UNITED STATES DISTRICT COURT
FOR THE SOUTHERN DISTRICT OF NEW YORK

UNITED STATES OF AMERICA, *ex. rel.* WILLIAM BARLOW, **Plaintiff,** **v.** **INTERNATIONAL BUSINESS MACHINES CORP. and AT&T, INC.,** **Defendants.**	**Case No.:** **JURY TRIAL DEMANDED** **FILED IN CAMERA AND UNDER SEAL**

COMPLAINT FOR VIOLATION OF THE FEDERAL FALSE CLAIMS ACT

Qui tam Relator, WILLIAM BARLOW (hereinafter referred to as "Relator"), by and through his undersigned counsel, on behalf of the United States of America, for their Complaint against Defendants, INTERNATIONAL BUSINESS MACHINES CORP. (hereinafter referred to as "Defendant" or "IBM") and AT&T, INC. (hereinafter referred to as "AT&T") (hereinafter collectively referred to as the "Defendants"), alleges, based upon personal knowledge, relevant documents and information and belief, as follows:

INTRODUCTION

1. This is an action to recover damages and civil penalties on behalf of the United States of America from false and/or fraudulent statements, records and claims made and caused to be made by Defendants and/or their agents, employees and co-conspirators in violation of the Federal False Claims Act, 31 U.S.C. § 3729, *et seq.* (hereinafter referred to as the "FCA").

2. The term "cloud" or "cloud computing" is the on-demand availability of computer system resources, especially data storage and computing power, without direct active management by the user. The term is generally used to describe data centers available to many users over the

Internet. IBM, along with its venture partner AT&T, operate one of the largest cloud computing systems in the world. IBM and AT&T hold many federal contracts in which they store sensitive and confidential data on behalf of federal agencies.

3. Both IBM and AT&T have failed to implement the necessary computing protocols including, but not limited to cybersecurity, communications and cloud computing protocols, throughout their core networks, as mandated by the Federal Acquisition Regulations ("FAR"), Defense Federal Acquisitions Regulations ("DFARS"), National Institute of Standards and Technology ("NIST") Special Publication ("SP") 800-63 and NIST SP 800-171.

4. Because IBM and AT&T have government contracts related to the storage of government records and data, there is liability under the False Claims Act.

5. IBM's core network is run by AT&T. IBM's network is what is referred to as a "flat network" as it has little to no network segmentation. In layman's terms, this means that a user in Los Angeles, California can access the same data as a user in Shanghai, China without any additional restrictions.

6. Every IBM employee and every IBM location around the globe connects to the Power 9 Network to conduct the day-to-day business of IBM. This includes new product development, software development the creation of intellectual property and patents, and work product involved in the response to RFPs.

7. For purposes of the False Claims Act and government customers, it also includes the storage and transmission of customer sensitive data used in the day-to-day business activities of IBM.

8. Upon information and belief, this includes data used in designing, building, and developing products that are purchased by the Federal Government along with data created and/or maintained/stored in providing services to the Federal Government.

9. Customer owned networks are often connected to the IBM network through trust relationships, jump servers, and boundary firewalls. These tools allow IBM employees to directly access customer networks from the Power 9 Network in order to provide system administration, maintenance and manage cloud computing environments.[1]

10. Federal Government data is stored in a separate security zone on the IBM network, but is wholly accessible via a jump server, and can be accessed either through a computer station/laptop or via IBM's cloud-based network

11. As such, IBM's cloud-computing and cybersecurity systems are all a part of the core network (hereinafter collectively referred to as the "IBM Core Network") that is at issue in this matter.

12. Similarly, as AT&T runs the IBM network on behalf of IBM, AT&T's communications, cloud-computing and cybersecurity systems are all a part of the core network (hereinafter collectively referred to as the "AT&T Core Network") that is at issue in this matter. (Together, the IBM Core Network and AT&T Core Network are hereinafter referred to as the "Core Networks")

13. On January 19, 2019, IBM acquired Red Hat, Inc. ("Red Hat") for $34 billion. Red Hat is, in layman's terms, a computer operating system (similar to Windows, MacOs, Linux, etc.) that is utilized pervasively throughout the Federal Government and the IBM Core Network and is one of the most popular operating systems used in cloud computing around the globe.

---

[1] https://www.ibm.com/support/knowledgecenter/en/SSGTJF/com.ibm.help.omcloud.getstart.doc/productconcepts/t_omc_connect_jumphosts.html

14. Upon information and belief, IBM never disclosed any of its security issues to government regulators during the acquisition of Red Hat even though IBM was aware that it was acquiring an asset that foreign adversaries - the very adversaries that had previously exploited the Core Networks - would be interested in exploiting.

15. As set forth in greater detail throughout this Complaint, both IBM and AT&T have knowledge that the Core Networks were improperly accessed and had data exfiltrated by foreign adversaries as well as unknown actors.

16. The data breaches are so large and the Core Networks so poorly designed that neither IBM nor AT&T knows exactly what data was breached, who breached the data, where the data was breached, when the data was breached or whether any data was exfiltrated, altered and/or modified in any respect.

17. IBM and AT&T would be able to determine all of this if they maintained the requisite and necessary audit control logs, which they do not. For purposes of the False Claims Act, both the failure to disclose data breaches and the failure of the Core Networks to meet government security standards violate a wide range of federal cybersecurity rules and regulations as outlined below.

18. IBM and AT&T fraudulently submitted invoices and submissions for reimbursement from the Federal Government and the United States Department of Defense ("DOD") by mispresenting that IBM and AT&T were in compliance with the applicable regulations and standards.

19. As part of the payment process, IBM, and upon information and belief, AT&T must certify that they are in compliance with all terms of their contract. A standard term of all government services contracts with the Federal Government is that the contractor shall comply

with all federal laws and regulations.[2] Neither IBM nor, upon information and belief, AT&T were in compliance with the applicable regulations and standards, and both knew that they were not in compliance at the time they submitted the invoices and submissions for reimbursement.

20. In a 2017 SEC 10-K report, IBM falsely represented that nothing material has ever occurred from a cyber security perspective. "To date, **there has not been a cybersecurity attack that has had a material adverse effect on the company**, though there is no assurance that there will not be a cybersecurity attack that has a material adverse effect in the future."[3] (Emphasis added.)

21. Although IBM no longer makes such claims in their SEC reports, it also has not disclosed any subsequent breaches as required by federal law.

22. This *qui tam* case is brought against Defendants for (1) failing to maintain their Core Networks' systems in accordance with Federal regulations; (2) fraudulently certifying that their Core Networks' systems met the minimum criteria necessary to be awarded Federal Government and DOD contracts, in violation of multiple Federal regulations; and (3) failing to disclose numerous events of hacking, resulting in the unauthorized access and exfiltration of federally protected, and potentially classified data to unknown users, in violation of Federal regulations.

23. Defendants' conduct alleged herein violates the FCA. The FCA was originally enacted during the Civil War. Congress substantially amended the FCA in 1986 – and again in 2009 and 2010 – to enhance the ability of the United States Government to recover losses sustained

---

[2] For example, see Section I.2.1.2(q) of Alliant 2 GWAC Unrestricted Contract that was awarded to IBM, which states "[IBM] shall comply with all applicable Federal, State and local laws, executive orders, rules and regulations applicable to its performance under this contract."

[3] IBM Corp. (2018). 2017 Form 10-K, available at https://www.sec.gov/Archives/edgar/data/51143/000104746918001117/a2233835z10-k.htm

as a result of fraud against it. The FCA was amended after Congress found that fraud in federal programs was pervasive and that the FCA, which Congress characterized as the primary tool for combating government fraud, needed modernization. Congress intended that the amendments would create incentives for individuals with knowledge of fraud against the Government to disclose the information without fear of reprisals or Government inaction, and to encourage the private bar to commit legal resources to prosecuting fraud on the Government's behalf.

24. The FCA prohibits: (a) knowingly presenting (or causing to be presented) to the Federal Government a false or fraudulent claim for payment or approval; (b) knowingly making or using, or causing to be made or used, a false or fraudulent record or statement material to a false or fraudulent claim; (c) knowingly making, using, or causing to be made or used, a false record or statement material to an obligation to pay or transmit money or property to the Government, or knowingly concealing or knowingly and improperly avoiding or decreasing an obligation to pay or transmit money or property to the Government; and (d) conspiring to engage in any of the activities set forth in (a) through (c) above. 31 U.S.C. §§ 3729(1)(A)-(C) and (G). Any person who violates the FCA is liable for a civil penalty for each violation, plus three times the amount of the damages sustained by the United States. 31 U.S.C. § 3729(a)(1).

25. The FCA allows any person having information about an FCA violation to bring an action on behalf of the United States, known as a *qui tam* suit, and to share in any recovery. The FCA requires that the *qui tam* Complaint be filed under seal and remain under seal for a minimum of 60 days (without service on the defendant(s) during that time) to allow the Government time to conduct its own investigation and to determine whether to join the suit.

26. United States government contracts are subject to FAR. There are also agency specific regulations that supplement FAR. Contracts entered with the DOD are subject to DFARS.

There are additional regulations and standards for United States government contracts that involve cloud products and services as set forth by the Federal Risk and Authorization Management Program ("FedRamp"). These rules are discussed in detail below.

27. The Federal Information Processing Standards ("FIPS") were issued by the National Institute of Standards and Technology ("NIST") after approval by the Secretary of Commerce pursuant to the Federal Information Security Management Act of 2002 ("FISMA").

28. FIPS 200, titled "Minimum Security Requirements for Federal Information and Information Systems" is applicable to:

> (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and
>
> (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). Agency officials shall use the security categorizations described in FIPS Publication 199 whenever there is a federal requirement to provide such a categorization of information or information systems.[4]

29. FIPS 200 specifies the minimum-security requirements for non-military federal information systems. Any contractor that creates or otherwise handles information for Federal agencies, must comply with FIPS 200's requirements. IBM and AT&T are subject to FIPS 200 as alleged in greater detail below.

I. FARs And DFARS Regulations and Standards

[4] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.200.pdf

30. The Federal Government requires that all companies that contract with it to provide goods or services to the Federal Government and DOD meet minimum standards to prevent the unauthorized access and disclosure of Controlled Unclassified Information ("UCI") , Unclassified Controlled Technical Information ("UCTI") or Sensitive but Unclassified Information ("SBU") (collectively referred to as "Protected Information") belonging to the government that will be stored with the contractor's computer system in the court of the contractor performing the government contract.

31. These minimum standards are set forth in the FAR and DFARS regulations and apply to all federal contracts where the contractor will have access to UCI or SBU belonging to the Federal Government.

32. 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.

33. Contractors were required to meet the minimum standards for cyber security set forth in the FAR and DFARS regulations in order to be awarded a government contract where they would have access to Protected Information belonging to the Federal Government.

34. The FAR and DFARS regulations required that contractors meet cyber security standards specified by the National Institute of Standards and Technology ("NIST").

35. Contracting officers with the Federal Government and DOD were required to review contracts to see if there would be access to Protected Information and to insert terms in the contract to make sure the FAR and DFARS regulations relating to cyber security were incorporated as a term of the contract.

36. In the case of the DOD, the agency would prepare a form set forth in DFARS part 253[5] that are incorporated in the contract.

37. On November 18, 2013, the DOD issued a regulation, 78 Fed. 69273 ("DOD REG"), which intensified the safeguards required by government defense contractors to protect their computer systems from cyberattacks that could result in unauthorized access and disclosure of UCTI belonging to the Federal Government.

38. UCTI, according to the DOD REG, included software as defined by DFARS Clause 252.227-7013 with a military application that is subject to DOD access controls.[6]

39. Technical information included engineering data, drawings, specifications, standards, and technical reports. These regulations include cloud computing applications.

40. The DOD REG, which was effective immediately imposed two requirements:

(1) That contractors provide adequate security for information systems that contain UCTI; and

(2) That they report cyber incidents or any compromise of information systems.

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

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

[5] DFARS Section 253 forms are available at: https://www.acquisition.gov/dfars/part-253-%E2%80%93-forms

[6] NIST SP 800-145 defines cloud computing as "a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction." One cloud-based service model is the "Software as a Service (Saas)" model.

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

44. In the event a contractor was deficient in meeting the NIST SP 800-53 standards in any respect, the contractor was 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.

45. The NIST SP 800-53 standards were originally implemented to apply to contractors operating computer systems on behalf of the Federal Government.

46. In June of 2015, the DOD published a new set of rules specifically tailored to defense contractors storing controlled UCTI on defense contractor computer systems, NIST SP 800-171. NIST SP 800-171 incorporated 109 cyber security controls from the NIST 800-53 standard.

47. In August of 2015, the DOD issued an interim rule modifying DFARS Clause 252.704-7012. Under the modified rule, defense contractors were only required to meet the NIST 800-171 cyber security standards, which were less stringent than the requirements of NIST SP 800-53. *See infra*.

48. When the NIST SP 800-171 standards were not met, the clause required that defense contractors provide "[a]lternative but equally effective security measures used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection approved in writing by an authorized representative of the Department of Defense Chief Information Officer ("DOD CIO") prior to contract award."

49. The DOD amended the interim DFARS Clause 252.704-7012 effective December 31, 2015. The new rule required contractors to be fully compliance with the NIST SP 800-171 standards as soon as practical, but no later than December 31, 2017.

50. For all contracts awarded prior to October 1, 2017, the contractor was required to notify the DOD CIO via email within 30 days of the contract award, of any security requirements specific by NIST SP 800-171 not implemented at the time of the contract award.

51. The contractor was required to submit requests to vary from NIST SP 800-171 standards in writing to the DOD CIO.

52. The contractor was only excused from a security control if it was "adjudicated by an authorized representative of the DOD CIO to be nonapplicable or to have an alternative, but equally effective, security measure that may be implemented in its place."

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

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

55. Compliance with DFARS regulations, NIST SP 800-53 and NIST SP 800-171 that are required by law to be incorporated in a federal contract, are non-waivable contract terms.

56. According to FAR 1.602-3(c)(3), the Federal Government can only ratify a change in a contract obligation if "[t]he resulting contract would otherwise have been proper if made by an appropriate contracting officer."

57. IBM and AT&T have entered multiple contracts with the Federal Government, and as subcontractors on contracts with the Federal Government, which required that IBM and AT&T meet the cyber security standards set forth in DFARS Clause 252.704-7012, NIST SP 800-53 and NIST SP 800-171, even though IBM and AT&T knew their information systems did not meet these cyber security requirements.

58. Defendants fraudulently entered into contracts with the Federal Government knowing that they did not meet the minimum standards required to be awarded a contract and they misled the Federal Government by concealing their non-compliance with these regulations.

59. For example, IBM was awarded the "Alliant 2 GWAC Unrestricted Master Contract" that requires, amongst other things, compliance with "[FIPS], the '[SP] 800 series' guidelines published by NIST, and the requirements of FISMA." This same contract requires that IBM comply with FIPS 199, FIPS 200, NIST SP 800-37 and NIST SP 800-53.[7]

60. As set forth in greater detail below, IBM has numerous contracts with a wide array of Federal Agencies, including, but not limited to, the Centers for Medicaid and Medicare Services.

61. AT&T, for example, was awarded a GSA Schedule 20 contract, with contract number GS-35F-0249J. This contract requires, amongst other things, that AT&T's cloud services

[7] *See* Alliant GSA Contract conformed contract dated December 2019, pages 167-168, found at https://www.ibm.com/downloads/cas/YGDJKJB9.

"must be capable of satisfying each of the five NIST essential characteristics as outlined in [SP] 800-145."[8,9]

62. Additionally, AT&T was recently awarded a $984 million contract with the Department of Justice in 2019 to provide "management networking services including IP, voice, data, security, cloud access, and professional services."[10]

63. IBM and AT&T have also entered into entered contracts amongst themselves for cloud-based services. For example, in July of 2019, AT&T announced that it had entered into an agreement with IBM wherein "AT&T's Business unit will be IBM's primary provider of SDN and for IBM to help AT&T improve and migrate its business application to IBM Cloud."[11]

64. As set forth in greater detail below, IBM and AT&T not only failed to comply with these regulations, but they also failed to notify the relevant Federal Government agency(ies) once their information technology systems were hacked, causing the unauthorized access and exfiltration of Protected Information.

65. As set forth in greater detail below, IBM and AT&T are aware of numerous breaches of their computer systems by nation state sponsored threat actors. Instead of reporting and addressing said breaches as required by DFARS regulations and DFARS Clause 252.704-7012, IBM continuously denied that any data was exfiltrated, and, upon information and belief, AT&T has not admitted that any data was exfiltrated.

---

[8] *See* GSA Schedule 20 contract found at https://www.business.att.com/content/dam/attbusiness/migrated/industries/briefs/IT_sched70_GS_35F_0249J.pdf.

[9] NIST SP 800-45 sets forth 5 essential characteristics of cloud-computing services: (1) on-demand service; (2) broad network access; (3) resource pooling; (4) rapid elasticity; and (5) measured service. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

[10] https://www.sdxcentral.com/articles/news/att-inks-1b-doj-telecom-support-deal/2019/07/

[11] https://www.sdxcentral.com/articles/opinion-editorial/atts-public-cloud-first-proclamation-a-stake-in-the-ground/2019/07/

66. IBM and AT&T's federal contracts required that they be 100% compliant with the DFARS security requirements, NIST SP 800-53 and NIST SP 800-171 cyber security requirements.

67. IBM and AT&T's management personnel were well aware that their computer systems did not 100% comply with these requirements.

68. Despite having this direct knowledge that their computer systems were not 100% compliant, IBM and AT&T continued to secure new contracts with the Federal Government and DOD and, in doing so, falsely and materially misrepresented to the Federal Government that they were 100% compliant. This is a material misrepresentation.

69. As set forth in greater detail below, Defendants were awarded numerous contracts with the Federal Government following these false and misleading statements.

70. IBM and AT&T engaged in a continuous and systematic pattern of providing false and misleading information to the Federal Government regarding its DFARS cyber security compliance, NIST SP 800-53 compliance, NIST 800-171 compliance and FedRamp compliance.

71. FAR 52.246-15 required that every invoice submitted by Defendants to the Federal Government for payment have a certification that the supplies or services were in accordance with all applicable requirements and the supplies and services are of the quality specified and conform in all respects with the contract requirements.

72. Had the Federal Government known the full extent of IBM and AT&T's non-compliance with the DFARS cyber security regulations, NIST SP 800-53, NIST 800-171 cyber security and FedRamp compliance standards, it may not have awarded these contracts to IBM and AT&T and made payments under the contracts.

II. FedRamp Regulations and Standards

73. FedRamp is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.[12]

74. On December 8, 2011, the Office of Management and Budget ("OMB") released a memorandum establishing the FedRamp "to provide a cost-effective, risk-based approach for the adoption and use of cloud services to Executive departments and agencies."[13]

75. The General Services Administration ("GSA") established the FedRAMP Program Management Office ("PMO") in June 2012. The FedRamp PMO mission is to "promote the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessment."[14]

76. The General Services Administration ("GSA") established the FedRAMP Program Management Office ("PMO") in June 2012. The FedRamp PMO mission is to "promote the adoption of secure cloud services across the Federal Government by providing a standardized approach to security and risk assessment."[15]

77. Per the OMB memorandum, any cloud services that hold federal data must be FedRamp Authorized.

78. FedRamp prescribes the security requirements and process cloud service providers ("CSP") must follow in order for the government to use their service.

---

[12] Before the introduction of FedRamp, individual federal agencies managed their own assessment methodologies following guidance set by the Federal Information Security Management Act of 2002.

[13] https://www.fedramp.gov/assets/resources/documents/FedRAMP_Policy_Memo.pdf
[14] https://www.fedramp.gov/
[15] https://www.fedramp.gov/

79. There are two ways to authorize a cloud service through FedRamp: a Joint Authorization Board ("JAB") provisional authorization ("P-ATO") and through individual Agencies.[16]

80. FIPS 199 provides the standards for categorizing information and information systems, which is the processes that CSP's use to ensure their services meet the minimum-security requirements for the data processed, stored and transmitted on them.[17] Like FIPS 200, the FIPS 199 standards apply to:

> (i) all information within the federal government other than that information that has been determined pursuant to Executive Order 12958, as amended by Executive Order 13292, or any predecessor order, or by the Atomic Energy Act of 1954, as amended, to require protection against unauthorized disclosure and is marked to indicate its classified status; and
>
> (ii) all federal information systems other than those information systems designated as national security systems as defined in 44 United States Code Section 3542(b)(2). Agency officials shall use the security categorizations described in FIPS Publication 199 whenever there is a federal requirement to provide such a categorization of information or information systems.[18]

81. CSP's are categorized into one of three impact levels: Low, Moderate, and High, and across three security objectives: Confidentiality, Integrity, and Availability.[19]

82. FIPS 199 sets forth the definitions of Confidentiality, Integrity, and Availability, as follows:

> "Confidentiality" means, "Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information…" [44 U.S.C., Sec. 3542] A loss of confidentiality is the unauthorized disclosure of information."

---

[16] https://www.fedramp.gov/jab-authorization/
[17] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf
[18] *Id.* at p. 5
[19] https://www.fedramp.gov/understanding-baselines-and-impact-levels/

> "Integrity" means, "Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity…" [44 U.S.C., Sec. 3542] A loss of integrity is the unauthorized modification or destruction of information."
>
> "Availability" means, AVAILABILITY "Ensuring timely and reliable access to and use of information…" [44 U.S.C., SEC. 3542] A loss of availability is the disruption of access to or use of information or an information system."[20]

83. FIPS 199 also defines the terms, Low, Moderate, and High Impact, as follows:

> The potential impact is LOW if – The loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, or individuals.
>
> The potential impact is MODERATE if – The loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals.
>
> The potential impact is HIGH if – The loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals.
>
> AMPLIFICATION: A severe or catastrophic adverse effect means that, for example, the loss of confidentiality, integrity, or availability might: (i) cause a severe degradation in or loss of mission capability to an extent and duration that the organization is not able to perform one or more of its primary functions; (ii) result in major damage to organizational assets; (iii) result in major financial loss; or (iv) result in severe or catastrophic harm to individuals involving loss of life or serious life threatening injuries.[21]

84. FIPS 200, as set forth above, follows FIPS 199's categorization system by specifying 17 areas of cybersecurity where minimum security requirements are specified.

---

[20] https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.199.pdf at p. 6
[21] *Id.* at 6-7.

85. NIST SP 800-53, as set forth throughout this Complaint, sets forth implementation standards for each of these 17 areas of cybersecurity that must be met by all CSPs, including IBM and AT&T.

86. By becoming FedRamp certified, IBM[22] and AT&T[23] have affirmatively stated to the Federal Government that their cloud-based systems meet all of the standards set forth in FIPS 199, FIPS 200, NIST SP 800-53 and NIST SP 800-37.

87. Additionally, FedRamp certification requires that CSP's "maintain the security of their FedRamp authorized systems by providing the JAB and Authorizing Officials monthly insight into the security posture of the system" which involves performing, logging, and producing monthly scan logs.[24]

88. FedRamp has issued its own separate Security Controls Baseline ("FedRamp Baseline").[25] In the FedRamp Baseline, the JAB notes that it "began the selection of security controls on the PMO's analysis and selected controls from the NIST SP 800-53 Revision 4 . . . The JAB then selected additional controls and enhancements to the 800-53 Revision 4 catalog of controls and provided additional guidance and requirements around these controls."

89. The FedRamp Baseline sets forth specific criteria to be satisfied by the CSPs. Specifically, the FedRamp Baseline notes that "In order to address the unique requirements of cloud computing for the Federal Government, some of the controls and enhancements selected are above the standard NIST guidelines and requirements for low, moderate, and high systems."

---

[22] IBM is listed as being FedRamp certified for: (1) IBM Cloud for Management (11 authorizations); (2) IBM Maximo and TRIRIGA on Cloud for U.S. Federal (4 authorizations); (3) MaaS360 Enterprise Mobility Management (14 authorizations); and (4) SmartCloud for Government (9 authorizations). See https://marketplace.fedramp.gov/#!/products?status=Compliant&sort=productName&productNameSearch=IBM

[23] AT&T is listed as being FedRamp certified for AT&T Cybersecurity

[24] https://www.fedramp.gov/assets/resources/documents/CSP_Vulnerability_Scanning_Requirements.pdf

[25] https://www.fedramp.gov/assets/resources/documents/FedRAMP_Security_Controls_Baseline.xlsx

90. To be clear, the FedRamp Baseline requirements are more stringent than the base standards set forth in NIST SP 800-53 and are required in addition to the NIST SP 800-53 standards for all cloud-based systems contracts with the Federal Government.

91. Therefore, the violations of NIST SP 800-53 set forth below are necessarily violations of the FedRamp Baseline.

92. In addition to the FedRamp Baseline, IBM and AT&T must also comply with NIST SP 800-37 in order to obtain and maintain FedRamp certification.[26]

93. NIST SP 800-37, titled "Risk Management Framework for Information Systems and Organizations" describes the Risk Management Framework ("RMF") and provides guidance for applying the RMF to information systems and organizations.[27] The NIST SP 800-37 Executive Summary notes that:

> "The significant increase in the complexity of the hardware, software, firmware, and systems within the public and private sectors (including the U.S. critical infrastructure) represents a significant increase in attack surface that can be exploited by adversaries. Moreover, adversaries are using the supply chain as an attack vector and effective means of penetrating our systems, compromising the integrity of system elements, and gaining access to critical assets.
>
> * * * * *
>
> The Task Force notes that the cyber threat to the U.S. critical infrastructure is outpacing efforts to reduce pervasive vulnerabilities, so that for the next decade at least the United States must lean significantly on deterrence to address the cyber threat posed by the most capable U.S. adversaries. It is clear that a more practice and systematic approach to U.S. cyber deterrence is urgently needed . . ."[28]

---

[26] https://www.fedramp.gov/cloud-service-providers/

[27] NIST SP 800-37 was developed in response to Executive Order 13800, OMB Memorandum M-17-25 and OMB Memorandum M-19-03. https://csrc.nist.gov/News/2018/rmf-update-nist-publishes-sp-800-37-rev-2

[28] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf at p.v.

94. NIST SP 800-37 was developed to provide guidelines for managing security and privacy risks and applying the RMF to information systems and organizations.

95. NIST SP 800-37 sets forth a seven-step process that must be followed:

(1) "Carry out essential activities at the organization, mission and business process, and information system levels of the organization to manage its security and privacy risks using the [RMF]."

(2) "Inform organizational risk management processes and tasks by determining the adverse impact to organizational operations and assets, individuals, other organizations, and the Nation with respect to the loss of confidentiality, integrity, and availability of organizational systems and the information processed, stored, and transmitted by those systems."

(3) "Select, tailor, and document the controls necessary to protect the information system and organization commensurate with risk to organizational operations and assets, individuals, other organizations, and the Nation."

(4) "Implement the controls in the security and privacy plans for the system and for the organization and to document in a basic configuration, the specific details of the control implementation.

(5) "Determine if the controls selected for implementation are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security and privacy requirements for the system and the organization."

(6) "Provide organizational accountability by requiring a senior management official to determine if the security and privacy risk (including supply chain risk) to organizational operations and assets, individuals, other organizations, or the Nation based on the operation of a system or the use of common controls, is acceptable."

(7) "Maintain an ongoing situational awareness about the security and privacy posture of the information system and the organization in support of risk management decisions."

96. As set forth in greater detail below, IBM and AT&T woefully failed to meet the requirements of NIST SP 800-37 and, as a result, were at all times material, non-compliant with the requirements for maintaining FedRamp certification.

III. Important Terms and Definitions Applicable to FARS, DFARS, FedRamp and NIST Regulations

97. FARS, DFARS, FedRamp and NIST all utilize terms and definitions that have technical meanings within the information technology world. Some of the important terms and definitions, for purposes of this complaint, are set forth below.

III.A. Access Control

98. Access control is a security technique that regulates who or what can view or use resources in a computing environment. There are two types of control: (1) physical access control, which limits access to buildings, rooms, campuses, and physical IT assets; and (2) logical access control, which limits connections to computer networks, system files and data.

99. Access control systems perform identification authorization and authorization of users and entities by evaluating login credentials that can include usernames, passwords, personal identification numbers (PINs), biometric scans, security tokens or authentication factors. Multifactored authentication, which requires two or more authentication factors, is often an important part of layered defense to protect access control systems.

100. These security controls work by identifying an individual or entity, verifying that that person or application is who or what it claims to be, and authorizing the access level and set of actions associated with the username or IP address. Organizations use different access control models depending on their compliance requirements and the security levels of information technology they are trying to protect.

III.B. Audit Control

101. Audit controls are another important internal control system used to ensure the integrity, validity, and reliability of information and to provide an assessment of a system's internal

controls. Without sufficient internal audit controls, it is impossible to measure the severity of any data intrusion or exfiltration.

102. While a financial audit will attest to the validity and reliability of information, the IT audit will attest to the confidentiality of the information, the integrity of the information and in situations where availability is a key factor will also attest to the availability and the ability to recover in the event of an incident.

103. Additionally, audit controls are put in place in order to keep logs of entry and exist on a given network, system or application identifying the who, what, when and where pertaining to access on a network, system, or application.

104. Without audit controls, it becomes impossible for IBM and AT&T to determine who accessed the Core Networks, when that individual(s) accessed the Core Networks, where that individual(s) was at the time they accessed the Core Networks, what data was accessed on the Core Networks or whether any data was altered/modified in any manner.

III.C. Information Security Risk

105. Information security risk assessments assist organizations in making educated security decisions. Understanding one's risk will help prevent arbitrary action. The entire process is designed to help IT departments find and evaluate risk while aligning with business objectives.

III.D. Security Assessment

106. A security risk assessment identifies, assesses, and implements key security controls in applications. It also focuses on preventing application security defects and vulnerabilities. Carrying out a risk assessment allows an organization to view the application portfolio holistically—from an attacker's perspective. It supports managers in making informed

resource allocation, tooling, and security control implementation decisions. Thus, conducting an assessment is an integral part of an organization's risk management process.

III.E. System and Communications Protection

107. System and communications protections require that a contractor protect, through access controls and other means, information transmitted or received by organizational systems at the external boundaries and key internal boundaries of organizational systems.

III.F. System and Information Integrity

108. System and information integrity require the identification, collection, and reporting of flaws within information systems within a timely manner. This includes actively monitoring information system security systems, including all inbound and outbound information traffic, and the prevention of access to data by unauthorized users.

IV. IBM & AT&T's Core Network Systems Are Non-Compliant with FARs, DFARS And FedRamp.

109. IBM's products and services are of no value to the Federal Government because the underlying IBM Core Network on which they were produced fails to adequately protect their development and delivery in compliance with the applicable regulations.

110. In many cases, the services, including, but not limited to, cloud services, provided by IBM are actually detrimental to the purchaser because it eliminates or reduces the protection provided by other security systems.

111. Notwithstanding the useless and potentially harmful nature of the product, IBM continues to sell and cause others to sell products and services that rely on its employees' usage of the Core Network to Federal and State purchasers.

112. Because the IBM Core Network services are worthless (and even harmful) infrastructure, any claims IBM submitted, or caused others to submit, to the United States are false claims within the meaning of the FCA.

113. Upon information and belief, the AT&T Core Network systems are likewise of no value to the Federal Government because they fail to meet their primary purpose: enhancing the security of the agencies that purchase it.

114. In many cases, these services provided by AT&T are actually detrimental to the purchase because it eliminates or reduces the protection provided by other communications' systems.

115. Notwithstanding the useless and potentially harmful nature of the product, AT&T continues to sell and cause others to sell its Core Network services, including, but not limited to communications, cloud-based and cybersecurity systems, to Federal and State purchasers.

116. Because the AT&T Core Network - that it ran for IBM - is worthless (and even harmful), any claims AT&T submitted, or caused others to submit, to the United States are false claims within the meaning of the FCA.

117. As part of the payment process, IBM, and upon information and belief, AT&T must certify that they are in compliance with all terms of their contract. Upon information and belief, IBM and AT&T knowingly presented, or caused to be presented, a false or fraudulent claim for payment or approval.

118. Apart from its own potential FCA liability to federal agencies with whom it contracts, AT&T is jointly and severally liable with IBM on IBM cloud computing contracts

because it both engaged in a joint venture[29] with IBM and because it operates the network upon which the IBM Core Network rests.

119. IBM and AT&T know that the products and services purchased by the Federal Government that utilize the Core Networks do not comply with the security standards imposed on government systems by the FISMA.

120. IBM and AT&T, nonetheless, sell or cause others to sell the products and services to Federal agencies while failing to inform government purchases of these critical security flaws or of the Core Networks' systems non-compliance with government standards.

121. Any claims for IBM and AT&T's products developed and delivered using the Core Networks' systems, caused by IBM and AT&T's explicit and implicit representations about the security features of the products, and the products' compliance with Federal information security standards, are false claims within the meaning of the FCA.

122. Moreover, under the terms of all of IBM and AT&T's contracts with the Federal Government, IBM and AT&T had a duty to remediate their Core Networks systems that it knew to be flawed, insecure or otherwise faulty.

123. Upon information and belief, IBM and AT&T conspired with each other, as well as with other parties to conceal defects in their Core Networks, and otherwise to facilitate knowingly selling to numerous Federal Government agencies worthless and harmful products.

---

[29] This joint venture and collaboration has been widely reported in the media. For example, see "AT&T joint venture with China Telecom will have expanded scope, including VoLTE roaming." https://www.rcrwireless.com/20170627/carriers/att-joint-venture-with-china-telecom-tag6 and "AT&T and China Telecom Sign Agreement to Expand Relationship, Deliver Global Solutions to Multinational Companies," https://www.prnewswire.com/news-releases/att-and-china-telecom-sign-agreement-to-expand-relationship-deliver-global-solutions-to-multinational-companies-134739693.html

RELATOR BACKGROUND

124. Relator is a United States citizen, currently residing in Newburyport, Massachusetts.

125. Relator was, until recently, Vice President of Threat Intelligence at IBM.

126. Relator had been employed in this capacity at IBM from January 2017 through August 2019.

127. Prior to his January 2017 role, Relator was employed by IBM in other roles at IBM. Since 2002, Relator has been employed by IBM on two (2) separate occasions.

128. As part of his duties and responsibilities, Relator was tasked with building IBM's commercial incident response and cyber threat intelligence business. Relator would be called in to help when IBM needed additional expertise to respond to cyber security incidents and system threats.

129. As set forth in greater detail below, Relator physically witnessed numerous incidents of hacking of IBM's Core Network systems, leading to the exfiltration of countless amounts of data.[30]

130. When Relator brought this to the attention of members of IBM's C-Suite, he was dismissed, instructed to "tone down" his reports and to not include certain information in reports.

131. Up until his resignation, IBM never addressed the issues raised by Relator.

132. Relator was silenced while IBM ignored serious threats that impacted not only their own networks but data belonging to thousands of customers including the federal government.

133. As defined by FIPS 199 (see above), these were considered "serious or catastrophic" events.

---

[30] Because of the lack of audit controls (explained later), it is unknown how much data belonged to the federal government and DOD.

134. In his capacity as Vice President of Threat Intelligence at IBM, Relator found that the IBM Core Network systems failed to meet the minimum requirements including, but not limited to cybersecurity and cloud-computing, required by the Federal Government to be awarded contracts funded by the Federal Government or DOD.

135. Relator is one of the top security professionals in the cyber security business and is intimately familiar with the FARs related to cyber security.

136. As set forth in greater detail below, IBM was not compliant with, at a minimum, DFARS' cyber security or cloud-based systems' requirements, NIST SP 800-53, NIST SP 800-171, or NIST SP 800-37 when Relator began his role as the Vice President of Threat Intelligence at IBM in January 2017.

137. Furthermore, during his employment with IBM, IBM never upgraded the IBM Core Network systems to where they became compliant with DFARS, NIST SP 800-53, NIST SP 800-171 or NIST SP 800-37.

138. Relator's investigations demonstrated adversarial activity going back several years.

139. Relator is informed and believes and thereon alleges that Defendants' Core Networks systems had not been compliance with DFARS cyber security requirements, NIST SP 800-53, NIST SP 800-171 or NIST SP 800-37 cyber security and cloud-based systems' requirements for several years dating back prior to Relator's role as a VP of Threat Intelligence.

140. Based on these provisions, Relator seeks to recover all available damages, civil penalties, and other relief for the Federal violations alleged herein.

DEFENDANTS

141. IBM is a New York Corporation with its headquarters in Armonk, New York. In 2019, IBM had over $75 billion in revenue. IBM is a publicly traded corporation, listed on the

New York Stock Exchange. IBM is one of the world's largest information technology service providers and has a large presence in the security software and cloud computing fields. IBM aggressively markets its cloud-based systems and other products to government purchasers, including agencies of the United States. Much of IBM's revenue is derived from a series of strategic imperatives that include both information security and cloud computing.

142. AT&T is a Texas Corporation with its headquarters in Dallas, Texas. In 2019, AT&T had over $181 billion in revenue. AT&T is a publicly traded corporation. It is one of the world's largest communications and network services providers and has a large presence in the cloud computing field. AT&T aggressively markets its communications and cybersecurity systems and other products to government purchasers and government contractors, including agencies of the United States and IBM.

JURISDICTION AND VENUE

143. This Court has jurisdiction over the subject matter of this action pursuant to 28 U.S.C. § 1331; 28 U.S.C. § 1367, and 31 U.S.C. § 3732, the last of which specifically confers jurisdiction on this Court for actions brought pursuant to 31 U.S.C. §§ 3729 and 3730.

144. Under 31 U.S.C. §3730(e), there has been no statutorily relevant public disclosure of the "allegations or transactions" in this case. Relator, moreover, would qualify under those provisions as an "original source" of the allegations in this Complaint even had such a public disclosure occurred.

145. To the extent that there could have been a public disclosure under 31 U.S.C. § 3732(e)(4)(A), Relator possess information that is independent or and materially adds to any potentially publicly disclosed allegations.

146. Relator has also voluntarily provided the information on which the allegations and transactions alleged herein to the Government before filing this action.

147. This Court has personal jurisdiction over IBM pursuant to 31 U.S.C. § 3732(a), which authorizes nationwide service of process and because IBM has minimum contacts with the United States and can be found in and/or transacts business in this District.

148. This Court has personal jurisdiction over AT&T pursuant to 31 U.S.C § 3732(a), which authorizes nationwide service of process and because AT&T has minimum contacts with the United States and can be found in and/or transacts business in this District.

149. Venue is proper in this District pursuant to 28 U.S.C. §1391(b) and 1395(a) and 31 U.S.C. § 3732(a) because IBM can be found in and/or transacts business in this District. At all times material to the Complaint, IBM regularly conducted substantial business within this District, maintained employees in this District and/or made significant sales within this District. In addition, statutory violations, as alleged here, occurred in this District.

150. Venue is proper in this District pursuant to 28 U.S.C. §1391(b) and 1395(a) and 31 U.S.C. § 3732(a) because AT&T can be found in and/or transacts business in this District. At all times material to the Complaint, AT&T regularly conducted substantial business within this District, maintained employees in this District and/or made significant sales within this District. In addition, statutory violations, as alleged here, occurred in this District.

APPLICABLE LAW

I. Federal Acquisition Regulation

151. The FAR, codified in Title 48 of the United States Code of Federal Regulations ("CFR"), govern the federal procurement process from need recognition and acquisition planning through contract formation and contract administration.

152. The FAR was amended on September 30, 2005 "to implement the information technology security provisions of [FISMA] (Title III of the E-government Act of 2002 (E-Gov Act))." 70 FR 57449, 57450 (2005) finalized without substantive change, 71 FR 57360 (2006). The motivation for and purpose of the FISMA and the implementing provisions were explained as follows:

> American society relies on the Federal Government for essential information and services provided through interconnected computer systems. **Both Government and industry face increasing security threats to essential services and must work in close partnership to address those risks**. Increasingly, contractors are supplying, operating, and accessing critical IT systems, performing critical functions throughout the life of IT systems. At the same time, it is apparent that information technology and the IT marketplace have become truly global. The security risks are shared globally as well.
>
> Unauthorized disclosure, corruption, theft, or denial of IT resources have the potential to disrupt agency operations and could have the financial, legal, human safety, personal privacy, and public confidence impacts. The Federal community has not focused on unclassified activities with regard to information technology resources involved in the acquisition and use of information on behalf of the Government. **In particular, there is need to focus on the role of contractors in security as more and more Federal agencies outsource various information technology functions. Until now, regulations have generally been silent regarding security requirements for contractors who provide goods and services with IT security implications**.
>
> This rule amends FAR parts 1, 2, 7, 11, and 39 to implement information technology security provisions of [FISMA]. The rule recognizes security as an important part of all phases of the IT acquisitions life cycle. The rule focuses much needed attention on the importance of system and data security by contracting officials and other members of the acquisition team.

> The intent of adding specific guidance in the FAR is to provide clear, consistent guidance to acquisition officials and program managers; and to encourage and strengthen communication with IT security officials, chief information officers, and other affected parties. *Id.* (Emphasis added)

153. To accommodate the growth, change and evolution of the information technology products and services to be purchased by the Government, the FAR incorporates external standards – the FIPS – rather than trying to create a separate standard. *Id.*

154. Accordingly, 48 C.F.R. § 11.102 requires agencies to adhere to the FIPS when minimum security requirements as defined herein, through the use of security controls in accordance with NIST SP 800-53, Recommended Security Controls for Federal Information Systems, as amended.

155. Therefore, any and all recommended controls contained in NIST SP 800-53 are binding on government agencies and government agencies may not procure, install, or maintain systems that do not comply with NIST SP 800-53 and FIPS 200.

156. NIST SP 800-53 is divided into various categories of security measures, including Access Controls ("AC"), Authority and Purpose, Accountability, Audit and Risk Management, Awareness and Training, Audit and Accountability ("AU"), Security Assessment and Authorization, Configuration Management, Contingency Planning, Data Quality, Data Minimization and Retention, Identification and Authentication ("IA"), Individual Participation and Redress, Incident Response ("IR"), System Maintenance Policies and Procedures, Media Protection, Physical and Environmental Protection, Planning, Personnel Security, Risk Assessment , System and Services Acquisition, System and Communications Protection ("SC"), Security ("SE"), System and Information Integrity ("SI"), Transparency, and Use Limitation.

157. As outlined in greater detail below, IBM and AT&T's cybersecurity, communications and cloud-based systems violate many of the NIST SP 800-53 requirements, including, but not limited to:

a. AC-3 (Access Control Enforcement);

b. AC-4 (Information Flow Enforcement);

c. AC-6 (Least Privilege);

d. AC-17 (Remote Access);

e. AC-23 (Data Mining Protection);

f. AC-24 (Access Control Decisions);

g. AU-1 (Audit and Accountability Policy and Procedures);

h. AU-3 (Content of Audit Records);

i. AU-13 (Monitoring for Information Disclosure);

j. IA-2 (Identification and Authentication (Organizational Users);

k. IA-3 (Device Identification and Authentication);

l. IA-5 (Authenticator Management);

m. IR-5 (Incident Monitoring);

n. SC-8 (Transmission Confidentiality and Integrity);

o. SC-23 (Session Authenticity);

p. SC-28 (Protection of Information at Rest);

q. SI-2 (Flaw Recognition);

r. SI-4 (Information System Monitoring);

s. SI-6 (Security Function Verification); and

t. SI-10 (Information Input Validation).

158. FIPS 200 makes no provision for waiver of its requirements. *Id.* at v ("No provision is provided under FISMA for waivers to FIPS made mandatory by the Secretary of Commerce."). Had federal purchasers been aware of the defects in the IBM and AT&T cybersecurity, communications, and cloud-based systems, they would have been unable to purchase it, because their information technology security would not have been compliance with FIPS 200 or NIST SP 800-53. *Id.* at iv.

159. Per NIST SP 800-53 rev 4 p. 7, "FIPS 200 and NIST Special Publication 800-53, in combination, ensure that appropriate security requirements and security controls are **applied to all federal information and information systems**." (Emphasis added.) "The guidelines apply to all components of an information system that process, store, or transmit federal information." NIST SP 800-53 rev 4 p25. NIST SP 800-53 sets forth baseline requirements that all federal contractors must meet.

II. Defense Federal Acquisition Regulations Supplement

160. As set forth above in the Introduction, in December 2015, the DOD published a FAR Supplement referred to as the DFARS, which is a set of cybersecurity regulations promulgated by the DOD that applies to all external contractors and suppliers of the DOD.

161. The DFARS intended to maintain cybersecurity standards according to requirements set forth in NIST SP 800-171. NIST SP 800-171 was constructed to protect the confidentiality of controlled unclassified information ("CUI") and had given DOD contractors until December 31, 2017 to meet the requirements necessary to be classified as DFARS compliant. Failure to meet these requirements could result in the loss of current DOD contracts.

162. With the December 31, 2017 deadline now passed, all DOD contractors must meet the minimum requirements and show proof to the DOD for all contracts moving forward.

163. NIST SP 800-171 states unequivocally that FISMA "requires federal agencies to identify and provide information security protections commensurate with the risk resulting from the unauthorized access, use, disclosure, disruption, modification, or destruction of: (i) information collected or maintained by or on behalf of an agency; or (ii) information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency" NIST SP 800-171 p. V.

164. All recommended guidelines set forth in NIST SP 800-171 are binding on the DOD and all contractors and suppliers that contract with the DOD. The DOD may not procure, install, or maintain systems that do not comply with NIST SP 800-171.

165. NIST SP 800-171 is divided into various categories of security measures, including Access Control, Awareness and Training, Audit and Accountability, Configuration Management, Identification and Authentication, Incident Response, Maintenance, Media Protection, Personnel Security, Physical Protection, Risk Assessment, Security Assessment, System and Communications Protection, and System and Information Integrity.

166. As outlined in greater detail below, IBM and AT&T's cybersecurity, communications and cloud-based systems violate many of the NIST SP 800-171 requirements, including, but not limited to:

a. Access Control 3.1.1;

b. Access Control 3.1.2;

c. Access Control 3.1.3;

d. Access Control 3.1.5;

e. Access Control 3.1.12;

f. Access Control 3.1.17;

g. Access Control 3.1.20;

h. Audit and Accountability 3.3.1;

i. Audit and Accountability 3.3.2;

j. Identification and Authentication 3.5.1;

k. Identification and Authentication 3.5.2;

l. Risk Assessment 3.11.2;

m. Risk Assessment 3.11.3;

n. Security Assessment 3.12.3;

o. System and Communications Protection 3.13.8;

p. System and Communications Protection 3.13.15;

q. System and Communications Protection 3.13.16;

r. System and Information Integrity 3.14.1;

s. System and Information Integrity 3.14.3;

t. System and Information Integrity 3.14.6; and

u. System and Information Integrity 3.14.7.

167. It is important to note that satisfying the requirements of NIST SP 800-171 does not in and of itself mean that the requirements of NIST SP 800-53 are satisfied, and vice versa. Instead, DOD contractors must meet both the requirements of NIST SP 171 and NIST SP 800-53 in order to be in compliance with the applicable DOD contract.

III. FedRamp And NIST SP 800-37

168. As set forth above in the Introduction, FedRamp is a US government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.

169. Per the OMB memorandum, any cloud services that hold federal data must be FedRAMP Authorized.

170. FedRamp requires compliance with NIST SP 800-37 in order to obtain and maintain FedRamp certification.

171. NIST SP 800-37 states unequivocally that agencies are required to "implement the RMF that is described in this guideline and requires agencies to integrate privacy into the RMF process. NIST SP 800-37, p. vi.

172. All recommended guidelines set forth in NIST SP 800-37 are binding on all companies that provide cloud-based services for the Federal Government.

173. NIST SP 800-37 is divided into seven categories: (1) Prepare; (2) Categorize; (3) Select; (4) Implement; (5) Assess; (6) Authorize; and (7) Monitor.

174. As outlined in greater detail below, IBM and AT&T's cybersecurity, communications and cloud-based systems violate many of the NIST SP 800-37 requirements, including, but not limited to:

a. Task P-7 (Continuous Monitoring Strategy – Organization);

b. Task S-5 (Continuous Monitoring Strategy – System);

c. Task I-1 (Control Implementation);

d. Task A-4 (Assessment Reports);

e. Task A-5 (Remediation Actions);

f. Task R-5 (Authorization Reporting); and

g. Task M-3 (Ongoing Risk Response).

FACTUAL BACKGROUND

I. IBM Core Network Systems Overview

175. Cybersecurity is one of the most serious challenges facing the federal government today.[31,32]

176. Lone wolf hackers, disgruntled workers, terrorists, organized crime, and nation-states are constantly seeking access to the United States' most sensitive and valuable information through remote-access attacks.

177. Companies have recognized the business risk of these threats and are working to detect and respond to them quickly to mitigate the consequences. Many of these companies, as well as government agencies, increasingly turn to vendors to help mitigate these risks.

178. For many, IBM is best known for its computer hardware, but the company does much more. In fact, IBM's cloud computing organization is one of the largest in the world.[33] IBM's vision is to run everyone's infrastructure. Yet, its own infrastructure is infected and flawed as described herein.

179. Tens of thousands of private companies and government agencies rely on IBM to keep their data safe.

---

[31] The Government Accountability Office ("GAO") reported that government agencies faced in excess of 35,000 cyber incidents in 2017, alone. *See* https://www.gao.gov/assets/700/693405.pdf p8.

[32] https://www.gao.gov/assets/700/697245.pdf

[33] IBM touts itself as "the world's largest information technology (IT) services company. The IT services leader, IBM's solutions and services span all major industries, including financial services, healthcare, government, automotive, telecommunications and education, among others." https://www.ibm.com/industries/federal/contracts/dhs-eagle-ii.

180. Thousands of federal, state, foreign and local agencies also rely on IBM to safeguard data including agencies as the DOD, Department of Homeland Security, U.S. Army, U.S. Air Force, the Centers for Medicare and Medicaid Services, and many others.[34]

I.A. IBM Repeatedly Makes Materially False and Misleading Statements Surrounding the IBM Core Network Systems

181. In its 2016 Annual Report, IBM boldly declared that it "has established the world's deepest portfolio of data and analytics solutions . . . including cloud data solutions."[35]

182. IBM's 2018 Annual Report declares that "IBM is the leader in information security for enterprises."[36] That same report claims that "IBM safeguards client data with world class technologies and approaches to security."

183. IBM makes such representations while knowing that its systems are not safe.

184. IBM opened its 2018 Annual Report with a letter to investors, entitled "Dear IBM Investor." In this letter, IBM represented that "IBM Security [is] the world's largest cybersecurity enterprise [and] has 8,000 subject matter experts serving more than 17,000 clients in more than 130 countries . . . IBM Systems produces innovative infrastructure for AI and hybrid cloud. The z14 is one of IBM's most successful mainframe programs in history, with broad global adoption across 27 different industry segments. In addition, the U.S. Department of Energy's POWER-9

[34] IBM's own website identifies the following active Federal contracts as of July 11, 2020: (1) GSA Alliant; (2) GSA Alliant 2; (3) NASA SEWP V; (4) NIH CIO-CS; (5) NIH CIO-SP3; (6) SA IT Schedule 70; (7) GSA Professional Schedule (PSS); (8) GSA Human Capital Management and Administrative Services; (9) GSA Office Imaging & Document Schedule 36; (10) Air Force NETCENTS 2 Net Ops Contract; (11) Air Force NETCENTS 2 Application Services Contract; (12) CDC CIMS; (13) DOI FCHS; (14) DHS Eagle II; (15) Army ITES-2S; (16) Army ITES-3D; (17) Army ITES-3H; (18) Army RS3; (19) DISA SETI; (20) GSA OASIS; (21) Navy Seaport-e 2014; (22) Navy Seaport-NxG; (23) OPM HCaTS; and (24) VA T4NG. https://www.ibm.com/industries/federal/contracts last accessed on July 11, 2020.

[35] *See* IBM 2016 Annual Report at p. 34. https://www.ibm.com/investor/att/pdf/IBM_Annual_Report_2016.pdf

[36] https://www.ibm.com/annualreport/assets/downloads/IBM_Annual_Report_2018.pdf

based supercomputers, Summit and Sierra, were ranked the most powerful supercomputers in the world in 2018."[37]

185. IBM falsely portrays its data security and cloud computing solutions as safe and goes so far as to represent itself as being the "gold standard for cybersecurity."[38]

186. IBM has made, and continues to make, these representations with knowledge that its systems, and its customer's data has been hacked.

187. Because of this, IBM's statement, that its data security and cloud computing solutions are safe, are materially false, fraudulent, and at best, misleading to the Federal Government agencies that contract with IBM.

188. In a number of different settings, IBM represents its cybersecurity as being secure and state of the art. For example, in a 2017 Form 10-K, IBM represents that its Cloud is "Secure to the Core."[39]

189. IBM has stated that it has a "longstanding reputation for trust, integrity and responsibility"[40] regarding its data security, and that it is "#1 in enterprise security."[41]

190. In a 2017 SEC 10-K report, IBM falsely represented that nothing material has ever occurred from a cyber security perspective. "To date, **there has not been a cybersecurity attack that has had a material adverse effect on the company**, though there is no assurance that there will not be a cybersecurity attack that has a material adverse effect in the future."[42] (Emphasis added.)

---

[37] *Id.*
[38] *See* 2017 IBM Annual Report at p5, available at https://www.ibm.com/investor/att/pdf/IBM_Annual_Report_2017.pdf
[39] *Id.*
[40] See 1028 Chairman's Dear Investor Letter, available at https://www.ibm.com/annualreport/2018/letter.html
[41] *Id.*
[42] IBM Corp. (2018). 2017 Form 10-K, available at https://www.sec.gov/Archives/edgar/data/51143/000104746918001117/a2233835z10-k.htm

191. As demonstrated below, the IBM Core Network is routinely hacked by foreign state actors and others. Additionally, data is routinely exfiltrated and the Federal Government agencies are never notified.

192. Even when IBM was confronted by media reports of a cybersecurity hacking incident, the company denied any exfiltration.

193. IBM even denied cyberhacking incidents when confronted by all 5 of the Five Eyes (an intelligence alliance comprised of Australia, Canada, New Zealand, the United Kingdom, and the United States).[43]

194. Equally responsible for these breaches and violations of government cyber security regulations is AT&T which is operates IBM's network and considers itself in a joint venture with IBM.

II. AT&T Core Network Overview.

195. AT&T is known to most individuals as a communications company, particularly since many people utilize AT&T's communications services for their telephone services. However, AT&T also provides cloud security services that it touts as achieving the "highest security and compliance standards."[44]

196. AT&T claims that its "AT&T cybersecurity solutions" offers:

> [T]he AT&T multi-layer defense approach to address cybersecurity risks in even the most complex environments. These services include:

---

[43] See, "IBM Says No Evidence that 'Sensitive' Data Was Taken By Hackers," Bloomberg Dec. 20, 2018, available at https://www.bloomberg.com/news/articles/2018-22-20/ibm-says-no-evidence-that-sensitive-data-was-taken-by-hackers ("We take responsible stewardship of client data very seriously, and have no evidence that sensitive IBM or client data has been compromised by this threat.")

[44] See AT&T Business Market Briefing report on Transforming the Public Sector Contact Sector, p. 5 available at https://www.business.att.com/content/dam/attbusiness/briefs/vc-conact-center-solutions-public-sector.pdf.

- Threat intelligence – a trusted advisor to help you put the right people, processes, and technology together to elevate trust with your customers, employees, and leaders in helping to prevent, detect, and respond to cybersecurity threats.

- Mobile and Endpoint Security – a trusted source with strategic and innovative suppliers so you can have the visibility and control of your data.

- Mobile Threat Defense – A tool that uses a mix of vulnerability management, anomaly detection, behavioral profiling, code emulation, intrusion prevention, and transport security technologies to help defend mobile decides and applications from cyber threats.

- Infrastructure Security – Giving your business the security it needs to help protect your network against threats that can cost you money, time, and reputation.[45]

197. Upon information and belief, despite these claims, AT&T's own infrastructure is infected and flawed as described herein.

198. Like IBM, tens of thousands of private companies and government agencies rely on AT&T to keep their data safe.

199. Thousands of federal, state, foreign and local agencies also rely on AT&T to safeguard data including agencies such as the DOJ, Department of Veteran's Affairs, U.S. Air Force, Social Security Agency, and Internal Revenue Service.[46]

[45] See AT&T's Security "In" "Of" the Cloud, available at https://www.business.att.com/learn/top-voices/security-in-and-of-the-cloud.html.

[46] AT&T's own website identifies the following active Federal contracts as of July 16, 2020: (1) VA BPA 549-00-6; (2) VA BPA 549-01-11; (3) Air Force BPA F19628-02-A-0039; (4) IRS BPA TIRNO-02-Z-00036; (5) GovWorks BPA Contract No. 05566; (6) USDA Enterprise Architecture BPA No. USDA, OPPM, POD 43-3142-05324; (6) Marine Corps CEOss BPA; (7) GSA Alliant Contract No. GS00Q09BDG0015; (8) Networx Universal GSA; (9) Networx Enterprise GSA; (10) GSA Connections II, Contract No. GS00Q12NSD0004; (11) GSA IT 70 Schedule No. GS-35F-0249J; (12) GSA IT 70 Schedule No. GS-35F-4507G; (13) GSA IT 17 Schedule No. GS-35F-0297K; (14) Management and Organization Business Improvement Schedule ("MOBIS") Contract No. GS-10F-0113J; (15) Professional Engineering Services GS-23F-0174S; (16) Logistics Worldwide Services GS-10F-0073M; and (17) Nortel Authorized Distributor Information Technology Schedule Contract No. GS-35F-0140L. https://www.corp.att.com/gov-contracts/all-contracts/ (last visited on July 16, 2020.)

200. In its 2018 Annual Report, AT&T represents that "[w]hile we have been subject to security incidents or cyberattacks, these did not result in a material adverse effect on our operations. However, as such attacks continue to increase in scope and frequency, we may be unable to prevent a significant attack in the future."[47]

201. While AT&T makes this general statement about security vulnerabilities, it failed to disclose the specific successful cybersecurity attacks on the IBM cloud systems of which AT&T was an integral part.

III. IBM and AT&T Work Together on The Core Networks.

202. AT&T advertises that it provides "cloud network enablement technology." In fact, it is an integral partner with IBM. The Financial Times reported in July 2019 that the two companies signed a multiyear contract "billions of dollars" for cloud computing technologies.[48]

203. IBM management has stated internally that the relationship between IBM and AT&T is so intertwined that if the two companies parted ways, it would be a "reportable" event for purposes of U.S. securities laws.

204. Unfortunately, AT&T's network is both rudimentary and obsolete. For example, the network AT&T runs for IBM does not keep comprehensive activity logs, a process considered by security experts to be both basic and necessary.

205. By operating without such logs, it becomes virtually impossible to detect hacking intrusions and data exfiltrations, and impossible to monitor and audit as required by government contracting regulations as set forth throughout this Complaint.

---

[47] *See* AT&T, Inc., 2018 Annual Report, p. 58, available at https://investors.att.com/~/media/Files/A/ATT-IR/financial-reports/annual-reports/2018/complete-2018-annual-report.pdf

[48] Richard Waters, "IBM lands AT&T contract worth 'billions,' Financial Times, July 16, 2019, available at https://www.ft.com/content/257b9a42-a78b-11e9-984c-fac8325aaa04

206. Relator, in his role as Vice President of Threat Intelligence, requested, on numerous occasions, that AT&T produce audit logs in order for his team to investigate an adversarial action that occurred on the IBM Core Network.

207. In response, AT&T would advise that it either did not have said logs or that the audit logs were incomplete.

208. Furthermore, AT&T was unable to associate users with logins to the IBM Core Network and IBM was unable to identify which computer was utilized to login to the IBM Core Network.

209. This was particularly problematic when said network access was routed through an AT&T virtual private network ("VPN") which would provide an outsider or remote employee with direct access to the Core Networks.

210. Audit logs are vitally important in cloud-computing given that cloud computing, by its very nature, does not require a computer connected directly to a physical network.

211. IBM had virtually no endpoint monitoring on its AT&T provided network.

212. As VP of Threat Intelligence, Relator routinely requested audit logs from AT&T for VPN access.

213. AT&T was unable to provide this data.

214. Instead, Relator was only provided with exit node data – showing the internet protocol address ("IP") that would appear on the IBM Core Network.

215. However, the exit node data is not the actual IP address of the user and the IP address cannot be fully tracked as the user's internet activity is encrypted.[49]

[49] https://cybersecurity.att.com/blogs/security-essentials/explain-how-vpn-works

216. To be clear, AT&T could not identify what user ID and password were being utilized on IBM's Core Network with any exit node.

217. Furthermore, IBM could not identify what workstation was assigned to the IP address identified in the exit node.

218. This is basic information that both IBM and AT&T should have maintained in an audit log, yet neither did.

219. Put another way, when a user accessed the Core Networks via the AT&T VPN neither IBM nor AT&T could associate the network access with a legitimate user.

220. Failure to have these basic audit abilities is a violation of numerous government regulations as outlined above.

221. There is still no comprehensive network segmentation and there is no logging of VPN access.

222. IBM has no idea who owns one of its IP addresses at any point in time and it has no way to detect or stop a rogue scan of the network environment.

223. There is still no comprehensive network segmentation and there is no logging of VPN access. IBM has no idea who owns one of its IP addresses at any point in time and it has no way to detect or stop a rogue scan of the network environment.

224. While both IBM and AT&T recognize these issues, they have failed to disclose this to the Federal government and have failed to remediate the problems.

225. While IBM and AT&T may offer security solutions to their customers, they fail to utilize this technology on the cloud services offered by IBM and upon information and belief, AT&T. In fact, AT&T's own network is both rudimentary and obsolete.

226. For example, the network AT&T runs for IBM does not keep comprehensive activity logs, a process considered by security experts to be both basic and essential.

227. Because the AT&T provided network is flat and lacks basic controls such as network segmentation and VPN logging, a hacker in China has the same privileges as a user in the United States and AT&T cannot tell one from the other.

228. The network upon which IBM offers cloud services to customers, including its federal government customers, operates without logs and without an internal firewall.

IV. AT&T's Outsourcing to The Chinese Government.

229. Upon information and belief, AT&T subcontracts part of its cloud-based technologies to China Telecom Corp. Ltd. A company owned by the People's Republic of China.[50]

230. Although the collaboration with China Telecom has been widely reported, AT&T has failed to disclose hacking incidents and cyber vulnerabilities involving its network and its global partner, IBM.

231. AT&T relies on China Telecom for much of its infrastructure in China.

232. IBM fails to disclose that fact to its users and customers, including those customers with extremely sensitive security needs such as the Federal Government.

233. As set forth in greater detail below, at least one of the actors is attributed to China – a threat group commonly referred to as APT 10.

234. Because the AT&T provided network is flat and lacks basic controls such as network segmentation and VPN logging, a user in China has the same privileges as a user in the United States and AT&T cannot tell one from the other.

[50] *See supra* note 28.

235. The basic IBM/AT&T network and cloud infrastructure remains outdated and archaic.

236. Despite claiming to be leaders in cybersecurity, AT&T operates a system without logs and IBM does not have an internal firewall or network segmentation.

237. Given the limitations on their systems, it is not even possible to know the full extent of *how much* data has already been exfiltrated, much less, *what* data was exfiltrated.

238. Most importantly, neither IBM nor AT&T has reported the continuous hacking and exfiltration of data from IBM's cloud that they have knowledge of.

V. IBM and AT&T Engage in Willful Blindness

239. IBM and AT&T have been the subject of continuous hacking and exfiltration of data for years.

240. Rather than report the problem to fix it, IBM has elected to ignore the problem for years.

241. Whenever someone proposed to fix the problem, IBM senior management thwarts such attempts.

242. The current thought process of IBM is that if the company were to "officially" know of the problem, it would be required to report the problem.

243. Relator has direct knowledge of these events of hacking and has investigated, reported, etc., these events of hacking and took the results to his superiors.

244. In response, IBM told Relator to "tone down" his reporting and IBM looked the other way.

245. The actual hacking events are outlined below as well as IBM's efforts to hide them from its customers, such as the Federal Government.

246. Relator, as IBM's Vice President of Threat Intelligence, witnessed instances of hacking, including exfiltration of data, and was directed to not take the necessary steps to determine the extent and seriousness of the hacking or the problem that lead to the hacking.

247. In fact, IBM consciously ignored the problem for so long that it may now be impossible to ever rid its extensive cloud data storage system of threats.

248. This "head in the sand" approach taken by IBM and AT&T jeopardizes national security.

249. Although IBM and AT&T have made it impossible to measure the full extent of the problem, it is easy to see how the ongoing breaches may cumulatively be the largest and most damaging breach in history.

250. Compounding the issues, IBM and AT&T cannot even measure how devastating the attacks are as there is no tracking of logs, which is mandated by NIST as set forth below.

251. The actions outlined below describe a pattern of deliberate "willful blindness" by IBM.[51]

252. In the instant matter, the situation has gone far beyond the word "may." Nation state hackers have infiltrated IBM and AT&T's Core Networks' systems and accessed and exfiltrated Federal Government data.

A. <u>The APT 10 Breaches.</u>

253. On December 17, 2018, a grand jury in the United States District Court for the Southern District of New York indicted Zhu Hua aka "Afwar" and "Godkiller," and Zhang Shilong aka "Atreexp," two members of a hacking group operating in China known in the cybersecurity

[51] *See generally, U.S. v. Raymond & Whitecomb, Co.*, 53 F.Supp.2d 436, 446 (S.D.N.Y. June 19, 1999) (quoting *United States v. Incorporated Village of Island Park*, 888 F.Supp. 419, 439 (E.D.N.Y. 1995)

community as Advanced Persistent Threat 10 (the "APT 10"), with a conspiracy to commit computer intrusion, conspiracy to commit wire fraud, and aggravated identity theft.

254. These two individuals worked for Huaying Haitai Science and Technology Development Company located in Tianjin, China. The FBI believes they acted in association with the Chinese Ministry of State Security's Tianjin State Security Bureau.

255. As alleged in the indictment, from at least 2006 through 2018, the APT 10 conducted extensive campaigns of global intrusions into computer systems aiming to steal, among other data, intellectual property and confidential business and technological information from more than 45 commercial and defense technology companies in at least a dozen U.S. states, managed service providers ("MSP"), which are companies that remotely manage the information technology infrastructure of businesses and governments around the world, and U.S. government agencies.

256. The victim companies targeted by Zhu Hua and Zhang Shilong were involved in a diverse array of commercial activity, industries, and technologies, including aviation, space and satellite technology, manufacturing technology, oil and gas exploration, production technology, communications technology, computer processor technology and maritime technology.

257. In addition, the APT 10's campaign compromised the data of an MSP and certain of its clients located in at least 12 countries including Brazil, Canada, Finland, France, Germany, India, Japan, Sweden, Switzerland, the United Arab Emirates, the United Kingdom, and the United States.

258. The APT 10 also compromised computer systems containing information regarding the United States Department of the Navy and stole the personally identifiable information of more than 100,000 Navy personnel.[52]

259. What is not public is that the APT 10 has compromised the IBM Core Network, and therefore the data maintained by IBM in partnership with AT&T.

260. On or about March 2017, IBM received a report from intelligence officials in the United States, Canada, United Kingdom, and Australia that IBM IP addresses were connecting to known APT 10 controllers. An internal IBM investigation revealed potentially malicious activity.

261. The IBM internal investigation – called the "Davis Investigation" – found

> "56,215 potential APT 10 hits dating between 2013 and 2016, but these indicators **could not be investigated further because there were no corresponding logs connecting the DNS requests to specific users or laptops that could then be searched further for evidence of compromise**. During the course of the Davis Investigation, the team was unable to identify conclusive evidence of ATP 10 activity within the limited scope of data sources analyzed, which covered less than 1% of the total BM system population." IBM's Bison Report of December 16, 2018 (Emphasis added).[53]

262. The Bison Report, *infra*, was shared with senior managers, several of whom sit on IBM's Cybersecurity Advisory Council.

263. These same senior managers wanted reports of hacking kept off the Council's agenda and did not want any minutes kept of these discussions.

264. No one from IBM – and upon information and belief – no one from AT&T, alerted the authorities or Federal Government regarding the data theft.

---

[52] U.S. DEPARTMENT OF JUSTICE, December 20, 2018, *Two Chinese Hackers Associated With the Ministry of State Security Charged with Global Computer Intrusion Campaigns Targeting Intellectual Property and Confidential Business Information*, available at https://www.justice.gov/opa/pr/two-chinese-hackers-associated-ministry-state-security-charged-global-computer-intrusion. (last visited September 9, 2020.)

[53] Relator's knowledge comes directly from his work as IBM's Vice President of Threat Intelligence.

265. AT&T, as network administrator, knew or should have known about the breaches and therefore had a duty to disclose this to regulators and its Federal Government customers.

266. AT&T was involved in this data breach investigation and failed to provide any information back to the Five Eyes that notified them of the breach.

267. The New York branch of the FBI and the United Kingdom government questioned IBM regarding this data breach investigation and in response, IBM disclosed extraordinarily little.

268. The U.S. National Security Agency ("NSA") even asked Relator questions pertaining to the breach, and Relator was instructed to "dodge" the questions.

269. IBM's Brian Truskowski handled most of the dialogue between IBM and the Five Eyes.

270. As IBM and AT&T's Core Networks' infrastructure is archaic, hackers have been able to gain access to the system on numerous occasions and can roam almost anywhere undetected.

271. On or about June 22, 2018, IBM received a report from the United Kingdom's National Cyber Security Centre of possible compromise of IBM data systems by the APT 10.

272. IBM investigated but never reported its findings or disclosed any actual hacking to the government and its government's clients as required by its contractual and legal obligations.

273. After completing its investigation – called the "Bison Investigation" - IBM's Computer Security Incident Response Team (which included Relator in his capacity as VP of Threat Intelligence) confirmed that four (4) IBM hosts appeared compromised.

274. IBM's efforts to fully investigate these intrusions was thwarted by the lack of activity logs from AT&T and the sophisticated nature of the attacks.

275. That the attacks were difficult to investigate does not obviate the need for full disclosure of the hacking incidents to regulators and Federal Government clients.

276. IBM, with full knowledge that its data cloud was being attacked by a hostile actor, made no disclosures and likewise, AT&T failed to do so as well.

277. The Bison Report - an internal IBM report - dated December 16, 2018, said

> "At the time of this report, the earliest attacker activity dates back to November 2017, with possible but as of yet unconfirmed activity dating back to January 2015. **From the time of the onset of the investigation, attacker activity has been observed on a nearly daily basis. The attackers have compromised and/or accessed nearly 400 compromised accounts and almost 200 total systems and servers across every IBM business unit, eighteen countries, and multiple IBM products**. The attackers have frequently focused on RDP activity between business units, geographies, and critical infrastructure." (Emphasis added.)

278. The Bison Report noted a number of deficiencies in IBM's ability to investigate these intrusions and prevent further attacks. All of the deficiencies are material, and none have ever been disclosed to the Federal Government or regulators. These deficiencies include:

- Currently, cyber security decisions are distributed through the CIO office, the CISO office, the corporate structure, and individual business units. The distributed nature of decision making directly results in an inconsistent security posture across the company and it hampers, and in some cases paralyzes, decision making during a crisis response. The frequent passing of the responsibility to others makes the organization slow to act on critical decisions and **the security culture lacks an understanding of duty to respond, duty to convene and the duty to act during a cyber incident**.

- The decentralized and distributed nature of the current organization enables personnel without security experience to make security decisions without understanding the risk they are presenting to the overall business as the entire organization is only as secure as the weakest link.

- The current escalation model of cyber security incidents to the Cybersecurity Advisory Council (CAC), is based on an

organizational structure and not an operational structure. This results in a disproportional amount of non-subject matter expert voices at the decision-making table.

- It is unclear who can raise an issue to the CAC, as even members of the CAC are reluctant to raise an issue or convene the group as multiple senior executives are members of the team.
    - Pervasive leadership failures occur due to the distributed nature of responsibility and the infrequent and scheduled nature of CAC interactions.
    - **Details of cybersecurity incidents are often edited, redacted and ultimately filtered by the time they reach the CAC** as this information moves northbound in the organization often resulting in a limited view of the risk faced by the organization.
    - Meeting notes, decisions, controls, and event agenda content/presentations from the CAC is not communications southbound in the organization.
- **From a technical standpoint, the decentralized and overall flat nature of the IBM network environment creates a large attack surface, which increases the risk of an attacker gaining an initial foothold on an endpoint or server and the open network allows them to move indiscriminately, laterally throughout different business units without any restrictions**.
- The combination of a CISO/BISO model and endpoint systems being owned by the CIO created a situation where there was not clear ownership or authority to respond to both the Davis and Bison investigations.
- The lack of comprehensive network monitoring due to the outsourcing to AT&T, the slow deployment of Endpoint Detection and Response across supported endpoints and the inability to establish an incident command structure to respond to an incident with speed have resulted in a "loss of control" where **we can neither detect the movement of the adversary nor stop their activities in a comprehensive and timely manner**."

(Emphasis added.)

279. When the APT 10 indictments were unsealed on December 18, 2018, IBM released a statement indicating that nothing sensitive had been lost.[54]

280. This statement was materially misleading in that IBM knows of mass exfiltration of data and knows that at least 176 systems had been impacted but does not have the ability to know what data was taken.

281. The inability to determine the data that was taken is further evidence of just how flawed IBM and AT&T's systems are and just how vulnerable the Federal Government clients are when entrusted to IBM.

282. In or about March 2019, an IBM analyst internally noted that if another rogue network attack occurred, IBM was still unlikely that IBM would catch it.

B. The Trusteer breach

283. In 2013, IBM acquired Trusteer, which is a portfolio of digital identity trust software products.

284. Trusteer's products help financial institutions detect and prevent malware infections and phishing attacks and today, many banks rely on Trusteer's security products.

285. In or about November 2018, an adversary suspected to be a hostile state or sophisticated criminal actor accessed the source code for three of Trusteer's software security products.

286. That intrusion potentially jeopardizes world financial markets.

[54] See "US charges Chinese hackers with over 12-year campaign to steal data from HPE, IBM, NASA and more", December 21, 2018 available at https://www.datacenterdynamics.com/en/news/us-charges-chinese-hackers-over-12-year-campaign-steal-data-hpe-ibm-nasa-and-more/ ("IBM has been aware of the reported attacks and already has taken extensive counter-measures worldwide as part of our continuous efforts to protect the company and our clients against constantly evolving threats. We take responsible stewardship of client data very seriously, and have no evidence that sensitive IBM or client data has been compromised by this threat.")

287. On December 10, 2018, IBM began developing a "client communication" protocol in case the public ever learned of the Trusteer incident.

288. All the while, there was still no disclosure to the Federal Government or regulators.

289. Two months later on January 9, 2019, IBM finally disclosed to the Federal Financial Institutions Examination Council[55] that there was a loss of source code and that the source code was updated.

290. While the failure to timely notify the FFIEC may or may not be a False Claims Act violation in and of itself, it is evidence of the much larger issue of not complying with FAR, DFARS, NIST regulations and FedRamp regulations.

291. Furthermore, the Trusteer breach evidences IBM's direct knowledge that its systems were not in compliance with these mandates and regulations and therefore each time IBM certified that it was in compliance, it violated the False Claims Act.[56]

292. Importantly, IBM never advised any of its banking clients, why a "critical patch" was necessary; once again, IBM failed to disclose this data breach.

293. Subsequently, IBM employee (and attorney), Warren Stramello, sent Relator a private message indicating that AT&T's virtual private network ("VPN") was involved in the Trusteer breach.

---

[55] The FFIEC is a governmental interagency body composed of five banking regulators that is "empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System (FRB), the Federal Deposit Insurance Corporation (FDIC), the National Credit Union Administration (NCUA), the Office of the Comptroller of the Currency (OCC), and the Consumer Financial Protection Bureau (CFPB) and to make recommendations to promote uniformity in the supervision of financial institutions . . . The [FFIEC] is responsible for developing uniform reporting systems for federally supervised financial institutions, their holding companies, and the nonfinancial institution subsidiaries of those institutions and holding companies." https://www.ffiec.gov/about.htm

[56] Aspects of the Trusteer breach may be a violation of the Financial Institutions Reform, Recovery and Enforcement Act of 1979.

294. IBM failed to disclose the breach of AT&T's VPN used to carry data on IBM's network and the subsequent loss of control of the network.

295. IBM rationalizes that since to its knowledge no data has been stolen; it need not report.

296. That is akin to saying that if the military lost the launch codes to its nuclear arsenal, it would not have to report until there was a confirmed missile launch. Here IBM lost the launch codes.

297. Upon information and belief, AT&T likewise failed to disclose the breach to customers or regulators.

298. The Trusteer breach was preventable as the much more serious APT 10 breaches began prior to Trusteer.

C. The Truven Breaches

299. IBM acquired Truven Health Analytics, LLC (hereinafter referred to as "Truven"), on or about April 8, 2016 for approximately $2.6 billion.

300. On August 1, 2014, it was announced that Truven was awarded the $7 billion Center for Medicaid and Medicaid Services' Research, Measurement, Assessment, Design and Analysis contract.[57]

301. This contract was for a period of 5 years and, as such, for all intents and purposes, was considered an IBM federal contract from April 8, 2016 through the expiration of the contract.

302. Truven provides information, analytical tools, benchmarks, research, and services to a variety of healthcare institutions, including hospitals, government agencies, employers, health plans, clinicians, pharmaceutical, biotech and medical device companies.

---

[57] https://www.businesswire.com/news/home/20140801005521/en/Truven-Health-Analytics-Awarded-Center-Medicare-Medicaid

303. Truven is used by the Federal Government for Medicare and Medicaid patient information.

304. There have been several actual and suspected breaches of Truven.

305. In one case, Relator observed an adversary operating on a system in real time. The actor was able to control patient dosing in a neonatal intensive care unit.

306. Later, on June 20, 2019, there was another significant attack on Truven that was part of the same sequence of events.

307. The admin account was compromised giving the actors full access to the entire domain.[58]

308. Neither of these breaches were thoroughly investigated or reported.

309. IBM also chose not to notify clients that the systems in which they were entrusting to provide dosing to neonatal patients has been compromised.

310. IBM lacked the logs to know if the data in these systems was integral which opened the possibility of devastating kinetic implications from this attack.

311. When it appeared that no disclosures would again be forthcoming, Relator elected to resign from his position within IBM.

D. IBM's Coverup Of the Breaches.

312. As Vice President of IBM's Threat Intelligence, Relator is aware of specific instances where IBM senior management became aware of the above-referenced vulnerabilities and/or actively took steps to cover up and conceal these vulnerabilities from regulators and its Federal Government clients.

[58] Given the nature of the data maintained by Truven, HIPAA and HITECH laws and protections were certainly implicated in this breach. As a CSP, IBM is considered a Business Associate under HIPAA rules. HIPAA violations can be a basis for liability pursuant to HIPAA violations. *See generally United States v. America at Home Healthcare and Nursing Services, Ltd.*, 2018 WL 319319 (E.D. Ill. Jan 8, 2018).

313. Relator was blocked from presenting his concerns to the CAC at IBM.

314. Dr. John Kelly was an IBM Senior Vice President reporting directly to the CEO and he was the most senior IBM officer with specific security responsibilities.

315. Given his role, Dr. Kelly had direct access to the NSA and other government agencies.

316. Dr. Kelly blocked attempts to escalate reporting of investigations to the CAC, the board of directors and, upon information and belief, the Federal Government.

317. Fletcher Previn, IBM's Chief Information Officer, directly blocked the usage of endpoint detection and monitoring tools that would have allowed IBM to better understand the scope and source of the above-referenced hacking.

318. Later, when Relator involved IBM's in-house counsel, Previn authorized the limited use of threat detection software ("Carbon Black"), but only on a small segment of IBM's system believed to be free from any adversary activity.

319. In other words, Previn at first resisted attempts to measure the hacking and later when forced, allowed limited investigation in a manner virtually guaranteed to turn up no evidence of hacking.

320. Previn and others acted in a way to prevent from having to verify and therefore report material breaches of IBM's network and cloud environments.

321. While all of this was taking place, IBM's cyber counsel suddenly changed the company's document retention policy on cyber hacking investigations and directed documents be kept for only 7 days.

322. After Relator questioned the legality of such a move, the policy was amended but still only allowed employees involved in the hacking investigation to keep documents for 1 month.[59]

323. Relator had discussions with Shamla Naidoo, IBM's Chief Information Security Officer ("CISO") and Ms. Naidoo told Relator that she would only address Relator's security concerns if Relator could prove that there was a security concern.

324. Naidoo also actively thwarted investigations and ensured that investigators were looking in all the wrong places.

325. On December 6, 2018, Mary O'Brien, General Manager of IBM Security, advised Relator that the data breaches were discussed at the CAC meeting.

326. O'Brien then suggested that Relator "tone down" his reports and stated that she believed then CEO, Virginia Rometty, was also aware of the data breaches but did not want to affect stock prices.

327. Following this warning, on December 19, 2018, O'Brien directed Relator to consider redacting comments about the breaches when preparing a report for the CAC.

---

[59] Such a retention period violates varies provisions of Sarbanes Oxley, specifically:

Section 302: Corporate Responsibility for Financial Reports; and
Section 409: Real Time Issuer Disclosures require the following processes be monitored, logged and audited:

a) network and database activity;
b) internal controls;
c) login attempts;
d) account and user activity; and
e) information access.

In addition, Section 802: Criminal Penalties for Altering Documents, focus on business data retention and protection. It governs alteration, destruction, or concealment of business records to obstruct or influence an investigation.

328. Relator refused to redact comments about the breaches when preparing a report for the CAC.

329. O'Brien also advised that Arvind Krishna – the now current CEO of IBM – was aware of and had read Relator's reports.

330. Relator is aware of a meeting in which senior managers discussed that if word of the data breach and cyber security problems were to become public, investors and customers – including the Federal Government – would lose confidence in the company.

331. On May 19, 2019, Koos Lodewijkx, IBM's Chief Information Security Officer, warned Plaintiff that he "needed to be careful" and that Relator's statements about IBM senior vice presidents engaging in insider trading was upsetting powerful people.

IV. The Significant Flaws in The IBM Core Network And AT&T Core Network Cause the Systems to Violate Multiple Federal Information Processing Standards.

A. NIST SP 800-53 Revision 4 Violations

332. As described above, the FIPS 200 Standard incorporates the NIST SP 800-53 revision 4 recommendations into its mandatory requirements for federal contracts.

333. As IBM and AT&T well know, federal agencies cannot purchase systems that are not FIPS compliant.

334. IBM markets and sells (and causes others to sell) its IBM Core Network systems' services to the Federal government notwithstanding its knowledge that the significant flaws in the systems violate numerous FIPS requirements and NIST SP 800-53 mandates.

335. AT&T markets and sells (and causes others to sell) its AT&T Core Network systems' services to the Federal government notwithstanding its knowledge that the significant flaws in the systems violate numerous FIPS requirements and NIST SP 800-53 mandated standards.

336. Some of these standards include, but are not limited to, the standards set forth in the following paragraphs:

337. AC-3 (Access Enforcement) requires that "The information system enforces approved authorizations for logical access to information and system resources in accordance with applicable access control policies."

338. AC-4 (Information Flow Enforcement) requires that "The information system enforces approved authorizations for controlling the flow of information within the system between interconnected systems based on an organization-defined information flow control policies."

339. AC-6 (Least Privilege) requires that "The organization employs the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions."

340. AC-17 (Remote Access) requires that "The organization: (a) Establishes and documents usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed; and (b) Authorizes remote access to the information system prior to allowing such connections."

341. AC-23 (Data Mining Protection) requires that "The organization employs organization-defined data mining prevention and detection techniques for data storage objects to adequately detect and protect against data mining."

342. AC-24 (Access Control Decisions) requires that "The organization establishes procedures to ensure access control decisions are applied to each access request prior to access enforcement."

343. AU-1 (Audit And Accountability Policy And Procedures) requires that "The organization: (a) Develops, documents, and disseminates to personnel or roles: (1) An audit and accountability policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and (2) Procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls; and (b) Reviews and updates the current: (1) Audit and accountability policy frequency; and (2) Audit and accountability procedures frequency."

344. AU-3 (Content of Audit Records) requires that "The information system generates audit records containing information that establishes what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals or subjects associated with the event."

345. AU-13 (Monitoring for Information Disclosure) requires that "The organization monitors open source information and/or information sites frequency for evidence of unauthorized disclosure of organizational information."

346. IA-2 (Identification and Authentication (Organizational Users)) requires that "The information system uniquely identifies and authenticates organizational users (or processes acting on behalf of organizational users)."

347. IA-3 (Device Identification and Authentication) requires that "The information system uniquely identifies and authenticates specific and/or types of devices before establishing a (one or more): local; remote; network connection."

348. IA-5 (Authenticator Management) requires that "The organization manages information system authenticators by: (a) Verifying, as part of the initial authenticator distribution, the identity of the individual, group, role, or device receiving the authenticator; (b) Establishing

initial authenticator content for authenticators defined by the organization; (c) Ensuring that authenticators have sufficient strength of mechanism for their intended use; (d) Establishing and implementing administrative procedures for initial authenticator distribution, for lost/compromised or damaged authenticators, and for revoking authenticators; (e) Changing default content of authenticators prior to information system installation; (f) Establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; (g) Changing/refreshing authenticators time period by authenticator type; (h) Protecting authenticator content from unauthorized disclosure and modification; (i) Requiring individuals to take, and having devices implement, specific security safeguards to protect authenticators; and (j) Changing authenticators for group/role accounts when membership to those accounts changes."

349. IR-5 (Incident Monitoring) requires that "The organization tracks and documents information system security incidents."

350. SC-8 (Transmission Confidentiality and Integrity) requires that "The information system protects the (one or more): confidentiality; integrity of transmitted information."

351. SC-23 (Session Authenticity) requires that "The information system protects the authenticity of communications sessions."

352. SC-28 (Protection of Information at Rest) requires that "The information system protects the (one or more): confidentiality; integrity of information at rest."

353. SI-2 (Flaw Remediation) requires that "The organization: (a) Identifies, reports, and corrects information system flaws; (b) Tests software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation; (c) Installs security-relevant software and firmware updates within time period of the release of the updates; and (d) Incorporates flaw remediation into the organizational configuration management process."

354. SI-4 (Information System Monitoring) requires that "The organization: (a) Monitors the information system to detect: (1) Attacks and indicators of potential attacks in accordance with monitoring objectives; and (2) Unauthorized local, network, and remote connections; (b) Identifies unauthorized use of the information system through techniques and methods; (c) Deploys monitoring devices: (1) Strategically within the information system to collect organization-determined essential information; and (2) At ad hoc locations within the system to track specific types of transactions of interest to the organization; (d) Protects information obtained from intrusion-monitoring tools from unauthorized access, modification, and deletion; (e) Heightens the level of information system monitoring activity whenever there is an indication of increased risk to organizational operations and assets, individuals, other organizations, or the Nation based on law enforcement information, intelligence information, or other credible sources of information; (f) Obtains legal opinion with regard to information system monitoring activities in accordance with applicable federal laws, Executive Orders, directives, policies, or regulations; and (g) Provides information system monitoring information to personnel or roles (one or more): as needed."

355. SI-6 (Security Function Verification) requires that "The information system: (a) Verifies the correct operation of security functions; (b) Performs this verification (one or more): system transitional states; upon command by user with appropriate privilege; frequency; (c) Notifies personnel or roles of failed security verification tests; and (d) Selection (one or more): shuts the information system down; restarts the information system; alternative action(s) when anomalies are discovered."

356. SI-10 (Information Input Validation) requires that "The information system checks the validity of information inputs."

357. IBM, and upon information and belief, AT&T, failed to adhere to each of the above standards.

B. NIST SP 800-171 Violations

358. As described above, the DFARS requires compliance with NIST SP 800-171 recommendation. As IBM and AT&T well know, the DOD cannot purchase systems that are not NIST SP 800-171 compliant.

359. IBM markets and sells (and causes others to sell) its IBM Core Network systems' services to the DOD and its agencies, notwithstanding its knowledge that the significant flaws in the systems violate numerous NIST SP 800-171 requirements.

360. AT&T markets and sells (and causes others to sell) its AT&T Core Network systems' services to the DOD and its agencies, notwithstanding its knowledge that the significant flaws in the systems violated numerous NIST SP 800-171 requirements.

361. Some of these standards include, but are not limited to, the standards set forth in the following paragraphs.

362. Access Control 3.1.1 requires that IBM and AT&T "Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems."

363. Access Control 3.1.2 requires that IBM and AT&T "Limit information system access to the types of transactions and functions that authorized users are permitted to execute."

364. Access Control 3.1.3 requires that IBM and AT&T "Control the flow of CUI in accordance with approved authorizations."

365. Access Control 3.1.5 requires that IBM and AT&T "Employ the principal of least privilege, including specific security functions and privileged accounts."

366. Access Control 3.1.12 requires that IBM and AT&T "Monitor and control remote access sessions."

367. Access Control 3.1.17 requires that IBM and AT&T "Protect wireless access using authentication and encryption."

368. Access Control 3.1.20 requires that IBM and AT&T "Verify and control/limit connections to and use of external information systems."

369. Audit and Accountability 3.3.1 requires that IBM and AT&T "Create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity."

370. Audit and Accountability 3.3.2; requires that IBM and AT&T "Ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions."

371. Identification and Authentication 3.5.1 requires that IBM and AT&T "Identify information system users, processes acting on behalf of users, or devices."

372. Identification and Authentication 3.5.2 requires that IBM and AT&T "Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems."

373. Risk Assessment 3.11.3 requires that IBM and AT&T "Remediate vulnerabilities in accordance with assessment of risk."

374. System and Communications Protection 3.13.8 requires that IBM and AT&T "Implement cryptographic mechanisms to prevent unauthorized disclosure of CUI during transmission unless otherwise protected by alternative physical safeguards."

375. System and Communications Protection 3.13.15 requires that IBM and AT&T "Protect the authenticity of communications sessions."

376. System and Communications Protection 3.13.16 requires that IBM and AT&T "Protect the confidentiality of CUI at rest."

377. System and Information Integrity 3.14.1 requires that IBM and AT&T "Identify, report, and correct information and information system flaws in a timely manner."

378. System and Information Integrity 3.14.3 requires that IBM and AT&T "Monitor information system security alerts and advisories and take appropriate actions in response." IBM and AT&T failed this standard by failing to take any response whatsoever to the unauthorized data access and exfiltration brought to its attention by Relator.

379. System and Information Integrity 3.14.6 requires that IBM and AT&T "Monitor the information system including inbound and outbound communication traffic, to detect attacks and indicators of potential attacks."

380. System and Information Integrity 3.14.7 requires that IBM and AT&T "Identify unauthorized use of the information system."

381. IBM, and upon information and belief, AT&T, failed to adhere to each of the above standards.

C. FedRamp and NIST SP 800-37 Violations

382. As described above, FedRamp certification requires compliance with NIST SP 800-37 recommendations.

383. As IBM and AT&T well know, the Federal Government cannot purchase cloud-based systems that are not NIST SP 800-37 compliant.

384. IBM markets and sells (and causes others to sell) its cloud-based systems to the Federal Government notwithstanding its knowledge that the significant flaws in the systems violate numerous NIST SP 800-37 requirements.

385. AT&T markets and sells (and causes others to sell) its cloud-based systems to the Federal Government notwithstanding its knowledge that the significant flaws in the systems violate numerous NIST SP 800-37 requirements

386. Some of these standards include, but are not limited to, the standards set forth in the following paragraphs:

387. Task P-7 (Continuous Monitoring Strategy – Organization) requires that IBM and AT&T "Develop and implement an organization-wide strategy for continuously monitoring effectiveness," noting that "An important aspect of risk management is the ability to monitor the security and privacy posture across the organization and the effectiveness of controls implemented within or inherited by organizational systems on an ongoing basis. An effective organization-wide continuous monitoring strategy is essential to efficiently and cost-effectively carrying out such monitoring."

388. Task S-5 (Continuous Monitoring Strategy – System) required that IBM and AT&T "Develop and implement a system-level strategy for monitoring control effectiveness that is consistent with and supplements the organizational continuous monitoring strategy."

389. Task I-1 (Control Implementation) requires that IBM and AT&T "Implement the controls in the security and privacy plans." These controls include those set forth in Cybersecurity

Framework Information Protection Process and Procedures ("PR.IP")-1[60] and PR.IP-2.[61] PR.IP's are "Security policies (that address purpose, scope, roles, responsibilities, management, commitment, and coordination amongst organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets."[62]

390. Task A-4 (Assessment Reports) requires that IBM and AT&T "Prepare the assessment reports documenting the findings and recommendations from the control assessments." An independent evaluation of privacy program and practices is not required per OBM A-130. However, an assessment report is mandated per Task A-4. Task A-4 notes that "Assessment reports are an important factor in a determining risk to organizational operations and assets, individuals, other organizations, and the Nation by the authorizing official."

391. Task A-5 (Remediation Actions) requires that IBM and AT&T "Conduct initial remediation actions on the controls and reassesses remediated controls." Task A-5 contemplates deficiencies that are discovered after a system has been implemented; thus, providing the CSP an opportunity to correct the issue.

392. Task R-5 (Authorization Reporting) requires that IBM and AT&T "Report the authorization decision and any deficiencies in controls that represent significant security or privacy risk."

393. Task M-3 (Ongoing Risk Response) requires that IBM and AT&T "Respond to risk based on the results of ongoing monitoring activities, risk assessments, and outstanding items in plans of action and milestones."

---

[60] PR.IP-1 is a "baseline configuration of information technology/industrial control systems [that] is created and maintained incorporating security principals (e.g. concept of least functionality." PR.IP-1 refers back to NIST SP 800-53 Rev. 4 Sections CM-2, CM-3, CM-4, CM-5, CM-6, CM-7, CM-9 and SA-10. https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf at p.33

[61] PR.IP-2 requires that a "System Development Life Cycle to manage systems is implemented." *Id.*

[62] *Id.*

394. IBM and upon information and belief, AT&T, failed to adhere to each of the above standards, resulting in the improper access to and exfiltration of Federal data by unauthorized users.

COUNT I
Federal False Claims Act – Against IBM
31 U.S.C. § 3729(a)(1)

395. Relator restates and realleges the allegations set forth in paragraphs one (1) through three hundred and ninety-four (394) above, as if fully set forth herein.

396. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729, *et seq*.

397. IBM entered into multiple contracts with the Federal Government wherein they had access to and stored Protected Information belonging to the government on their computer systems, which required IBM to meet minimum cyber security requirements to protect that information as set for above.

398. The Federal Government set forth these minimum cyber security requirements in FAR, DFARS, NIST SP 800-53, NIST SP 800-171 and NIST SP 800-37. Compliance with these regulations was not only a pre-requisite to payment on these contracts but IBM was required to meet these requirements to participate in the contracts at all.

399. IBM falsely represented that it was compliant with the DFARS cyber security regulations, NIST SP 800-53 standards and NIST SP 800-171 standards. This included, but is not limited to, signing contracts that included these cyber security requirements that IBM knew it was not complying with

400. IBM concealed information form the Federal Government regarding the state of its compliance with these cyber security requirements because it knew that it would not be eligible to participate in the federal contracts and that if it disclosed this information, it would not be awarded the contracts.

401. The Federal Government was misled by IBM's false statements and would never have entered into the contracts with IBM had the government been aware that IBM was not in compliance with the requisite cyber security standards and regulations.

402. Compliance with these regulations was material to the Federal Government's decision to enter these contracts as no federal officer has authority to enter into a contract where the contractor is not complying with the law.

403. By virtue of the acts described above, IBM knowingly presented or caused to be presented or caused to be presented, false or fraudulent claims for the IBM Core Network systems and related services to the United States Government for payment or approval.

404. By virtue of the acts described above, IBM knowingly has conspired with AT&T and other of its partners and affiliates, to commit statutory violations as set forth in this Count.

405. Relator cannot at this time identify all of the false claims for payment that were caused by IBM's conduct. The false claims were presented by numerous separate entities across the United States and submitted to numerous Federal Government agencies. Relator has no control over or dealings with such entities and has no access to the records in their possession.

406. The United States Government, unaware of the falsity of the records, statements, and claims, made or caused to be made by IBM, paid, and continues to pay the claims that would not be paid but for IBM's illegal conduct.

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

408. Additionally, the United States is entitled to the maximum penalty provided for in the FCA for each and every violation alleged herein.

COUNT II
Federal False Claims Act – Against AT&T
31 U.S.C. § 3729(a)(1)

409. Relator restates and realleges the allegations set forth in paragraphs one (1) through three hundred and ninety-four (394) above, as if fully set forth herein.

410. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729, *et seq*.

411. AT&T entered into multiple contracts with the Federal Government wherein they had access to and stored Protected Information belonging to the government on their computer systems, which required AT&T to meet minimum cyber security requirements to protect that information as set for above.

412. The Federal Government set forth these minimum cyber security requirements in FARs, DFARS, NIST SP 800-53, NIST SP 800-171 and NIST SP 800-37. Compliance with these regulations was not only a pre-requisite to payment on these contracts but AT&T was required to meet these requirements to participate in the contracts at all.

413. AT&T falsely represented that it was compliant with the DFARS cyber security regulations, NIST SP 800-53 standards and NIST SP 800-171 standards. This included, but is not limited to, signing contracts that included these cyber security requirements that AT&T knew it was not complying with

414. AT&T concealed information form the Federal Government regarding the state of its compliance with these cyber security requirements because it knew that it would not be eligible to participate in the federal contracts and that if it disclosed this information, it would not be awarded the contracts.

415. The Federal Government was misled by AT&T's false statements and would never have entered into the contracts with AT&T had the government been aware that AT&T was not in compliance with the requisite cyber security standards and regulations.

416. Compliance with these regulations was material to the Federal Government's decision to enter these contracts as no federal officer has authority to enter into a contract where the contractor is not complying with the law.

417. By virtue of the acts described above, AT&T knowingly presented or caused to be presented or caused to be presented, false or fraudulent claims for the AT&T Core Network systems and related services to the United States Government for payment or approval.

418. By virtue of the acts described above, AT&T knowingly has conspired with IBM and other of its partners and affiliates, to commit statutory violations as set forth in this Count.

419. Relator cannot at this time identify all of the false claims for payment that were caused by AT&T's conduct. The false claims were presented by numerous separate entities across the United States and submitted to numerous Federal Government agencies. Relator has no control over or dealings with such entities and has no access to the records in their possession.

420. The United States Government, unaware of the falsity of the records, statements, and claims, made or caused to be made by AT&T, paid, and continues to pay the claims that would not be paid but for AT&T's illegal conduct.

421. By reason of AT&T's fraudulent acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

422. Additionally, the United States is entitled to the maximum penalty provided for in the FCA for each and every violation alleged herein.

COUNT III
Federal False Claims Act – Against IBM
31 U.S.C. § 3729(a)(2)

423. Relator restates and realleges the allegations set forth in paragraphs one (1) through three hundred and ninety-four (394) above, as if fully set forth herein.

424. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729, *et seq.*

425. IBM entered into multiple contracts with the Federal Government wherein they had access to and stored Protected Information belonging to the government on their computer systems, which required IBM to meet minimum cyber security requirements to protect that information as set for above.

426. The Federal Government set forth these minimum cyber security requirements in FARs, DFARS, NIST SP 800-53, NIST SP 800-171 and NIST SP 800-37. Compliance with these regulations was not only a pre-requisite to payment on these contracts but IBM was required to meet these requirements to participate in the contracts at all.

427. IBM falsely represented that it was compliant with the DFARS cyber security regulations, NIST SP 800-53 standards and NIST SP 800-171 standards. This included, but is not limited to, signing contracts that included these cyber security requirements that IBM knew it was not complying with

428. IBM concealed information form the Federal Government regarding the state of its compliance with these cyber security requirements because it knew that it would not be eligible to participate in the federal contracts and that if it disclosed this information, it would not be awarded the contracts.

429. The Federal Government was misled by IBM's false statements and would never have entered into the contracts with IBM had the government been aware that IBM was not in compliance with the requisite cyber security standards and regulations.

430. Compliance with these regulations was material to the Federal Government's decision to enter these contracts as no federal officer has authority to enter into a contract where the contractor is not complying with the law.

431. By virtue of the acts described above, IBM knowingly made, used, or caused to be made or used, false, or fraudulent records or statements material to false or fraudulent claims for the IBM Core Network systems and related services to the United States Government.

432. By virtue of the acts described above, IBM knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the United States Government, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the United States Government.

433. By virtue of the acts described above, IBM knowingly has conspired with AT&T and other of its partners and affiliates, to commit statutory violations as set forth in this Count.

434. Relator cannot at this time identify all of the false claims for payment that were caused by IBM's conduct. The false claims were presented by numerous separate entities across the United States and submitted to numerous Federal Government agencies. Relator has no control over or dealings with such entities and has no access to the records in their possession.

435. The United States Government, unaware of the falsity of the records, statements, and claims, made or caused to be made by IBM, paid, and continues to pay the claims that would not be paid but for IBM's illegal conduct.

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

437. Additionally, the United States is entitled to the maximum penalty provided for in the FCA for each and every violation alleged herein.

COUNT IV
Federal False Claims Act – Against AT&T
31 U.S.C. § 3729(a)(2)

438. Relator restates and realleges the allegations set forth in paragraphs one (1) through three hundred and ninety-four (394) above, as if fully set forth herein.

439. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729, *et seq*.

440. AT&T entered into multiple contracts with the Federal Government wherein they had access to and stored Protected Information belonging to the government on their computer systems, which required AT&T to meet minimum cyber security requirements to protect that information as set for above.

441. The Federal Government set forth these minimum cyber security requirements in FARs, DFARS, NIST SP 800-53, NIST SP 800-171 and NIST SP 800-37. Compliance with these regulations was not only a pre-requisite to payment on these contracts but AT&T was required to meet these requirements to participate in the contracts at all.

442. AT&T falsely represented that it was compliant with the DFARS cyber security regulations, NIST SP 800-53 standards and NIST SP 800-171 standards. This included, but is not

limited to, signing contracts that included these cyber security requirements that AT&T knew it was not complying with

443. AT&T concealed information form the Federal Government regarding the state of its compliance with these cyber security requirements because it knew that it would not be eligible to participate in the federal contracts and that if it disclosed this information, it would not be awarded the contracts.

444. The Federal Government was misled by AT&T's false statements and would never have entered into the contracts with AT&T had the government been aware that AT&T was not in compliance with the requisite cyber security standards and regulations.

445. Compliance with these regulations was material to the Federal Government's decision to enter these contracts as no federal officer has authority to enter into a contract where the contractor is not complying with the law.

446. By virtue of the acts described above, AT&T knowingly made, used, or caused to be made or used, false or fraudulent records or statements material to false or fraudulent claims for the AT&T Core Network systems and related services to the United States Government.

447. By virtue of the acts described above, AT&T knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money to the United States Government, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money to the United States Government.

448. By virtue of the acts described above, AT&T knowingly has conspired with IBM and other of its partners and affiliates, to commit statutory violations as set forth in this Count.

449. Relator cannot at this time identify all of the false claims for payment that were caused by AT&T's conduct. The false claims were presented by numerous separate entities across

the United States and submitted to numerous Federal Government agencies. Relator has no control over or dealings with such entities and has no access to the records in their possession.

450. The United States Government, unaware of the falsity of the records, statements, and claims, made or caused to be made by AT&T, paid, and continues to pay the claims that would not be paid but for AT&T's illegal conduct.

451. By reason of AT&T's fraudulent acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

452. Additionally, the United States is entitled to the maximum penalty provided for in the FCA for each and every violation alleged herein.

COUNT V
Federal False Claims Act – Against IBM
31 U.S.C. § 3729(a)(3)

453. Relator restates and realleges the allegations set forth in paragraphs one (1) through three hundred and ninety-four (394) above, as if fully set forth herein.

454. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729, *et seq*.

455. IBM entered into multiple contracts with the Federal Government wherein they had access to and stored Protected Information belonging to the government on their computer systems, which required IBM to meet minimum cyber security requirements to protect that information as set for above.

456. The Federal Government set forth these minimum cyber security requirements in FARs, DFARS, NIST SP 800-53, NIST SP 800-171 and NIST SP 800-37. Compliance with these regulations was not only a pre-requisite to payment on these contracts but IBM was required to meet these requirements to participate in the contracts at all.

457. IBM falsely represented that it was compliant with the DFARS cyber security regulations, NIST SP 800-53 standards and NIST SP 800-171 standards. This included, but is not limited to, signing contracts that included these cyber security requirements that IBM knew it was not complying with

458. IBM concealed information form the Federal Government regarding the state of its compliance with these cyber security requirements because it knew that it would not be eligible to participate in the federal contracts and that if it disclosed this information, it would not be awarded the contracts.

459. The Federal Government was misled by IBM's false statements and would never have entered into the contracts with IBM had the government been aware that IBM was not in compliance with the requisite cyber security standards and regulations.

460. Compliance with these regulations was material to the Federal Government's decision to enter these contracts as no federal officer has authority to enter into a contract where the contractor is not complying with the law.

461. By virtue of the acts described above, IBM knowingly has conspired with AT&T and other of its partners and affiliates, to defraud the United States by submitting false and fraudulent claims for reimbursement to the United States Government.

462. Relator cannot at this time identify all of the false claims for payment that were caused by IBM's conduct. The false claims were presented by numerous separate entities across the United States and submitted to numerous Federal Government agencies. Relator has no control over or dealings with such entities and has no access to the records in their possession.

463. The United States Government, unaware of the falsity of the records, statements, and claims, made or caused to be made by IBM, paid, and continues to pay the claims that would not be paid but for IBM's illegal conduct.

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

465. Additionally, the United States is entitled to the maximum penalty provided for in the FCA for each and every violation alleged herein.

COUNT VI
Federal False Claims Act – Against AT&T
31 U.S.C. § 3729(a)(3)

466. Relator restates and realleges the allegations set forth in paragraphs one (1) through three hundred and ninety-four (394) above, as if fully set forth herein.

467. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729, *et seq*.

468. AT&T entered into multiple contracts with the Federal Government wherein they had access to and stored Protected Information belonging to the government on their computer systems, which required AT&T to meet minimum cyber security requirements to protect that information as set for above.

469. The Federal Government set forth these minimum cyber security requirements in FARs, DFARS, NIST SP 800-53, NIST SP 800-171 and NIST SP 800-37. Compliance with these regulations was not only a pre-requisite to payment on these contracts but AT&T was required to meet these requirements to participate in the contracts at all.

470. AT&T falsely represented that it was compliant with the DFARS cyber security regulations, NIST SP 800-53 standards and NIST SP 800-171 standards. This included, but is not

limited to, signing contracts that included these cyber security requirements that AT&T knew it was not complying with

471. AT&T concealed information form the Federal Government regarding the state of its compliance with these cyber security requirements because it knew that it would not be eligible to participate in the federal contracts and that if it disclosed this information, it would not be awarded the contracts.

472. The Federal Government was misled by AT&T's false statements and would never have entered into the contracts with AT&T had the government been aware that AT&T was not in compliance with the requisite cyber security standards and regulations.

473. Compliance with these regulations was material to the Federal Government's decision to enter these contracts as no federal officer has authority to enter into a contract where the contractor is not complying with the law.

474. By virtue of the acts described above, AT&T knowingly has conspired with IBM and other of its partners and affiliates, to defraud the United States by submitting false and fraudulent claims for reimbursement to the United States Government.

475. Relator cannot at this time identify all of the false claims for payment that were caused by AT&T's conduct. The false claims were presented by numerous separate entities across the United States and submitted to numerous Federal Government agencies. Relator has no control over or dealings with such entities and has no access to the records in their possession.

476. The United States Government, unaware of the falsity of the records, statements, and claims, made or caused to be made by AT&T, paid, and continues to pay the claims that would not be paid but for AT&T's illegal conduct.

477. By reason of AT&T's fraudulent acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

478. Additionally, the United States is entitled to the maximum penalty provided for in the FCA for each and every violation alleged herein.

COUNT VII
Federal False Claims Act – Against IBM
31 U.S.C. § 3729(a)(7)

479. Relator restates and realleges the allegations set forth in paragraphs one (1) through three hundred and ninety-four (394) above, as if fully set forth herein.

480. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729, *et seq*.

481. IBM entered into multiple contracts with the Federal Government wherein they had access to and stored Protected Information belonging to the government on their computer systems, which required IBM to meet minimum cyber security requirements to protect that information as set for above.

482. The Federal Government set forth these minimum cyber security requirements in FARs, DFARS, NIST SP 800-53, NIST SP 800-171 and NIST SP 800-37. Compliance with these regulations was not only a pre-requisite to payment on these contracts but IBM was required to meet these requirements to participate in the contracts at all.

483. IBM falsely represented that it was compliant with the DFARS cyber security regulations, NIST SP 800-53 standards and NIST SP 800-171 standards. This included, but is not limited to, signing contracts that included these cyber security requirements that IBM knew it was not complying with

484. IBM concealed information form the Federal Government regarding the state of its compliance with these cyber security requirements because it knew that it would not be eligible to participate in the federal contracts and that if it disclosed this information, it would not be awarded the contracts.

485. The Federal Government was misled by IBM's false statements and would never have entered into the contracts with IBM had the government been aware that IBM was not in compliance with the requisite cyber security standards and regulations.

486. Compliance with these regulations was material to the Federal Government's decision to enter these contracts as no federal officer has authority to enter into a contract where the contractor is not complying with the law.

487. By virtue of the acts described above, IBM failed to reimburse the United States Government for moneys wrongfully received.

488. Relator cannot at this time identify all of the false claims for payment that were caused by IBM's conduct. The false claims were presented by numerous separate entities across the United States and submitted to numerous Federal Government agencies. Relator has no control over or dealings with such entities and has no access to the records in their possession.

489. The United States Government, unaware of the falsity of the records, statements, and claims, made or caused to be made by IBM, paid, and continues to pay the claims that would not be paid but for IBM's illegal conduct.

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

491. Additionally, the United States is entitled to the maximum penalty provided for in the FCA for each and every violation alleged herein.

COUNT VIII
Federal False Claims Act – Against AT&T
31 U.S.C. § 3729(a)(3)

492. Relator restates and realleges the allegations set forth in paragraphs one (1) through three hundred and ninety-four (394) above, as if fully set forth herein.

493. This is a claim for treble damages and penalties under the FCA, 31 U.S.C. § 3729, *et seq*.

494. AT&T entered into multiple contracts with the Federal Government wherein they had access to and stored Protected Information belonging to the government on their computer systems, which required AT&T to meet minimum cyber security requirements to protect that information as set for above.

495. The Federal Government set forth these minimum cyber security requirements in FARs, DFARS, NIST SP 800-53, NIST SP 800-171 and NIST SP 800-37. Compliance with these regulations was not only a pre-requisite to payment on these contracts but AT&T was required to meet these requirements to participate in the contracts at all.

496. AT&T falsely represented that it was compliant with the DFARS cyber security regulations, NIST SP 800-53 standards and NIST SP 800-171 standards. This included, but is not limited to, signing contracts that included these cyber security requirements that AT&T knew it was not complying with

497. AT&T concealed information form the Federal Government regarding the state of its compliance with these cyber security requirements because it knew that it would not be eligible

to participate in the federal contracts and that if it disclosed this information, it would not be awarded the contracts.

498. The Federal Government was misled by AT&T's false statements and would never have entered into the contracts with AT&T had the government been aware that AT&T was not in compliance with the requisite cyber security standards and regulations.

499. Compliance with these regulations was material to the Federal Government's decision to enter these contracts as no federal officer has authority to enter into a contract where the contractor is not complying with the law.

500. By virtue of the acts described above, AT&T failed to reimburse the United States Government for moneys wrongfully received.

501. Relator cannot at this time identify all of the false claims for payment that were caused by AT&T's conduct. The false claims were presented by numerous separate entities across the United States and submitted to numerous Federal Government agencies. Relator has no control over or dealings with such entities and has no access to the records in their possession.

502. The United States Government, unaware of the falsity of the records, statements, and claims, made or caused to be made by AT&T, paid, and continues to pay the claims that would not be paid but for AT&T's illegal conduct.

503. By reason of AT&T's fraudulent acts, the United States has been damaged, and continues to be damaged, in a substantial amount to be determined at trial.

504. Additionally, the United States is entitled to the maximum penalty provided for in the FCA for each and every violation alleged herein.

PRAYER FOR RELIEF

WHEREFORE, *qui tam* Relator prays for judgment against the Defendants as follows:

1. That Defendants cease and desist from violating the FCA, 31 U.S.C. § 3729, *et seq.*;

2. That this Court enter judgment against the Defendants in an amount equal to three times the amount of damages the United States have sustained because of the Defendants' actions, plus a civil penalty for each violation of 31 U.S.C. § 3729;

3. That the *qui tam* Relator be awarded the maximum amount allowed pursuant to § 3730(d) of the False Claims Act;

4. That the *qui tam* Relator be awarded all costs of this action, including attorneys' fees and expenses; and

5. That the United States and the *qui tam* Relator recover such other and further relief as the Court deems just and proper.

DEMAND FOR JURY TRIAL

Pursuant to Rule 38 of the Federal Rules of Civil Procedure, *qui tam* Relator, William Barlow, hereby demands a trial by jury.

Respectfully submitted this 9th day of September, 2020.

David Weber

David P. Weber
SDNY Bar No.: DW7073
Goodwin Weber PLLC
267 Kentlands Boulevard
Suite 250
Gaithersburg, MD 20878
(301) 850-3370 - Telephone
(301) 850-3374 – Facsimile
David.Weber@goodwinweberlaw.com

-and –

Brian H. Mahany
Wisconsin Bar No.: 1065623
(Pro Hac Vice Admission Pending)
Bryen N. Hill

Florida Bar No.: 0095993
(Pro Hac Vice Admission Pending)
Mahany Law
8112 West Bluemound Road
Suite 101
Wauwatosa, WI 53213
(414) 258-2375 – Telephone
(414) 777-0776 – Fax
brian@mahanylaw.com
bhill@mahanylaw.com

Attorneys for *qui tam* Relator