 91. AR signed two contracts that required it comply with August 2015 interim
11 rule modifying DFARS Clause 252.704-7012 so as to require it comply with the NIST SP
12 800-171 cyber security standards.

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

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

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

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

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

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

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

9 99. AR did not submit requests in writing to deviate from all of the NIST SP
10 800-171 standards where it was not compliant.

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

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

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

20 103. AR entered these contracts knowing it was not providing “Adequate
21 Security” because its system had already been breached by foreign nation states in 2013
22 and 2014 and it knew it was no more than 25% compliant with the NIST controls
23 required to protect UCTI.
24
25
26
27
28

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

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

9
10 116. At the time AR solicited these contracts AR was not compliant with the NIST
11 SP 800-53 moderate cyber security controls. As of October 2015 AR was only compliant with
12 63 of the 264 required controls. As of the end of November 2015 AR was only compliant
13 with 78 of the 264 controls.

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

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

22
23 119. AR tried to get other IT personnel including Jens Landreth and David
24 Chamberlin to sign these NASA reports but they refused. AR kept circulating the report until
25 they could find someone to sign it.

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

1 125. Defendants also concealed information from the government regarding the
2 state of its compliance with NASA FARS Clause 1852.204-76 and DFARS Clause
3 252.704-7012 because they knew they were not eligible to participate in these contracts
4 and that if they disclosed this information they would not get the contract award.
5

6 126. Defendants obtained subcontracts that were subject to federal acquisition
7 regulations, NASA FARS Clause 1852.204-76 and DFARS Clause 252.704-7012, related
8 to cyber security by falsely representing that they were compliant with those regulations.
9 These prime contractors included Boeing, Lockheed Martin and Raytheon.
10

11 127. The federal government was misled by defendants' false statements and
12 would never have entered these contracts with defendants had the government been
13 aware that defendants were not complying with the NASA FARS Clause 1852.204-76 and
14 DFARS Clause 252.704-7012 cyber security regulations. These regulations prohibited
15 the federal government from entering contract with a party that would have access to
16 UCTI or SBU belonging to the federal government unless that party was complying with
17 these cyber security regulations.
18
19

20 128. Compliance with these regulations was material to the federal
21 government's decision to enter these contracts as no federal contracting officer has
22 authority to enter a contract where the contractor is not complying with the law. Federal
23 Acquisition Regulation ("FAR") 1.602-1(b) provides that: "No contract shall be entered
24 into unless the contracting officer ensures that all of the requirements of law, executive
25
26
27
28

1 orders, regulations, and all other applicable procedures, including clearances and
2 approvals, have been met.”

3
4 129. As a result of defendants’ false representations and material omissions the
5 federal government paid out money on contracts they would have never entered.

6 130. As a result of these false representations and material omissions the federal
7 government paid out more money to defendants than they would not have otherwise paid
8 as the government would have demanded a discount on the money they paid defendants
9 for their goods and services had they known defendants were not complying with these
10 federal acquisition regulations.
11

12 131. The federal government has also been damaged as UCTI and SBU
13 belonging to the federal government has been made available to unauthorized parties,
14 including technical work product information such as engineering designs that the
15 government was paying defendants to create.
16

17
18 **COUNT TWO**
FALSE OR FRAUDULENT STATEMENT OR RECORD 31 U.S.C. §3729(a)(1)(B)

19 132. Relator re-alleges and incorporates the allegations of paragraphs 1–131 as
20 if fully set forth herein.
21

22 133. Defendants’ knowingly made, used, or verified a false record or statement
23 that was material to the false or fraudulent claim.
24

25 134. Defendants signed contracts with the DOD and NASA representing to the
26 government that they were DFARS and NASA FARS compliant when they knew they
27 were not. They submitted IT Security Management Plans indicating that that were
28

1 complying with NASA FARS Clause 1852.204-76 when they were not. AR also sent
2 monthly reports for its NASA contracts certifying it was complying with NASA FARS
3 Clause 1852.204-76 when it was not.
4

5 135. FAR 52.246-15 required that every invoice AR submitted to the government
6 for payment have a certification certifying that the supplies or services were in accordance
7 with all applicable requirements and the supplies or services are of the quality specified and
8 conform in all respects with the contract requirements.
9

10 136. Relator is informed and believes and thereon alleges that AR submitted
11 invoices to the government for payment for the services on the contracts alleged herein and
12 that AR falsely certified in those invoice that the services conformed in all respects with the
13 contract requirements when it knew it was not complying with NASA FARS Clause
14 1852.204-76 and DFARS Clause 252.704-7012 including providing “Adequate Security”
15 to protect UCTI belonging to the federal government.
16

17 137. All of these statements were made to get the federal government to make
18 payments to which defendants were not entitled or would have been substantially
19 discounted had the government been aware that defendants were not compliant with the
20 federal acquisition regulations related to cyber security, NASA FARS Clause 1852.204-
21 76 and DFARS Clause 252.704-7012.
22

23 138. This course of conduct violated the False Claims Act, 31 U.S.C. §§ 3729 *et*
24 *seq.*
25

26 139. The federal government was unaware of the falsity of the claims and/or
27

1 statements, and acted in reliance on the accuracy thereof.

2 140. The federal government was damaged as a result of defendants' conduct as
3 they paid defendants for bills and invoices they would not have otherwise paid.
4

5 141. The federal government was damaged because they paid defendants more
6 than their good services were worth given defendants' failure to comply with the federal
7 acquisition regulations that were required by these contracts. The federal government
8 would have demanded a discount if it had known defendants were not complying with the
9 cyber security regulations required by the contracts..
10

11 142. The federal government has also been damaged as its UCTI and SBU has
12 been made available to unauthorized parties, including technical work product
13 information such as engineering designs that the government was paying defendants to
14 create.
15

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

18 143. Relator re-alleges and incorporates the allegations of paragraphs 1–142 as
19 if fully set forth herein.
20

21 144. Defendants and their officers and managing agents combined, conspired,
22 and agreed together to defraud the United States by knowingly submitting false claims to
23 the United States and to its grantees for the purpose of getting the false or fraudulent
24 claims paid or allowed and committed the other overt acts set forth above in furtherance
25 of that conspiracy, all in violation of 31 U.S.C. § 3729(a)(1)(C), causing damage to the
26 United States.
27

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

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

5 146. On September 14, 2015, *qui tam* plaintiff MARKUS was terminated in his
6 employment by defendants as a result of his lawful acts done in furtherance of this action,
7 including complaints to management regarding the false claims described herein and his
8 refusal to falsely sign a document indicating that defendants were compliant with DFARS
9 and NASA FARS. MARKUS' termination was in violation of 31 U.S.C. § 3730(h).
10

11 147. As a direct and proximate result of this unlawful termination, MARKUS
12 has suffered emotional pain and mental anguish, together with serious economic
13 hardship, including lost wages and special damages associated with his efforts to obtain
14 alternative employment, in an amount to be proven at trial.
15
16

17 **COUNT FIVE**
18 **MISREPRESENTATION IN VIOLATION OF LABOR CODE § 970**

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

21 149. Defendant made false promises to MARKUS in order to induce him to
22 move from the southern California where he was working for Raytheon to Northern
23 California to work for AR.
24

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

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;

1 (h) Punitive damages; and,

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

3

4

DEMAND FOR JURY TRIAL

5

6

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

7

8

DATED: January 4, 2019

THYBERGLAW

9

10

11

12

13

14

15

16

17

18

19

20

21

22

23

24

25

26

27

28

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