

Hand-Delivered

IN THE UNITED STATES DISTRICT COURT
FOR THE WESTERN DISTRICT OF NORTH CAROLINA

FILED
CHARLOTTE, NC

MAR 25 2022

US DISTRICT COURT
WESTERN DISTRICT OF NC

UNITED STATES OF AMERICA ex rel.)

[REDACTED])

Plaintiff-Relator)

v.)

HONEYWELL INTERNATIONAL,)
INC.)

Defendant)

Civil Action No. 3:22-cv-129 - EDW

FILED IN CAMERA
AND UNDER SEAL

Jury Trial Requested

COMPLAINT

TABLE OF CONTENTS

I.	STATEMENT OF THE CASE	1
II.	LEGAL FRAMEWORK	8
A.	Parties	8
B.	Jurisdiction and Venue	9
C.	Time Period	10
D.	The False Claims Act	10
III.	THE REGULATORY FRAMEWORK	12
A.	Government Contracting Requirements.....	12
B.	Protection of CUI Is Critical to National Security	19
IV.	THE QUANTUM CONTRACTS	24
V.	THE FRAUDULENT SCHEME.....	31
A.	Knowing Failure to Comply with Cybersecurity Standards	34
1.	The Firewall Was a Smokescreen.....	38
2.	Inadequate Malicious Code Protection	43
3.	Inadequate Access Control	51
4.	Inadequate Incident Testing & Response	61
5.	Inadequate Oversight of Suspicious Activity	64
B.	Knowing Failure to Report Cybersecurity Incidents or Breaches	73
VI.	MATERIALITY	75
VII.	[REDACTED]	81
VIII.	COUNTS.....	88

This is a False Claims Act *qui tam* action by Relator to recover treble damages and civil penalties arising from the actions of Honeywell International Inc. (Honeywell or Defendant).

I. STATEMENT OF THE CASE

1. Honeywell International Inc. is an American publicly traded, multinational conglomerate corporation with over 100,000 employees, headquartered in Charlotte, North Carolina. It operates in several areas of business such as aerospace, building technologies, chemicals, safety, supply chain, health care and pharma research and development to provide quantum-computing. Honeywell is a government contractor that provides services related to its quantum-computing technologies to the U.S. Department of Defense [REDACTED]. Honeywell also manages the U.S. Department of Energy's Kansas City National Security Campus. At issue in this case are government contracts for Honeywell's quantum-computing services.

2. The Government awarded Honeywell tens of millions of dollars in contracts for services related to Honeywell's quantum computing technologies. Quantum computers perform higher-speed calculations than normal computers—they are super computers—which the Government needs for intelligence and law enforcement. The Government contracted with Honeywell under the belief that Honeywell's proprietary quantum computer technology would support and

enhance national security interests. Because of its speed alone, quantum computing is superior to any other technology in support of national security and was expected to enhance the United States' own satellite technology.

3. To perform under the Quantum Contracts, Honeywell was required to handle and store raw Government data and information in native format, which the quantum computers then used to perform specified calculations and other work. That raw data and information was designated by the Government as "Controlled Unclassified Information," which generally means the information, while not classified, is not intended to be shared with the public. It includes drawings, specifications, testing, simulations and other information related to U.S. secret intelligence programs that no other country possesses.

4. The Government secrets entrusted to Honeywell were promised to be "walled off" from external threats, especially those posed by foreign intelligence operatives like the Russian SolarWinds Attackers. In the wrong hands, this Controlled Unclassified Information could jeopardize American national security, impair the Government's operations, enable an adversary to replicate rare and highly sensitive U.S. defense technology and use it against us, and infiltrate the inner workings of essential U.S. Department of Defense functions [REDACTED]

[REDACTED]

5. Accordingly, a series of contractual provisions and Federal Cybersecurity Requirements obligated Honeywell to protect this sensitive Government information on a secure network.

6. Despite these obligations and the national security implications, Honeywell knowingly failed to provide even the most basic cybersecurity safeguards to protect the sensitive Government information on its network, with a firewall as its primary protection, inadequate antivirus software—a basic safeguard that even the average consumer might put in place on their personal computers; inadequate control over who had access to sensitive Government information; and inadequate incident response training and testing for employees; and knowingly failed to properly respond to suspicious activity that could compromise sensitive Government information.

7. Further, on information and belief, Honeywell knowingly failed to report cyber incidents of the network containing the sensitive information—called the “Gray Network”—to the proper officials at the U.S. Department of Defense.

8. When the SolarWinds Attack occurred in early 2020, Honeywell’s chickens came home to roost. The Gray Network, containing the Controlled Unclassified Information was easy pickings for even beginner hackers let alone the SolarWinds Attackers. Left to its own devices, Honeywell will continue to leave U.S. national security vulnerable.

9. Honeywell's dismissive approach to cybersecurity protection for the U.S. Government's sensitive information was in stark contrast to Honeywell's commitment to the commercial side. Honeywell invested significant money, resources and human capital to its quantum commercial business because of its ambitions to grow this sector.

10. Honeywell intentionally devoted these resources to its quantum startup business to the detriment of its obligations to the Government and failed to properly oversee and protect the Controlled Unclassified Information on Honeywell's quantum computing network known as the Gray Network, even though Honeywell had the capability to provide the necessary protections. This failure to prioritize its work for the Government led to systemic and material violations of the Quantum Contracts and Federal Cybersecurity Requirements.

11. Simply put, Honeywell's pattern and practice alleged in this Complaint deprived the Government of the cybersecurity benefits it bargained for. Troublingly, the Government paid Honeywell for an advanced technology intended to protect national security and serve the public interest, but instead, Honeywell put national security at risk in its performance of the contracts.

12. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government

paid those claims.

13. The protection of U.S. Government secrets does not involve partisan politics. Both the last and the current Administration have prioritized holding government contractors accountable for knowing cybersecurity failures. Under the last Administration, the National Institute of Standards and Technology created Cybersecurity Requirements, while stating that when the United States entrusts contractors with Controlled Unclassified Information, safeguarding such material “is of paramount importance” because it can “directly impact the ability of the federal government to successfully conduct its essential missions.”

14. The Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012 (“DFARS 7012”) applies to all U.S. Department of Defense contracts, including these Quantum Contracts, and requires contractors like Honeywell to implement technical and procedural controls as specified by the NIST Cybersecurity Requirements to protect sensitive information and to timely report cyber incidents.

15. In part driven by the Russian SolarWinds Attack, which became public in December 2020, the current Administration through an Executive Order has stepped up the timetable to hold government contractors like Honeywell accountable for the failure to protect the Government’s sensitive information. To combat cyber threats, “[t]he private sector must adapt to the continuously changing

threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace.”

16. Honeywell has placed in jeopardy our collective national security and the victims of this fraud are ordinary Americans, including taxpayers. In doing so, Honeywell failed to heed the words of Supreme Court Justice Oliver Wendell Holmes: “Men must turn square corners when they deal with the government” whether those corners are real or virtual.

17. This case is **precisely** the type of fraud scheme the U.S. Department of Justice is seeking to remedy under the False Claims Act.

18. The Deputy Attorney General (DAG) announced three months ago that DOJ had created a Civil Cyber-Fraud Initiative to pursue cyber fraud by government contractors like the fraud scheme alleged here, to “hold accountable entities or individuals that put U.S. information or systems at risk by

- knowingly providing deficient cybersecurity products or services
- knowingly misrepresenting their cybersecurity practices or protocols, or
- knowingly violating obligations to monitor and report cybersecurity incidents and breaches.”

Press Release, Office of Public Affairs, U.S. Department of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative

(Oct. 6, 2021), <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>; and <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

19. Use of the False Claims Act as an enforcement tool in this case will hold Honeywell accountable for its knowing and material cybersecurity failures, deter future cyber misconduct by Honeywell and other government contractors, and protect highly confidential Government information from exposure in the event of another attack on Honeywell systems like (or worse than) the SolarWinds Attack.

20. The DAG further directed comments at whistleblowers: “to those who witness irresponsibility that exposes the government to cyber breaches, our message is this: if you see something, say something.” But for Relator the Government would not be on notice of the allegations in this Complaint.

<https://www.justice.gov/opa/speech/deputy-attorney-general-lisa-o-monaco-and-assistant-attorney-general-kenneth-polite-jr>

II. LEGAL FRAMEWORK

A. Parties

21. Relator alleges, based upon personal knowledge, relevant documents, and information, and on information and belief, the facts set forth in this Complaint.

22. Relator has extensive first-hand knowledge of Defendant's pattern and practice alleged in the Complaint.

23. Relator was retaliated against for raising, objecting to, and opposing the pattern and practice alleged in this Complaint.

24. Relator has standing to bring this action pursuant to 31 U.S.C. § 3730(b)(1). Relator is entitled to either between 15-25 percent of the proceeds that result from this action, or any settlement of the claims raised or identified in this complaint, under 31 U.S.C. § 3730(d)(1); or between 25-35 percent of the proceeds pursuant to 31 U.S.C. § 3730(d)(2); or of any amounts specified in any state's False Claims Act.

25. Relator voluntarily disclosed to the Government the information on which the allegations or transactions in the claims are based; and Relator has knowledge that is independent of and materially adds to any publicly disclosed allegations or transactions that may exist and has voluntarily provided the information to the Government before filing an action under this section. Relator

is the original source of these allegations as defined in 31 U.S.C. §§ 3730(e)(4)(A)-(B).

26. Relator has complied with all procedural requirements of the laws under which this Complaint is brought.

27. Defendant Honeywell International Inc. (Honeywell or Defendant) is an American publicly traded, multinational conglomerate corporation with over 100,000 employees, incorporated in Delaware, and headquartered in Charlotte, North Carolina.

28. Honeywell operates in several areas of business such as aerospace, building technologies, chemicals, safety, supply chain, health care, pharma and research and development to provide quantum-computing services. Honeywell is also a government contractor that provides services related to its quantum-computing technologies to the U.S. Department of Defense [REDACTED]. Honeywell also manages the U.S. Department of Energy's Kansas City National Security Campus. At issue in this case are government contracts for Honeywell's quantum computing.

B. Jurisdiction and Venue

29. This Court has subject matter jurisdiction over the claims asserted in this Complaint, pursuant to the False Claims Act, 31 U.S.C. §§ 3729 *et seq.*, including § 3730(h), and 28 U.S.C. §§ 1331, 1345. This Court also has

supplemental jurisdiction over the related state law claims pursuant to 28 U.S.C. § 1367(a).

30. Venue is proper in this judicial district, pursuant to 31 U.S.C. §§ 3732(a) and 28 U.S.C. 1391(b) and (c), because defendant may be found, resides, and/or transacts business in this District, or because an act, proscribed by 31 U.S.C. § 3729, occurred in this District.

C. Time Period

31. On information and belief, Honeywell's conduct alleged in this Complaint began at the start of its earliest Quantum Contract.

D. The False Claims Act

32. This Complaint alleges violations of the False Claims Act.

33. The False Claims Act provides, in part: Liability for Certain Acts.

— (1) In general. —[] any person who—

(A) knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval

(B) knowingly makes, uses, or causes to be made or used, a false record or statement material to a false or fraudulent claim

(C) conspires to commit a violation of subparagraph (A), (B), [] or (G), []

(G) knowingly makes, uses, or causes 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 conceals or knowingly and improperly avoids or decreases an obligation to pay or transmit money or property to the Government, []

is liable to the United States Government for a civil penalty of not less than \$5,000 and not more than \$10,000, as adjusted by the Federal Civil Penalties Inflation Adjustment Act of 1990 (28 U.S.C. 2461 note; Public Law 104-410 [1]), plus 3 times the amount of damages which the Government sustains because of the act of that person. 31 U.S.C. § 3729(a)(1)(A), (B), (C), (G).

34. Under the False Claims Act, scienter must be demonstrated:

Definitions—For purposes of this section— (1) the terms “knowing” and “knowingly”— (A) mean that a person, with respect to information— (i) has actual knowledge of the information; (ii) acts in deliberate ignorance of the truth or falsity of the information; or (iii) acts in reckless disregard of the truth or falsity of the information; and (B) require no proof of specific intent to defraud. 31 U.S.C. § 3729(b)(1)-(2).

35. Under section (b)(2) the term “claim ” — (A) means any request or demand, whether under a contract or otherwise, for money or property and whether or not the United States has title to the money or property, that— (i) is presented

to an officer, employee, or agent of the United States; or (ii) is made to a contractor, grantee, or other recipient, if the money or property is to be spent or used on the Government's behalf or to advance a Government program or interest, and if the United States Government— (I) provides or has provided any portion of the money or property requested or demanded; or (II) will reimburse such contractor, grantee, or other recipient for any portion of the money or property which is requested or demanded; []. 31 U.S.C. § 3729(b)(1)-(2).

36. Under the False Claims Act, materiality is defined as “having a natural tendency to influence, or be capable of influencing, the payment or receipt of money or property.” 31 U.S.C. § 3729(b)(4).

III. THE REGULATORY FRAMEWORK

A. Government Contracting Requirements

37. Contracts with the United States for cybersecurity are subject to Federal Acquisition Regulations (“FARs”), agency-specific requirements, including regulations and other standards such as those issued by the National Institute of Standards and Technology (“NIST”)—the federal agency that establishes standards and best practices for several industries—and the Defense Federal Acquisition Regulation Supplement (“DFARS”) for contracts with the U.S. Department of Defense (“DOD”), 252.204-7012 (“DFARS 7012”). Collectively, the government contracting requirements discussed under this Section are alleged

as “Federal Cybersecurity Requirements.”

38. Pursuant to various laws and policies of different agencies, the Government has three primary classification levels for national security information: (1) “Top Secret” – unauthorized disclosure could reasonably cause exceptionally grave damage to national security, (2) “Secret” – unauthorized disclosure could reasonably cause serious damage to national security, and (3) “Confidential” – unauthorized disclosure could reasonably cause damage to national security.

39. “Confidential” information can become “Secret” information if enough fragments of “Confidential” information are combined to provide a description of a process or key equipment. As a result, the Government prioritizes protecting “Confidential” information that, if pieced together by bad actors, could cause serious damage to national security.

40. Examples of “Confidential” information include the strength and condition of the U.S. Military, national security data or intelligence reports, or research and development of processes, equipment, or personnel to enhance national security.

41. Accordingly, even if Government information is not classified as secret, it may still be sensitive enough to require confidentiality. A large volume of unclassified information is also confidential and would harm national security or

the public interest if disclosed to the public. For example, among many others, technical information and specifications related to technologies used for military, space, or intelligence applications, critical energy infrastructure information like the location and design of nuclear reactors and hazardous liquid pipelines, proprietary information collected by agencies from businesses, information pertaining to ongoing law enforcement investigations, and personal information like social security and medical records of citizens and Government employees are all unclassified but highly sensitive.

42. In an acknowledgement of the need to protect information that is intended to be unclassified but non-public, then-President Barack Obama signed an Executive Order that established a category of unclassified-but-non-public information called Controlled Unclassified Information (“CUI”).

43. CUI encompasses a wide range of information, including the examples above, and is defined broadly as information “that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.” The CUI category consolidates various types of sensitive information designated by various federal agencies as exempt from public disclosure under the Freedom of Information Act due to its sensitivity.

32 CFR § 2002.4(h)

44. Relevant here, CUI includes “[c]overed defense information,” which

is defined in U.S. Department of Defense (“DOD”) regulations as (1) “unclassified controlled technical information” or (2) other information “that requires safeguarding or dissemination controls” as described in the National Archives and Records Administration’s Controlled Unclassified Information (CUI) Registry and that is either marked or otherwise identified in the contract as CUI or “[c]ollected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.” 48 C.F.R. § 204.7301.

45. “Controlled technical information” is defined as “technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.” 48 C.F.R. § 252.204-7012 (DFARS 7012)

46. In turn, “technical information” means a wide range of technical data and computer software, including but not limited to “research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.” The terms “computer software” and “technical data” are broadly defined. 48 C.F.R. § 252.227-7013(3) and (15)

47. CUI also includes information marked FOR OFFICIAL USE ONLY (“FOUO”) and NOT RELEASABLE TO FOREIGN NATIONALS (“NOFORN”).

Prior to the creation of the CUI designation in 2010, DOD used the FOUO AND NOFORN designations to identify documents that were protected from public disclosure due to their sensitivity. Thus, DOD used the FOUO and NOFORN designations to mark and protect the same types of information discussed above, which is now marked as CUI instead.

48. As the [REDACTED] explains, “FOUO protection is afforded to information such as the names of [REDACTED] [REDACTED] employees and certain missions and functions,” and FOUO “may also be referred to as controlled unclassified information.”

49. A DOD cybersecurity rule requires all contractors and subcontractors whose computer networks will house CUI during performance of a contract to (1) “provide adequate security” on any such network and (2) immediately report cyber incidents occurring on, or any compromise of, such network to DOD. 78 Fed. 69273 (Nov. 18, 2013).

50. National Institute of Standards and Technology (“NIST”) Special Publication 800-171 (“SP 800-171”) specifically establishes the baseline controls for an adequately secured contractor network housing CUI. These requirements were codified and made applicable to all contracts (the “Adequate Security Rule”). 48 C.F.R. § 204.7302(a)(1) and (b); 48 C.F.R. § 3252.204-7012(b)(2)(i) (DFARS 7012)

51. Under DFAR 252.704-7012, contractors were required to be fully compliant with NIST 800-171 standards as soon as practicable but not later than December 31, 2017. 48 C.F.R. § 3252.204-7012(b)(2)(i) (DFARS 7012)

52. Specifically, the regulations require DFARS 252.704-7012 (safeguarding covered defense information and cyber incident reporting) to be inserted into every contract that involves contractor access to CUI. 48 C.F.R. §§ 204.7300, 204.7304(c), 252.204-7012(b)(2)(i) (DFARS 7012)

53. “Adequate security” is defined as “protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.” 48 C.F.R. § 204.7301

54. Under the “Adequate Security DFARS,” government contractors are required to meet the “adequate security” standard by adhering to basic cybersecurity standards. 48 CFR § 252.704-7012 (DFARS 7012)

55. The NIST Cybersecurity Requirements specifically establish the baseline controls for an adequately secured contractor network housing CUI such as Honeywell, as codified at DFARS 7012. 48 CFR § 252.704-7012 (DFARS 7012)

56. Under the Adequate Security DFARS, contractors were required to be fully compliant with the NIST Cybersecurity Requirements as soon as practicable but not later than December 31, 2017. 48 CFR § 252.204-7012(b)(2)(i)

(DFARS 7012).

57. For all contracts awarded prior to October 1, 2017, the Adequate Security DFARS required the contractor to notify the DOD's Chief Information Officer by email within 30 days of the contract award of any security requirements specified by the NIST Cybersecurity Requirements not implemented at the time of contract award. 48 CFR § 252.204-7012(b)(2)(ii)(A) (DFARS 7012)

58. Additionally, contractors were required to submit any requests to deviate from the NIST Cybersecurity Requirements in writing to the DOD's Chief Information Officer. A contractor was only excused from a security control of the NIST Cybersecurity Requirements 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." 48 CFR § 252.204-7012(b)(2)(ii)(B) (DFARS 7012)

59. Further, the NIST Cybersecurity Requirements have mandated that contractors "rapidly report" directly to the appropriate agency officials any cyber incident. Rapidly report means within 72 hours of discovery of any cyber incident. 48 CFR § 252.204-7012(c)(1)(ii) (DFARS 7012)

60. "Cyber incident" means "actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein." 48 CFR §

252.239-7010 (DFARS 7010)(Cyber incident “means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.”); see also SEC Proposed Rule: Cybersecurity Risk Management, Strategy, Governance, and Incident Disclosure, 17 CFR Parts 229, 232, 239, 240 and 249 at II.D(3)(“What constitutes a “cybersecurity incident” for purposes of our proposal should be construed broadly and may result from any one or more of the following: an accidental exposure of data, a deliberate action or activity to gain unauthorized access to systems or to steal or alter data, or other system compromises or data breaches.”) (March 2022)

61. As codified, the NIST Cybersecurity Requirements established the benchmark for every contractor required to secure a network that houses CUI. 48 C.F.R. § 204.7302(a)(1) and/or 48 C.F.R. § 252.204-7012 (DFARS 7012)

62. The NIST Cybersecurity Requirements are the benchmark against which to measure a contractor’s efforts to secure a network that houses sensitive CUI.

B. Protection of CUI Is Critical to National Security

63. The protection of CUI is critical to national security and the public interest. As the DOD explained, the establishment of CUI was “a watershed moment in the Department’s information security program, formally

acknowledging that certain types of unclassified information are extremely sensitive, valuable to the United States, sought after by strategic competitors and adversaries, and often have legal safeguarding requirements.”

64. The NIST Cybersecurity Requirements are consistent with DOD’s statement, explaining in the abstract that the protection of CUI in contractor (“non-federal”) information systems “is of paramount importance to federal agencies and can directly impact the ability of the federal government to successfully conduct its essential missions and functions.”

65. Recently, the Government’s concern for protecting sensitive information such as CUI against cyber threats has come even more sharply into focus after dozens of cyber attacks in recent years have targeted government agencies, large corporations, and universities around the world. The most prominent of these instances was the SolarWinds Attack described in this Complaint.

66. SolarWinds Inc. (“SolarWinds”) is an American publicly-traded company, headquartered in Austin, Texas, that develops software for commercial and government customers to help manage their networks, systems, and information technology infrastructure.

67. In early 2020, hackers determined by U.S. officials to be affiliated with the Russian government broke into SolarWinds’ systems and implanted

malicious code (or malware) in its “Orion” software, a platform used by tens of thousands of customers to monitor and manage its computer networks. Honeywell used Orion to monitor commercial and government contracts and Orion had high-level permissions on the Honeywell Network that housed CUI.

68. Like most software providers, SolarWinds periodically sends updates of its software programs, including Orion, to customers to fix bugs, improve security, or improve the program’s performance. When SolarWinds sent updates to customers in March 2020, it unwittingly sent updates of Orion that included the malicious code. This embedded code mimicked the language of the Orion software, allowing the malicious code to “hide in plain sight,” and gave hackers a doorway into otherwise secured networks. Throughout this Complaint, this incident is referred to as the “SolarWinds Attack” and the hackers as “the Attackers.”

69. Once inside the customer networks, the SolarWinds Attackers were able to access, steal, alter, and delete customer data and install additional hidden programs, known as “persistence mechanisms,” that allowed the SolarWinds Attackers to keep spying on the networks for months or years without being detected.

70. News of the SolarWinds Attack occurred in December 2020. The victims of this cyber incident numbered as many as 18,000 SolarWinds customers,

including cybersecurity firms, government contractors like Honeywell, Fortune 500 companies, and numerous federal government agencies.

71. The SolarWinds Attack required commercial businesses, government contractors like Honeywell and the Government to deploy their incident response plans and take mitigation steps. To aid in the response, the Cybersecurity and Infrastructure Security Agency (“CISA”) issued emergency alerts and directives to federal agencies, including agencies using third-party service providers (government contractors) regarding the steps that should be taken to mitigate damage and prevent further compromise. As alleged in the Complaint, this is referred to as the “CISA Remediation Plan.”

72. The SolarWinds Attack also deepened the United States’ commitment to enforcing cybersecurity standards and ensuring that government contractors do their part to secure the nation’s sensitive information.

73. On May 12, 2021, President Biden signed an Executive Order called “Improving the Nation’s Cybersecurity,” and declaring that “the prevention, detection, assessment, and remediation of cyber incidents is a top priority and essential to national and economic security.” This statement of policy was supported by his determination that the country “faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people’s security and privacy.” Moreover,

President Biden observed that to secure the nation's sensitive information from compromise, "[t]he private sector must adapt to the continuously changing threat environment, ensure its products are built and operate securely, and partner with the Federal Government to foster a more secure cyberspace. In the end, the trust we place in our digital infrastructure should be proportional to how trustworthy and transparent that infrastructure is, and to the consequences we will incur if that trust is misplaced."

74. The Acting Assistant Attorney General for the Civil Division at DOJ recently explained that "protecting against malicious cyber campaigns is a matter of national concern and a top priority for the [current] Administration." Thus, he further observed, "[w]hen companies that do business with the government knowingly make misrepresentations about their own cybersecurity practices, or when they fail to abide by cybersecurity requirements in their contracts, grants or licenses, the government does not get what it bargained for." And "when false assurances are made to the government, sensitive government information and systems may be put at risk without the government even knowing it." Remarks of Brian Boynton, Acting Assistant Attorney General, Civil Division, U.S. Department of Justice (Oct. 13, 2021), <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

75. On October 6, 2021, the Department of Justice announced a new

enforcement initiative aimed at “cybersecurity related fraud by government contractors and grant recipients.” The intent of the Civil Cyber-Fraud Initiative is to use the False Claims Act to combat cyber fraud that could endanger sensitive Government information such as CUI and “combine the department’s expertise in civil fraud enforcement, government procurement and cybersecurity to promote the critical mission of combating new and emerging cyber-threats.” Press Release, Office of Public Affairs, U.S. Department of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>

76. In sum, the Government has long recognized the importance of securing sensitive government information like CUI, and it requires government contractors to take the appropriate steps to reasonably secure such information from malicious actors as required by the Quantum Contracts and Federal Cybersecurity Requirements.

IV. THE QUANTUM CONTRACTS

77. The Government awarded Honeywell tens of millions of dollars in contracts for services related to Honeywell’s quantum computing technologies. Quantum computers perform higher-speeder calculations than normal computers—they are super computers—which the Government needs for intelligence and law

enforcement. The Government contracted with Honeywell to use its quantum computers to perform highly sophisticated and confidential research and development for new technologies that would help preserve and strengthen our national security.

78. Quantum computers are in their infancy. To overcome challenges, engineers, computer software developers, theorists, and mathematicians perform complex experimentation to identify improved and novel methods of performing quantum operations. Quantum computers are decades away from attaining their most powerful and broad real-world applicability. However, the game-changing effects on military superiority and potential to disrupt global balance of power is well known, and the race is on. In certain cases, the race is quite close. The theoretical applicability of quantum technologies is vast. Preparation for the future state of quantum technologies has begun for most world powers and is well documented around the globe. Within the realm of military and intelligence applications, quantum can and will sharpen capabilities across warfare domains (land, air, space, cyber, under water, and ISR, i.e., intelligence, surveillance and reconnaissance). Capabilities such as precision navigation, ultra-secure communication, artificial intelligence, to name a few, are game changers under development by the United States in preparation for a future state when quantum computers are fully operational and readily available.

79. Much of the discussion around quantum communication revolves around confidentiality. Quantum technologies providing speed and precision, have the potential to revolutionize secure communication. For instance, a quantum computer with a certain speed has the power to break into encrypted channel using today's technology. Much research is taking place to be able to break encryption using quantum computers, as well as the development of "post-quantum encryption" methods, to prepare for an eventual state when these ultra-fast quantum computing poses a threat to secret communications. The ultimate goal in quantum communication is quantum internet, a network of entangled quantum computers connected with ultra-secure quantum communication guaranteed by the fundamental laws of physics. The importance of this technology in counterintelligence (resilience to spying) cannot be overstated.

80. [REDACTED]

[REDACTED]

[REDACTED]. That came as a shock for allies and adversary governments alike, who rely on encryption to maintain secure, confidential communication. These revelations allowed other countries to begin the process of developing countermeasures to U.S. defense technologies and to replicate the technology as a means of leveling the playing field. If hostile nations are allowed to monitor the [REDACTED] [REDACTED] development of these technologies,

subsequently develop countermeasures, and replicate or reverse engineer them, the U.S. may face our own strategic surprise in having our own innovation turned and used against us. What is worse, if the loss of confidentiality remains unknown to the U.S., we become vulnerable to manipulation, sabotage or other kinds of exploitation.

81. The “race” really is quite close in some respects, particularly when it comes to China. Its military-civil fusion strategy would be like Silicon Valley merging with the Pentagon [REDACTED]. Maintaining the U.S. edge in the race really can come down to an individual breakthrough remaining secret. So, when it comes to impact of the loss of confidentiality and the potential theft of information for the quantum contracts, it’s important to understand the extreme sensitivity of the issues alleged in this complaint.

82. Honeywell represented to the Government that it would treat information contained on its network that performed the quantum computing as “highly confidential,” which Honeywell defined as:

[i]nformation that is extremely sensitive and of highest value to Honeywell customers, government partners or individuals and/or which may be subject to protection by law, regulation, or contractual terms. This includes information containing highly sensitive personal data and/or sensitive identification data . . . This information is intended for use only by authorized individuals on a strict need to know basis . . . This information is not generally known or readily accessible, has independent economic value or repercussion due to its secrecy or violation and

therefore requires additional measure to protect its confidentiality.

83. Honeywell has executed numerous contracts with components of DOD, [REDACTED], for quantum computing. Collectively, the Government contracts at issue in this Complaint related to Honeywell's quantum-computing services are alleged as "the Quantum Contracts."

84. In May 2016, DOD awarded [REDACTED] (original award date May 17, 2016) (the [REDACTED] Contract"), an indefinite-length contract for secret services to be performed [REDACTED]. The specific contours of the program are classified, but the [REDACTED] Contract involves Honeywell providing certain electronic network services, including cybersecurity protections, related to its quantum computing technology. DOD subsequently modified the contract on several occasions from 2016 to 2020, but these modifications did not change the applicable cybersecurity requirements.

85. The [REDACTED] Contract explicitly stated that it would require Honeywell to have access to both classified information and CUI. As to CUI, the Contract indicated that the required work would involve "FOR OFFICIAL USE ONLY INFORMATION." As explained, FOR OFFICIAL USE ONLY INFORMATION ("FOUO") is a marking previously used by the DOD [REDACTED] to identify and control the sensitive unclassified information that is now marked as CUI. "CUI legally replaces programs like For Official Use Only (FUOU), Official Use Only,

Sensitive But Unclassified (SBU), and others.”

86. In addition, the [REDACTED] Contract required Honeywell to handle and protect at least two specifically described forms of CUI and to mark them as such.

Attachment B to the [REDACTED] Contract required:

- “Any external view or photographs of end item hardware, when all covers are in place, shall be unclassified, but the information shall be restricted as FOR OFFICIAL USE ONLY. This information will not be published without prior approval of the [contracting officer].”
- “The contractor/subcontractor shall not divulge to any individual, company, organization, or other U.S. Government department or agency any information, classified or unclassified, pertaining to the design or capabilities of COMSEC or communications protection systems or equipment being developed, produced, purchased or provided as government furnished equipment (GFE) under this or any other [REDACTED] contract unless prior [REDACTED] approval is obtained.”

87. Thus, the [REDACTED] Contract put Honeywell on express notice that it would be handling at least two types of Controlled Unclassified Information:

- “external view or photographs of end item hardware, when all

covers are in place”

- unclassified information pertaining to “the design or capabilities of COMSEC or communications protection systems or equipment” being developed, produced, purchased, or provided under the [REDACTED] Contract.

88. And Honeywell acknowledged that Controlled Unclassified Information should be afforded Honeywell’s highest cybersecurity protections as “highly confidential” information.

89. As described, CUI encompasses any materials that are unclassified but still protected from public disclosure due to their sensitivity, and there is no difference between materials marked as FOUO and materials marked as CUI. They are just two different terms used to describe the same materials. Thus, any references to FOUO or unclassified materials protected from public disclosure triggered the cybersecurity protections that must be afforded to CUI.

90. As Honeywell acknowledged, “CUI replaces legacy programs like For Official Use Only (FOUO) Official Use Only, Sensitive But Unclassified (SBU) and others.”

91. On information and belief, the [REDACTED] Contract required Honeywell to ensure the protection of CUI on its electronic network in accordance with all Federal Cybersecurity Requirements to include incorporation of the Adequate

Security DFARS, which is required to be inserted in all contracts involving contractor networks housing CUI.

92. Further, on information and belief, all the Quantum Contracts contained the same or similar requirements for the safeguarding of CUI.

V. THE FRAUDULENT SCHEME

93. Honeywell had the sophistication, experience, technology and expertise to perform on the Quantum Contracts. According to its own public statements:

- it is a “**leader in quantum computing**” with a “complete team of technologists, including atomic, molecular and optical physicists, scientists, engineers, and technicians who specialize in the design and development of trapped-ion quantum computers.”
- “for the past decade, we have been building **technological capabilities** and a **world-class team** to shape how this exciting new industry evolves.”

(emphasis added)

94. Honeywell had a unit called “ACST,” which stood for Advanced Connected Sustainability Technologies. This unit acted as a traditional information technology unit; so, the ACST unit is referred to in this Complaint as the “IT Unit.” The IT Unit administered the Quantum Contracts and was tasked

with performing the following services for Honeywell's Government and commercial business:

- identify counterintelligence and insider security threats
- initiate appropriate countermeasures to threats
- monitor open-source intelligence, supply chain risk, social media platforms, and the dark web for known and potential threats
- investigate alerts of anomalous activity and escalate internal and external threats
- organize, monitor, and investigate personnel security matters

95. Sometime after its first Quantum Contract, Honeywell created a Special Use Network for its work on the Quantum Contracts called the "Gray Network." The Gray Network was used to perform the services under the Quantum Contracts, and Honeywell represented that the Gray Network was created to protect and preserve this highly confidential Government research and development.

96. The Government furnished all its proprietary information and data through the Gray Network to allow Honeywell scientists – with the appropriate security clearances – to process this raw data using quantum computing technology. The scientists performed sophisticated and highly confidential

algorithms and calculations on the Gray Network.

97. Honeywell scientists then shared the output or results with the Government, [REDACTED]

98. The Gray Network housed everything that went into developing advanced technology, to strengthen national security for the Government—the raw data and the quantum computing technology, including the processes by which Honeywell scientists helped the Government develop enhanced technology and security.

99. Honeywell knew that the highly confidential nature of its quantum computing work under the Quantum Contracts on the Gray Network was the foundation for the Government's quantum readiness.

100. Accordingly, Honeywell used SolarWinds' Orion software for its commercial business and government contracts. Orion monitored and had high-level permissions on the Gray Network that housed CUI.

101. Even though it was well-funded under the Quantum Contracts to perform these services, however, Government business played second fiddle to Honeywell's ambitions to grow its quantum computing commercial business. Honeywell raced competitors to publish milestones in development of its quantum computing technologies while disregarding its obligations to the Government.

102. So, when the SolarWinds Attack occurred in early 2020, the Gray Network was a sitting duck for the Attackers. But not so for most of Honeywell's commercial business enterprise. Honeywell brought to bear its incident-response plan for its commercial customers while refusing to leverage the same protection of the Government's CUI on the Gray Network. It consistently gave short shrift to the Government under the Quantum Contracts.

103. In short, Honeywell's pattern and practice alleged in this Complaint deprived the Government of the cybersecurity benefits it bargained for because its cybersecurity measures fell far short of even minimal standards and CUI housed on the Gray Network was placed at risk. Further, when cybersecurity incidents like the SolarWinds Attack exposed its failures to comply with the Quantum Contracts and Federal Cybersecurity Requirements, Honeywell turned a blind eye and knowingly failed to report the cyber incidents to the Government.

104. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

A. Knowing Failure to Comply with Cybersecurity Standards

105. Honeywell knowingly failed to comply with cybersecurity standards

on its Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Such failures were pervasive and systemic, exposing CUI to hackers such as the SolarWinds Attackers.

106. Minimum cybersecurity standards for a network housing CUI, include at least these:

- use of a network firewall (electronic separation from other networks)
- configuration of connected devices with malicious code protection like antivirus software
- access control, including limiting who can access a network & purposes for access of a network, limiting remote access, encryption and automatically terminating sessions after a time
- training and testing personnel on their ability to respond to a cyber incident
- having personnel monitor suspicious network traffic and respond appropriately, including to CISA alerts & advisories
- reporting cyber incidents to the Government involving CUI after the SolarWinds Attack

SP 800-171 §§ 3.1, 3.6, and 3.14 (codified in DFARS 7012)

107. Yet Honeywell failed to meet these minimum cybersecurity

standards in all material respects.

108. These basic, minimum components of network security are required by the Quantum Contracts and the Federal Cybersecurity Requirements and spelled out in the NIST Cybersecurity Requirements. SP 800-171 §§ 3.1, 3.6, and 3.14 (codified in DFARS 7012)

109. Further, the NIST Cybersecurity Requirements provide the template for an adequately secured network with the basic protections and components, and government contractors are expected to be fully conversant with these standards. SP 800-171 §§ 3.1.1 through 3.1.3, 3.1.11 through 3.1.15 (codified in DFARS 7012)

110. Honeywell knew that it was required to comply with the NIST Cybersecurity Requirements as shown by its written security plan to include processes and procedures that it represented were “firmly in place.”

111. Honeywell understood the significance to the Government of a strong cybersecurity program, and it represented itself to be a **“leader in quantum computing”** with a **“world class team”** of “technologists, including atomic, molecular and optical physicists, scientists, engineers, and technicians who specialize in the design and development of trapped-ion quantum computers,” which it deployed for its commercial business. (emphasis added)

112. While Honeywell created the Gray Network to segregate information

it designated as “highly confidential” and IT staff to oversee the Gray Network, it failed to provide the necessary cybersecurity protections for the Gray Network, despite knowing that such protections were required by the Quantum Contracts.

113. Honeywell turned a blind eye to its obligations under the Quantum Contracts and instead dedicated its collective efforts to manage and grow its commercial business (namely, its quantum startup business) to the detriment of the Government’s cybersecurity needs. As a result, Honeywell consistently failed to comply with the Quantum Contracts and Federal Cybersecurity Requirements.

114. These Government requirements became paramount when Honeywell became a target of numerous attacks, including attacks from the dark web and the SolarWinds Attack, and Honeywell’s noncompliance was material.

115. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

116. Honeywell’s knowing violations deprived the Government of what it bargained for. As DOJ has pronounced, “the False Claims Act is a natural fit to pursue knowing failures to comply with cybersecurity standards.”

<https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

1. The Firewall Was a Smokescreen

117. Honeywell's use of a firewall was a smokescreen to hide its inadequate security practices on the Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Having such inadequate security exposed CUI to hackers such as the SolarWinds Attackers. Further, Honeywell understood the significance of needing more than a basic firewall for a legitimate cybersecurity program because it had a "world class" team that it deployed for its commercial quantum business.

118. Honeywell hosted a Special Use Network for CUI known within Honeywell as the "Gray Network."

119. The types of CUI the Gray Network handled and stored included:

- highly confidential information proprietary to [REDACTED] agencies, including details, drawings, specifications, testing, and simulation of cutting-edge, state-of-the-art quantum computing programs that no other country possesses, and which can be used in secret intelligence programs
- technical information and specifications related to technologies used for military, space, or intelligence applications, and personal information about Government employees involved in the Quantum Contracts, which are highly sensitive

- multiple databases containing three-dimensional engineering diagrams and technical component specifications
- technical data, research and computer software, including processes, standards, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code

120. Honeywell scientists, for example, used the Gray Network to perform modeling and simulation of technology of top-secret programs developed under the Quantum Contracts. The Gray Network also contained other sensitive information such as the names of Honeywell scientists with top security clearance working on these secretive technologies.

121. The Gray Network was segmented from (“walled off from”) the broader Honeywell corporate networks and the Internet by a firewall. A firewall is a security device that blocks unauthorized users from connecting to a network. It sifts through both incoming and outgoing traffic, either blocking it completely or filtering it through certain access points that allow for heightened monitoring and investigation.

122. While important to protect CUI from exposure, a firewall is only one component of an adequate cybersecurity program. Firewalls are intended to supplement other necessary safeguards to secure a network from unauthorized

access, not perform that function in isolation.

123. From the start of the earliest Quantum Contract, Honeywell was overly reliant on its firewall to protect the Gray Network.

124. The Gray Network's firewall was only a programmable separation from outside connections or traffic—and not an airgapped network, as described below. Most Gray Network users and devices could still access the internet while connected to the Gray Network, even if the firewall somewhat limited that access. Further, the lack of policy and enforcement of acceptable use practices allowed devices intended for the Gray Network to be taken home where the device was out of reach of the firewall. In the absence of other safeguards to complement the firewall, Honeywell's firewall was useless as security protection.

125. A firewall is only an **electronic** (and not a physical) separation from other networks and malware could still have infected the Gray Network. Air gapping is a practice used in the cybersecurity industry. Air gapping describes a secured network that is **physically** separated from outside connections—meaning that it is not wired into the Internet or other networks capable of being accessed wirelessly. Thus, the only way data can be added to or taken from an air gapped network is through removable hardware or media like a USB drive, and other devices like laptops can connect to the network only with very specific permissions. Even if the Gray Network had been airgapped, allowing users to take

home laptops and re-introduce them to the lab environment defeated firewall protections entirely.

126. Indeed, Honeywell knew that its firewall did not limit “ALL software” from reaching the Gray Network and knew that this was a material limitation, as shown by dialogue internal to Honeywell after the SolarWinds Attack:

Given this entire scenario [SolarWinds], it seems as a general security posture that our best bet would be to always limit ALL software from reaching out past the firewall (and where it must, be extremely controlled) . . . From DarkTrace guidance: . . . The threat-actor set the hostnames on their command and control infrastructure to match a legitimate hostname found within the victim’s environment. This allowed the adversary to blend into the environment, avoid suspicion, and evade detection.

127. Further, Honeywell knew or should have known that its firewall was insufficient even before the SolarWinds Attack.

128. Because Honeywell knowingly failed to implement adequate measures to secure the Gray Network, the implementation of a firewall was used as a smokescreen by IT Unit Management to brush aside concerns about the Gray Network’s inadequate security.

129. Worse, creating a firewall between the Gray Network and Honeywell’s corporate network further decreased protections for CUI because the Honeywell corporate network had basic cybersecurity safeguards that the Gray

Network did not.

130. On information and belief, Honeywell knowingly failed to put in place the necessary security protections from the start of its first Quantum Contract, placing the Government's sensitive information at risk from the get-go. And this was by choice because Honeywell had the capability to provide the necessary security. But it chose to instead commit its money, resources and human capital to its quantum commercial business to support its ambitions to grow this sector.

131. After the Government awarded Honeywell its first Quantum Contract, commercial demand for Honeywell's quantum computing services grew steadily and substantially. This resulted in Honeywell devoting more resources and attention to its commercial business while continuing to give short shrift to its obligations to the Government. This pattern or practice included Honeywell bypassing or disabling safeguards required to protect Government information on the Gray Network to give unrestricted access to employees handling commercial business.

132. Because of its disproportionate commitment to its commercial interests, Honeywell diverted the resources and human capital its IT Unit needed to properly monitor and secure the Gray Network to its separate commercial operations, and the already serious deficiencies in the Gray Network's security

grew more numerous.

133. Prior to the establishment of even this untested process, Honeywell had “not a lot of procedures for a lot of things” on the Gray Network.

2. Inadequate Malicious Code Protection

134. Honeywell knowingly failed to implement adequate malicious code protection throughout the Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Having inadequate malicious code protection on critical Gray Network assets exposed CUI to hackers such as the SolarWinds Attackers. Further, Honeywell understood the significance of malicious code protection because it had this protection for corporate network assets.

135. Protection against malicious code is the cornerstone of any cybersecurity program because malicious code is the tool that allows hackers to break into and compromise a network. Broadly speaking, malicious code is any type of unwanted file or program used to harm a computer or network, compromise data stored on a computer or network, or give unauthorized persons access to or control over a computer or network.

136. There are various types of malicious code, including, for example:

- viruses (code designed to damage or destroy files and spread through various means)

- worms (code designed to freeze up a computer or network by using up all its resources)
- trojan horses (code that disguises itself so it can reside on a computer or network without being detected and continue to exploit the computer or network for unauthorized purposes (such as spying or data theft))

137. The malicious code used in Orion in the SolarWinds Attack was a form of trojan horse code, also known as a back door.

138. Lack of adequate malicious code protection on computers connected to a network exposes the network to malicious code, which allows hackers to access and extract information from it. This is akin to a consumer connecting to the Internet with a personal computer with no antivirus software—except most consumers are not the targets of sophisticated state-backed hackers dedicated to stealing confidential Government information. American consumers understand the importance of protecting their personal computer with antivirus software to avoid Internet hackers from accessing their personal information.

139. Many readily available programs can be used to detect and thwart malicious code. These include popular antivirus software programs like those used by consumers on personal computers. Although these programs are not totally foolproof, they detect the vast majority of malicious code in use today, and their

developers constantly update them to catch new forms of malicious code as they come to light. Thus, installing common antivirus software on the devices that connect to the network is an easy, inexpensive, and truly rudimentary step that any competent company seeking to protect its sensitive information could and would take.

140. Yet Honeywell was so deficient in protecting the Gray Network from malicious code that it did not even take adequate steps that the average consumer would take to protect their household computer.

141. For years, Honeywell allowed employees working on the Quantum Contracts to purchase new off-the-shelf computers and connect them to the Gray Network without even basic antivirus protection installed to detect or combat malicious code. Basic network security in this area does not require much; the antivirus software available to and used by millions of consumers is the baseline. But Honeywell failed to ensure that its employees took this basic security measure.

142. Honeywell required malicious code protection for domain-joined and stand-alone and remotely connected personal computers to the Gray Network only after the SolarWinds Attack and, even then its protections remained inadequate. For example, on information and belief, these late-created protections were not monitored or enforced because Honeywell was unable to even identify all the personal computers that were joined to the Gray Network:

As you know, we had compromised SolarWinds DLL's [dynamic link library's] [Microsoft's implementation of the shared library concept] installed in our environment. While we haven't found any concrete evidence of exploitation, we are taking every precautionary step we can. One of the quickest and easiest remediation steps is to download the newest mpam files of Windows Defender, install it, and do a complete scan of the system. Windows Defender will search for and quarantine any located nefarious files and processes related to this security breach. Kevin has already setup a push through all domain joined systems to perform this task on domain joined workstations and servers, so we've already covered much of the environment.

Dan, what I need you to do:

- (1) Domain join any remaining stand-alone PC's (if any), on the gray network and instruct the users

(emphasis added)

143. This failure to ensure that malicious code protection was installed on all the computers that connected to the Gray Network created a gaping hole in the Gray Network's security. As Honeywell IT specialists acknowledged: "the only 'AV' [audiovisual] on the Gray network is MS defender and it was previously only deployed to workstations and not servers."

144. These unprotected devices each could serve as a gateway for malicious code to embed itself in the Gray Network, infect or extract CUI, and transfer it off the Network into the possession of criminal or state-backed hackers like the SolarWinds Attackers.

145. Honeywell knew for years that its employees' ad hoc choices when

using devices connected to the Gray Network created these security lapses, but Honeywell never put a stop to it. As one Honeywell IT specialist acknowledged:

“I am aware of a few off domain PCs that are not domain joined, and I can work on getting them added or scanned. But I think we might need a better list. Perhaps a communication requesting users list any off domain or non-blue network computer might be a start to track all of these down?”

146. In response to this request, one IT Unit Manager acknowledged that this basic step should be performed:

In order to locate and verify those systems, you will need to be on-site and manually check PCs wherever found, **especially in the labs to verify their on/off domain status and join them for management.** . .

(emphasis added)

147. Instead of taking this basic step to protect the Gray Network from the infection of malicious code, Honeywell prioritized the growth of its quantum startup business, dedicating its resources and human capital to those efforts and leaving the Gray Network so low on the priority chain that it made a choice to not put controls in place to make sure that malicious code protection was installed and running on all the devices connected to the Gray Network.

148. Further, in response to the SolarWinds Attack, Honeywell employees overseeing the Gray Network also failed to take the basic step of identifying and removing “persistence mechanisms.” Persistence mechanisms are tools and

methods hackers like the SolarWinds Attackers used to gain access to the victim's environment to set up persistence using specific techniques, as outlined by CISA immediately following the discovery of the SolarWinds Attack. The persistence mechanisms allowed the adversary to maintain illicit access to the environment to finish the job, even after defenders discovered the initial point of entry and closed it.

149. As discussed again later in this Complaint, Honeywell never addressed the suspicious activity resembling SolarWinds persistence mechanisms on the Gray Network, but instead simply disconnected the Orion software from the Network.

150. Given the sophistication of the SolarWinds Attackers, disconnecting Orion from the Gray Network was only the first step in a series called for by the Federal Cybersecurity Requirements to eliminate the continued threat.

151. After the SolarWinds Attack in early 2020, the continuing risk to the Gray Network throughout 2020 from Honeywell's lack of malicious code protection was realized at least twice.

152. In the first incident, on December 14, 2020—one day after the Government notified the public about the SolarWinds Attack—Honeywell staff from the Gray Network's IT Unit "pinged" the domain called "avsvmcloud.com," which (a) served as the command-and-control center for the SolarWinds Attackers

and (b) communicated with the Orion software containing the malicious code.

This serious error further demonstrates Honeywell's failure to properly secure the Gray Network.

153. In the second incident, on December 14, 2020, another Honeywell employee in the IT Unit downloaded several electronic SolarWinds files that contained the malicious code behind SolarWinds. While the purpose of the exercise was innocent—to determine the precise time when malicious code had first been introduced to the Gray Network by comparing updated SolarWinds files with earlier SolarWinds files—Honeywell failed to follow well-accepted cybersecurity investigative protocol and placed the Gray Network at further risk.

154. Instead, one appropriate tool to perform this comparison would have been a “sandbox,” a computer program commonly used by researchers and practitioners to securely download and run code. The purpose of a sandbox is to observe the behaviors of the malware, while keeping it quarantined and unable to spread. However, the IT Unit employee downloaded the updated SolarWinds files directly onto his computer, which he used often to connect to the Gray Network, thereby putting CUI at further risk.

155. Further, despite clear evidence of continued suspicious activity even after the SolarWinds server was shut down, Honeywell's internal repeated refrain was that there was no evidence of further activity from the server or evidence of

compromise, and thus no further remediation was necessary:

We have in fact confirmed this system [the Gray Network] has the compromised DLL's present, and we have confirmed there have been no attempts to reach any of the internet sites. We have already undertaken analysis and remediation efforts (so far, other than shutting the system down, no suspect DLL's have been found).

156. However, this was false and misleading. Continued activity, including high volume data transfers (over 1,200 megabytes of data) from the core of the Gray Network (the privileged administrative server or "Gray Network Central Server") to the compromised SolarWinds Orion server (the server that the Solar Winds Attackers had assumed control of and used to infiltrate networks like Honeywell networks) raised red flags. These red flags required investigation, definitive understanding of the threat, and remediation:

- "How can we know this is not the result [of] a compromised account?"
- "Why was there continued traffic to the server if it had been powered off?"

157. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

3. Inadequate Access Control

158. Honeywell knowingly allowed unrestricted and unmonitored access to sensitive Government information within the Gray Network in at least several important respects in violation of the Quantum Contracts and Federal Cybersecurity Requirements:

- Control Over Users
- Remote Access Point Control
- Encryption
- Automatic Session Termination

159. Allowing such unrestricted and unmonitored access to the Gray Network exposed Controlled Unclassified Information to individuals like (or worse than) the SolarWinds Attackers.

a. Control Over Users

160. Honeywell knowingly failed to limit users who had access to the Gray Network or limit the purposes for use of the Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Having inadequate limitations on use of its Gray Network exposed CUI to hackers such as the SolarWinds Attackers. Further, Honeywell understood the significance of implementing a policy limiting users and uses because it implemented one for its

commercial customers on its corporate network.

161. The first basic step toward controlling access to a network are established policies limiting:

- users who have access: “control [of] access between active entities or subjects (i.e., **users or processes acting on behalf of users**) and passive entities or objects (e.g., **devices, files, records, and domains**) in systems”
- the purposes for which users have access: “[l]imit[s for] system access to the **types of transactions and functions** that authorized users are permitted to execute”

(emphasis added)

162. Honeywell failed to meet minimum requirements regarding access control within the Gray Network, i.e., limiting authorization to Gray Network assets and identifying the purposes (types of transactions and functions) for which authorized individuals were allowed to access them.

163. Honeywell routinely allowed employees to access the Gray Network without approval and without tracking who was accessing the Gray Network or the purpose for which they were accessing it.

164. Further, Honeywell employees who worked exclusively on matters for commercial customers and were not authorized to work on the Quantum

Contracts routinely accessed the Gray Network. Honeywell failed to track their access, or their actions on the Gray Network once they had access, or even their identities. In short, Honeywell allowed free rein access to the Gray Network.

165. As shown, Honeywell lulled the Government into believing the Gray Network was created as a distinct network segment to protect Government work on the Quantum Contracts when, in fact, Honeywell allowed unauthorized access to the Gray Network, including for commercial business, introducing risks that Honeywell was not tracking much less able to assess.

166. After the SolarWinds Attack, suspicious activity was detected on the Gray Network. However, the IT Unit was unable to identify the users with access to the Gray Network, the users who in fact accessed CUI on the Gray Network, or the reasons users may have accessed CUI. Because of these failures, Honeywell was unable to properly investigate suspicious activity on the Gray Network after the SolarWinds Attack: it could not attribute activity to known users and could not evaluate whether suspicious activity was performed for a legitimate purpose.

167. Further, in response to the SolarWinds Attack, the CISA Remediation Plan directed that any electronic accounts that could be used to exploit the vulnerability in Orion should be located, identified and removed.

168. However, Honeywell failed to take any steps to remove unauthorized accounts on the Gray Network. Instead, IT Unit Management shut down its

SolarWinds investigation before ever reviewing the activity on the Gray Network. An investigation would have exposed Honeywell's blatant cybersecurity violations relating to the Gray Network and would have been futile because of these very violations.

169. On information and belief, Honeywell knowingly failed to report these cyber incidents to the Government.

170. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

b. Remote Access Point Control

171. On information and belief, Honeywell knowingly failed to implement adequate remote access point or endpoint control on its Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Having inadequate remote access point control on its Gray Network exposed CUI to hackers such as the SolarWinds Attackers. Further, Honeywell understood the significance of securing network endpoints because it secured network endpoints on its corporate network.

172. In a computer network, an access point (or endpoint) is the device that allows wireless devices to connect with each other. On the Gray Network,

these network entry and exit points include routers, remote access servers, and the Gray Network firewall. The basic security standard is to “[i]mplement ... malicious code protection mechanisms at system entry and exit points to detect and eradicate malicious code.” SP 800-171 § 3.14.2 (codified in DFARS 7012)

173. Access points are the critical places along a network where hackers like the SolarWinds Attackers can try to break in. A helpful analogy is the front door of a government building—because it is the way in, it should have metal detectors installed to scan for dangerous objects being snuck in or government property being smuggled out. Code scanning and malicious code protection at entry and exit points are the metal detectors on a network.

174. System endpoints can be protected against malicious code through use of an endpoint protection platform (EPP). An EPP works by examining electronic files as they enter and leave the network to identify suspect code. There are many commercially available EPPs, and they are used on countless networks throughout the world.

175. During its administration of the Quantum Contracts, Honeywell used EPPs including CrowdStrike Falcon and Microsoft Defender for commercial customers.

176. Honeywell turned a blind eye to its contractual obligations to the Government to dedicate its collective efforts to manage and grow its commercial

business to the detriment of the Government's cybersecurity needs. As a result, Honeywell consistently failed to comply with the Quantum Contracts and Federal Cybersecurity Requirements.

177. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

c. Remote Access Limitations

178. Honeywell knowingly failed to limit remote access usage and protocols within the Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Remote access is logging into a network from an off-site computer or device through the Internet. Yet Honeywell understood the significance of placing limitations on remote access because it had such limitations on its corporate network for commercial business.

179. The failure to place limitations on remote access within its Gray Network exposed CUI to hackers such as the SolarWinds Attackers who can easily break into the network by a number of means, even where computers directly connected to the network are secured.

180. Like its allowance of unrestricted users and uses for the Gray Network, Honeywell's remote-access policy for the Gray Network was "anything

goes.”

181. Honeywell failed to ensure that remote access may be achieved only through designated, safe network access control points. A network has multiple access points such as remote access, but for more restricted access, the network administrator can configure it such that all remote-access traffic is routed through specific access points, which the administrator can monitor and control to prevent unauthorized access or exporting of sensitive data like CUI.

182. For example, a network administrator could choose to configure only one or two physically connected computers to allow users to login to them remotely for access to the network. That way, the administrator could augment those one or two computers with special software and other enhanced security safeguards. This is comparable to a school or government building locking all the doors to the building except doors that have metal detectors or security checkpoints installed behind them.

183. But Honeywell simply unlocked the whole building by using a peer-to-peer remote access protocol that essentially allowed connection to the Gray Network through any access point along the Gray Network. The confusion and inability to identify the source of this traffic resulted from the Microsoft Remote Desktop protocol, which allowed connections through any access point. As a result of this lack of remote access control, Honeywell was unable to differentiate

legitimate from illicit access to the Gray Network after the SolarWinds Attack, which made it difficult to determine whether the Gray Network had been breached.

184. On information and belief, Honeywell knowingly failed to report these cyber incidents to the Government.

185. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

d. Encryption

186. Honeywell knowingly failed to require encryption on its Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Not requiring encryption on its Gray Network exposed CUI to hackers such as the SolarWinds Attackers because it compounded the other failures. Further, Honeywell understood the significance of encryption for the “highly confidential” information stored on the Gray Network because it required encryption on its corporate network for highly confidential information of its commercial customers.

187. On information and belief, Honeywell knowingly failed to control remote access by the most rudimentary method through encryption of inbound and outbound traffic on the Gray Network. Due to the allowance of tunneling protocol

within the Gray Network, users and attackers alike were able to circumvent or defeat fundamental safeguards, like encryption standards and basic firewall rules. Tunneling occurs when a user “wraps” (encapsulates) one form of communication inside another. This practice is risky for organizations because it allows the individual to perform actions which would normally be flagged as anomalous (suspicious) or blocked. On the Gray Network, tunneling protocol was not even vetted, tracked, or monitored in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Researchers published observations of threat actors using this technique for lateral movement, maintaining persistence, and to access network segments (like the Gray Network) reachable through only an administrative jump box (like the one used for the Gray Network). Further, the SolarWinds Attackers used a tool specifically designed for such a technique. Put simply, tunneling should not have been used on the Gray Network because of the sensitivity of information residing there.

188. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

e. Automatic Session Termination

189. Honeywell knowingly failed to implement automatic session

termination on its Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Having no automatic session termination on its Gray Network exposed CUI to hackers such as the SolarWinds Attackers because it compounded the other failures. Further, Honeywell understood the significance of automatic session termination because it required this feature on its corporate network.

190. Another basic protection to prevent unauthorized access to a network is timed sessions. When a user is logged into a network for a long period but appears inactive, the session is expected to automatically terminate or “time out.” Timed sessions serve several security purposes such as preventing hackers such as the SolarWinds Attackers from staying on the network for long periods of time while appearing inactive to tracking software, and while secretly harvesting and exporting stolen information. SP 800-171 § 3.1.11 (codified in DFARS 7012) (providing for safeguards that “[t]erminate (automatically) a user session after a defined condition”)

191. Having no automatic session termination made it difficult or impossible for the IT Unit to discover a cyber incident such as the SolarWinds Attack because users and services could access the Gray Network and remain on it for long periods of time without being detected.

192. Indeed, after the SolarWinds Attack, the IT Unit encountered

suspicious sessions that showed that the Gray Network Central Server was making high volume data transfers (over 1,200 megabytes of data) to the compromised SolarWinds Orion server. When IT Unit employees sought an explanation and investigation, the IT Unit Management improperly shrugged off the suspicious activity as a harmless “hung session” (i.e., instance of long inactivity”) even though the duration of one session was over 3 hours. Because of Honeywell’s failure to implement automatic session termination, these data transfers were enabled without interruption.

193. On information and belief, Honeywell knowingly failed to report these cyber incidents to the Government.

194. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

4. Inadequate Incident Testing & Response

195. Honeywell knowingly failed to test its IT Unit’s incident response capability of the Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Providing no testing of its incident response exposed CUI to hackers such as the SolarWinds Attackers. Further, Honeywell understood the significance of incident response testing because it required this practice for its

corporate network.

196. Testing of its incident response capability is crucial to evaluating an organization's ability to confront suspicious cyber incidents. Typically, testing is conducted through exercises that simulate a security incident and evaluate personnel's response to it. Naturally, any such exercises would require a playbook or incident response plan against which performance is evaluated. SP 800-171 §§ 3.6.3 (codified in DFARS 7012)

197. However, Honeywell performed no such testing of the Gray Network and conducted no exercises.

198. As a result, Honeywell's Gray Network was a "sitting duck" for a cybersecurity attack like SolarWinds, and the IT Unit staff were wholly unprepared and unable to handle this serious incident.

199. Worse than its unpreparedness, Honeywell knowingly failed to perform a root cause analysis of, or follow up on, suspicious activity on the Gray Network after the Attack; and, improperly dismissed alerts of suspicious activity and threat intelligence research and analysis showing commonalities between known SolarWinds threat actor techniques and the suspicious traffic, i.e., traffic spoofing the Orion software.

200. This suspicious activity was significant, representing a transfer of over 1,200 megabytes of data from the Gray Network Central Server to the

compromised SolarWinds Orion server; further, the transfers took place after the Orion server was shut down, which is indicative of traffic spoofing to mimic Orion.

201. On information and belief, Honeywell knowingly failed to report these cyber incidents to the Government. Yet in the absence of a Honeywell investigation or disclosure to the Government, it is unknown whether the SolarWinds Attackers are privy to the Government's secrets on the Gray Network.

202. By contrast, Honeywell immediately followed up on similar suspicious activity related to its commercial business after the SolarWinds Attack. In doing so, Honeywell became aware that suspicious activity on the Gray Network preceded the SolarWinds Attack by at least several months:

While investigating the [SolarWinds] incident. We have found DNS [Domain Name System] logs towards suspicious domain shared by advisory ("avsmcloud[.]com")[SolarWinds Attackers' domain] on June'20 to July'20. We were unable to identify the actual host from the logs . . . I am attaching the sample DNS logs, could you please help us identify the actual host behind this traffic so we can take the necessary remediation steps.

203. However, Honeywell knowingly failed to conduct meaningful incident response of the Gray Network. More troubling, despite knowing that malicious DLL (Microsoft version of shared libraries) was introduced to the Gray Network and remained on the Gray Network in its "trojan horse" form, Honeywell

conducted no meaningful incident response. Failure to take these basic cybersecurity steps violated the Quantum Contracts and Federal Cybersecurity Requirements.

204. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

5. Inadequate Oversight of Suspicious Activity

205. Honeywell knowingly failed to provide adequate human monitoring and response of suspicious network activity on its Gray Network in violation of the Quantum Contracts and Federal Cybersecurity Requirements. Having inadequate human oversight of suspicious activity of its Gray Network exposed CUI to hackers such as the SolarWinds Attackers. Further, Honeywell understood the significance of human oversight of suspicious activity because it required this practice on its corporate network.

206. Suspicious network traffic, most often identified by software programmed to look for signs of anomalous or malicious behavior on the network, can indicate that unauthorized persons have accessed, or attempted to access, a network. When monitoring software alerts for suspicious activity, it is crucial for trained personnel to rapidly review and investigate the incident and, where

necessary, begin mitigation and remediation.

207. Honeywell used network monitoring software (Darktrace and the Palo Alto Network Firewall) that generated security alerts for suspicious network activity on the Gray Network, but as evidenced by its failure to follow up on suspicious network traffic in the wake of SolarWinds, Honeywell did not assign trained and qualified personnel to follow up on these alerts

208. When employees raised concerns about Honeywell's failure to investigate and respond to suspicious activity on the Gray Network, Management response in the IT Unit was to brush aside these concerns by pointing to the fact that monitoring software was being used.

209. The one Honeywell IT Unit employee with prior cybersecurity experience pointed out that these Darktrace alerts required basic follow-up as required by CISA:

In the interest of evaluating network activity for signs of persistence/compromise beyond Point of Entry (SolarWinds), this is the simplest and most basic due diligence. Please ensure these connections and data transfers line up with normal business operations. . . . **It is recommended by CISA, FBI, and private sector entities – to identify all threat actor-controlled accounts and persistence mechanisms – using endpoint, network, event logs and system logs. This is one small portion of that due diligence.**

(emphasis added)

210. Yet a Honeywell Manager responded: “Looking at these logs, I don’t see a lot of information. . . . In any case, I don’t see anything concerning based on the available evidence.” When presented with troubling evidence of suspicious activity, Management refused to acknowledge the serious nature of incidents or take action to remediate.

211. Compounding Management’s knowing failure to respond, monitoring software is only an early warning system that allows detection but not response. There was simply no “set it and forget it” option, because even the most sophisticated network monitoring software is limited to identifying suspicious behavior on the network. Without the deployment of dedicated and trained cybersecurity professionals to act on these alerts, the alerts themselves are useless. And Honeywell did not attempt to address this glaring security weakness. . . . Honeywell failed to deploy an intrusion protection system—special software capable of automatic response to anomalous activity—on the Gray Network.

212. A useful comparison is security alerts on a consumer’s personal computer: if an antivirus program sends a security alert to the consumer, that alert is useless unless the consumer reviews the alert and takes the recommended steps to safeguard against the threat. In the network-security context, this is more complicated because the person reviewing the alerts must be trained to know the specific (and sometimes highly technical) steps that must be taken to rectify the

problem. But the principle is the same: a person must follow up when the software sends an alert.

213. Moreover, even if personnel in the IT Unit had been reviewing alerts generated by the software, no one within the Unit was trained on how to properly investigate or respond to them and Honeywell failed to test its IT Unit's incident response capability in violation of federal requirements and the Quantum Contracts. When such incidents occur, decisions must be made quickly, and a series of specific steps must be taken to contain the threat. Honeywell never trained or tested its personnel in charge of administering the Gray Network to respond to cybersecurity incidents.

214. Instead, Honeywell turned a blind eye to its contractual obligations to the Government to dedicate its collective efforts to manage and grow its commercial business. Even though it was well-funded under the Quantum Contracts to perform these services, Government business played second fiddle to Honeywell's ambitions to grow its quantum computing commercial business.

215. Honeywell knew this basic tenet of network security because it had a team of personnel, the Security Operations Center, dedicated specifically to monitoring, investigating, and responding to suspicious network traffic on the corporate network for its commercial customers.

216. Yet Honeywell did not address suspicious incidents on the Gray

Network. Because Honeywell's Gray Network was segmented from its corporate network as a Special Use Network, its Security Operation Center personnel had no access to, and could not monitor or investigate, traffic on the Gray Network.

217. Honeywell also ignored cybersecurity alerts and advisories by CISA even though one of the most fundamental steps for the owner of a network and certainly for Honeywell as a government contractor to ensure its network is to act on cybersecurity alerts and advisories issued by CISA.

218. Even though the Gray Network contained CUI, Honeywell had no mechanism for reviewing or addressing CISA alerts and advisories and made no effort to create one.

219. In response to the SolarWinds Attack, CISA issued a Remediation Plan to include critical information regarding how the malicious code operated, its origination and steps to neutralize it and instructions to disconnect networks such as the Gray Network from all traffic to and from external connections using Orion.

220. Yet, personnel in Honeywell's IT Unit were provided no instructions to follow the CISA Remediation Plan, thereby leaving the Gray Network exposed to the SolarWinds Attackers.

221. On December 14, 2020, the day that Honeywell disconnected Orion from the Gray Network in response to the SolarWinds Attack, Honeywell's monitoring software sent a series of alerts indicating (a) malware had been used to

infiltrate and install programs on the Gray Network to intercept or extract information, and (b) instances of anomalous remote access from unknown sources to systems on the Gray Network that handle CUI. The incidents occurred between 9:30 a.m. and midnight Central Time.

222. The first incident occurred on December 14, 2020, at 9:30 a.m. CST. Orion initiated a connection with the device of a Honeywell employee working on the Quantum Contracts to issue a “service update.” However, following the connection, the activity performed triggered security alerts from security software set up to monitor the Gray Network.

223. Once the remote Orion connection to the Honeywell employee’s device was established, the device’s configuration was modified.

224. The IT Unit’s monitoring software vendor identified this configuration change as consistent with the pattern of activity used by the SolarWinds Attackers to gain access into networks and infect more devices; the monitoring software strongly signaled that the Attackers had gained access to the Gray Network. The vendor recommended steps to investigate and validate the potential breach. Further, Honeywell’s IT Unit concluded that (a) an originator other than Honeywell personnel did in fact install software files on the device connected to the Gray Network and (b) no one from the Unit initiated an Orion service update.

225. These facts were strong indicators to suggest that the SolarWinds Attackers gained access to the Gray Network.

226. Also sounding the alarm bell, during each of the incidents:

- the “traffic” (i.e., data moving across a computer network) passing between the “Gray Network Central Server” and the compromised SolarWinds Orion server was an unusually high volume (over 1,200 megabytes of data)
- these remote sessions had the same Internet Protocol (IP) address (i.e., the numerical label assigned to each device) as Orion’s IP, only the traffic continued after the SolarWinds Orion server was shut down
- the Gray Network administrators who had access to the “Gray Network Central Server” were not able to identify who was conducting these suspicious remote sessions
- the last session ended around midnight when no one at Honeywell was working on the Gray Network
- the traffic appeared to have originated from the compromised SolarWinds Orion server, which Honeywell had already disconnected from the Gray Network

227. These facts were strong indicators that the SolarWinds Attackers

were continuing to access the Gray Network even after Honeywell disconnected from the Orion network.

228. The IT Unit Manager dismissed all these serious indicators because he determined there was no further activity. However, even if there were “no further activity,” that factor alone was not determinative of whether the SolarWinds Attackers had infiltrated the Gray Network with such compelling facts to the contrary.

229. Further, closing the matter without further investigation left the Gray Network vulnerable to the SolarWinds Attackers. As the Honeywell IT Manager stated: “Looking at these logs, I don’t see a lot of information. . . . In any case, I don’t see anything concerning based on the available evidence.”

230. Yet Honeywell closed the matter of the SolarWinds Attack of the Gray Network at the direction of the IT Unit Chief Security Officer with no further internal investigation and without implementing necessary CISA Remediation Steps.

231. While Management within the IT Unit properly disconnected the server containing Orion from the Gray Network, it failed to take the next important step under the CISA Remediation Plan to block all network traffic to and from external connections containing any version of Orion, not just the version known to be exploited. CISA described the reason:

Operating even version 2020.2.1 HF2 of the SolarWinds Orion platform may still carry some risk. The adversary enjoyed longstanding, covert access to the build process that SolarWinds uses for Orion, including to the code underlying the Orion platform. While the immediate known consequence of this access was the insertion of the malicious code into the affected versions of SolarWinds Orion, there may be other unknown consequences as well. The adversary can be presumed to be familiar with at least some aspects of the SolarWinds development and coding practices, as well as the SolarWinds Orion code itself (CISA is unable to assess the level of access the adversary may have had to other SolarWinds [non-Orion] code). Consequently, it is likely that the adversary is in a strong position to identify any potential (and as yet unknown) vulnerabilities in the SolarWinds Orion code that are unrelated to the inserted malicious code and may therefore survive its removal. This adversary has demonstrated the capability and willingness to exploit SolarWinds Orion to compromise U.S. government agencies, critical infrastructure entities, and private organizations.

(emphasis added).

232. To avoid inconvenience to its commercial business caused by a temporary disruption in service, Honeywell failed to mitigate, disregarding the CISA Remediation Plan and leaving the Gray Network at risk of the malicious code in the Orion software.

233. The IT Unit's failure to block all network traffic to and from external connections where any version of Orion was installed undermined any protections that such separation would have provided. In turn, many users—including those who were on networks that were still running the Orion endpoint agent—continued

to login to the Gray Network from home or other remote locations. This made the Gray Network vulnerable to the SolarWinds Attackers because of the malevolent code embedded in Orion through remote connections, even after the Gray Network itself stopped using the Orion software.

234. Further, on information and belief, Honeywell knowingly failed to report this cyber incident and other breaches to the Government.

235. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

B. Knowing Failure to Report Cybersecurity Incidents or Breaches

236. Honeywell knowingly failed to report suspected cyber incidents or breaches in violation of the Quantum Contracts and Federal Cybersecurity Requirements.

237. Under the Federal Cybersecurity Requirements, contractors must “rapidly report cyber incidents” directly to DOD and other agencies when the contractor’s network housing CUI is impacted. Adequate Security Rule § (b) and Adequate Security DFARS § (c) (report directly to DOD using prescribed channels)

238. As DOJ observed, “[p]rompt reporting by contractors often is crucial

for agencies to respond to a breach, remediate the vulnerability and limit the resulting harm.” <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

239. Yet a series of troubling cybersecurity incidents in 2020 culminating in the SolarWinds Attack brought Honeywell’s chickens home to roost by exposing its pervasive and systemic failures to adequately secure the Gray Network.

240. Honeywell knew of at least several cyber incidents or breaches alleged in this Complaint but failed to report them, leaving the Government unable to respond, remediate the vulnerability and limit the resulting harm.

241. After these cyber incidents occurred, Honeywell continued to present invoices for payment under the Quantum Contracts, falsely certifying that the Gray Network was secure and that no cyber incidents had occurred on the Gray Network; and the Government paid those claims.

242. Through its fraudulent course of conduct, Honeywell knowingly submitted or caused to be submitted false or fraudulent claims for payment under the Quantum Contracts, in violation of the False Claims Act, and the Government paid those claims.

243. The False Claims Act is the appropriate tool to remedy Honeywell’s knowing violation. DOJ is seeking to hold accountable “entities or individuals that

put U.S. information or systems at risk by knowingly violating obligations to monitor and report cybersecurity incidents and breaches” because “[p]rompt reporting by contractors often is crucial for agencies to respond to a breach, remediate the vulnerability and limit the resulting harm.”

<https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>; <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

VI. MATERIALITY

244. Honeywell knew that compliance with the Quantum Contracts and Federal Cybersecurity Requirements was material to the government’s decision to pay claims under the Quantum Contracts. Honeywell also knew that truthful records and statements in support of claims for the Quantum Contracts were material to the government’s decision to pay these claims.

245. Some of the factors in evaluating materiality under the False Claims Act include (a) statutory, regulatory, and contractual language, (b) whether the violations go to the heart of the benefit of the bargain, (c) whether the violations were serious and material and not merely technical or minor infractions of rules, (d) the government’s actions relative to similar violations, (e) whether any reasonable person would attach importance to Defendant’s choice of actions, and (f) Defendant’s knowledge relative to these factors. All these factors demonstrate

materiality in this case and have been addressed throughout this Complaint.

246. Honeywell knowingly submitted or caused to be submitted thousands of false or fraudulent claims and used false records and statements in support of false or fraudulent claims under the Quantum Contracts in violation of the Federal Cybersecurity Requirements designed to safeguard sensitive Government information.

247. Further, Honeywell knowingly submitted claims under the Quantum Contracts. In turn, those fraudulent claims were submitted to the Government and the Government paid those claims.

248. Therefore, Honeywell knowingly submitted or caused to be submitted thousands of false or fraudulent claims and used false records and statements in support of false or fraudulent claims under the Quantum Contracts.

249. This case is precisely the type of fraud scheme remedied by the False Claims Act. One example is the settled case, *U.S. ex rel. Glenn v. Cisco Systems, Inc.*, Case No. 1:11-cv-00400 (W.D.N.Y. 2019) in which relators alleged that Cisco knowingly sold flawed video surveillance systems to federal and state governments that could have but had not yet resulted in severe cybersecurity breaches. Cisco paid \$8.6M for its failure to protect against a potential cybersecurity failure. *United States ex rel. Glenn v. Cisco Systems, Inc.*, No. 1:11-cv-00400- RJA (W.D.N.Y. July 31, 2019); Press Release, *Attorney General James*

Secures \$6 Million from Cisco Systems in Multistate Settlement (Aug.

1. 2019), <https://ag.ny.gov/press-release/2019/attorney-general-james-secures-6-million-cisco-systems-multistate-settlement>.

250. Another example is the litigated cases of *U.S. ex rel. Markus v. Aerojet RocketDyne Holdings, Inc.*, Case No. 2:15-cv-02245 (E.D. Cal. Oct. 2021), in which the United States filed a “statement of interest,” and the Court recently denied all summary judgment motions, allowing the case to proceed to trial. <https://casetext.com/case/united-states-ex-rel-markus-v-aerojet-rocketdyne-holdings-inc-6>

251. Citing cybersecurity breaches in 2013 and a 2014 outside audit that determined that **Aerojet was noncompliant with 5 of the 59 required controls under DFARS**, the Court held that there was a genuine dispute of fact as to whether the company fully disclosed its noncompliance with DFARS and NASA FARS cybersecurity requirements. *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, Memorandum and Order Re: Cross Motions for Summary Judgment, 2:15-cv-02245 WBS AC, slip op. at *12-13 (E.D. Cal. Feb. 1, 2022).

252. The Court found that “[i]t may be reasonably inferred that compliance was significant to the government because without complete knowledge about compliance, or noncompliance, with the clauses, the government

cannot adequately protect its information.” *United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, Memorandum and Order Re: Cross Motions for Summary Judgment, 2:15-cv-02245 WBS AC, slip op. at *12-13 (E.D. Cal. Feb. 1, 2022).

253. In the Court’s denial of Aerojet’s prior motion to dismiss, the Court found that failure to comply with applicable security controls such as the “adequate security” NIST standards and further, failure to disclose noncompliance of those requirements could be sufficient to establish materiality under the FCA:

These acquisition regulations require that the defense contractor can handle certain technical information.

Here, compliance with these cybersecurity requirements could have affected [Aerojet]’s ability to handle technical information pertaining to missile defense and rocket engine technology. Accordingly, misrepresentations as to compliance with these cybersecurity requirements could have influenced the extent to which [Aerojet] could have performed the work specified by the contract.

United States ex rel. Markus v. Aerojet Rocketdyne Holdings, Inc., Memorandum and Order Re: Motion to Dismiss, 2:15-cv-02245 WBS AC, slip op. at *13 (E.D. Cal. May 8, 2019).

254. The Deputy Attorney General (DAG) announced recently that DOJ has created a Civil Cyber-Fraud Initiative to pursue cybersecurity related fraud by government contractors, including the fraud scheme alleged here, to “hold accountable entities or individuals that put U.S. information or systems at risk by

- knowingly providing deficient cybersecurity products or services
- knowingly misrepresenting their cybersecurity practices or protocols, or
- knowingly violating obligations to monitor and report cybersecurity incidents and breaches.”

Press Release, Office of Public Affairs, U.S. Department of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative (Oct. 6, 2021), <https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative>; and <https://www.justice.gov/opa/speech/acting-assistant-attorney-general-brian-m-boynton-delivers-remarks-cybersecurity-and>

255. The facts alleged in this Complaint show that Honeywell was well aware of the requirements under the Quantum Contracts and the Federal Cybersecurity Requirements; and, further, that the violations alleged in this Complaint were material to the Government’s decision to pay.

256. Honeywell also well knew that the unlawful conduct alleged in this

Complaint went to the very heart of the bargain under for the payment of claims for cybersecurity services. The Government expects and requires that claims be paid only for accurate and truthful claims under the Quantum Contracts.

257. Honeywell's statutory and programmatic requirements for complete, accurate, and truthful reporting during the claims submission process under the Quantum Contracts go directly to the "essence of the bargain." These requirements are neither "minor nor insubstantial."

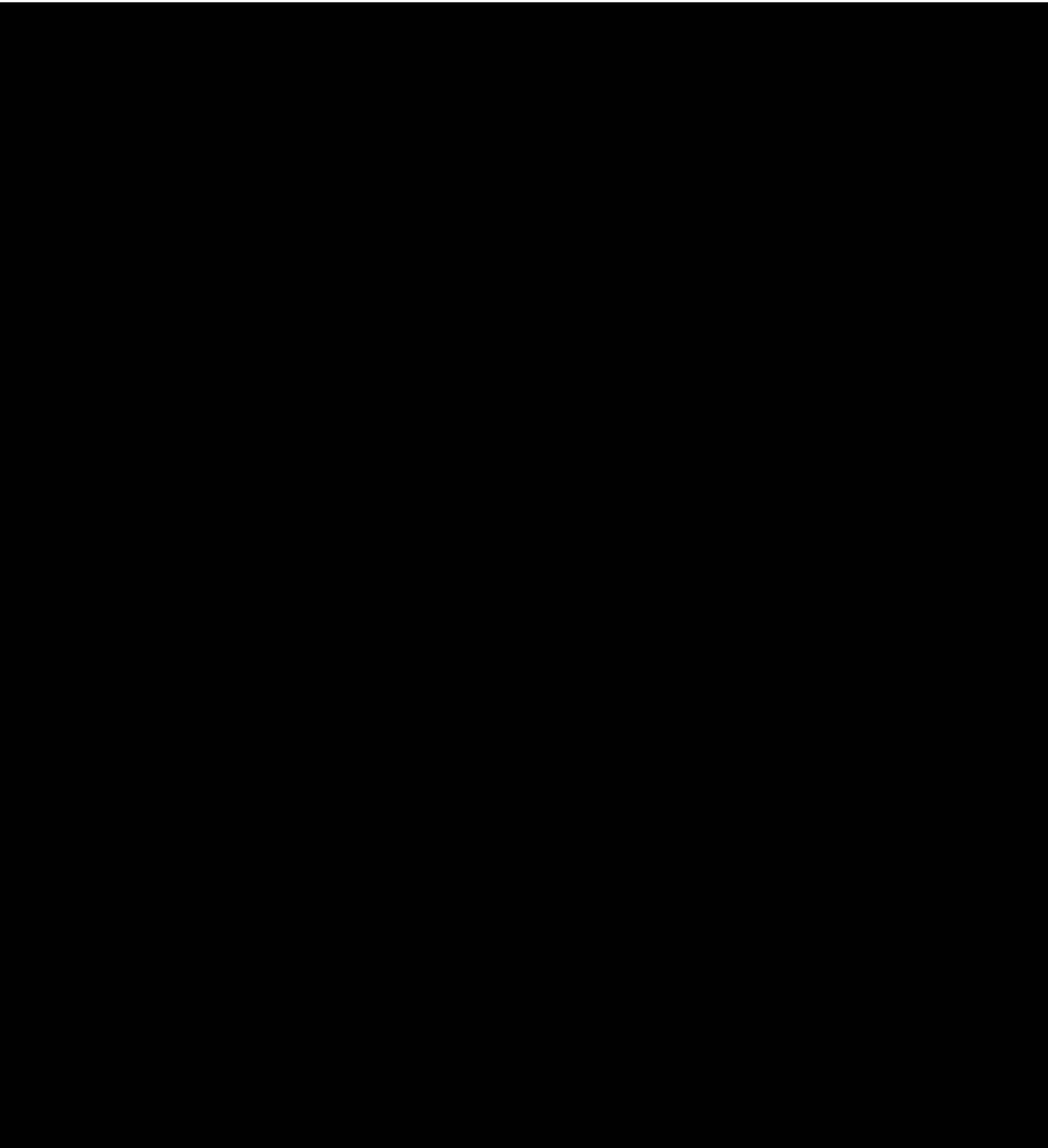
258. Honeywell's violations of the statutory, regulatory, and programmatic requirements were serious and material, leading to actual or potential harm, and were made with at least reckless disregard of the seriousness of their violations.

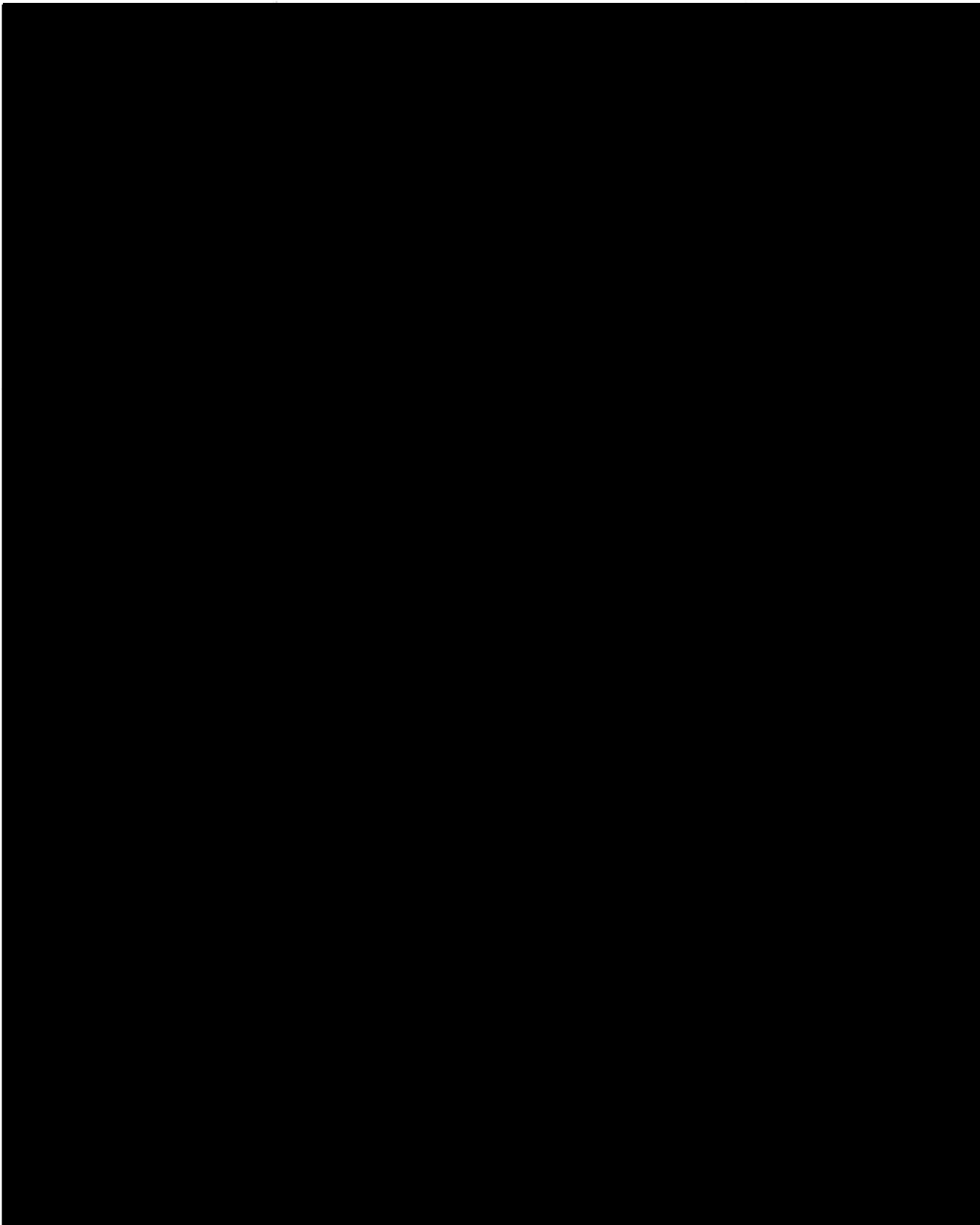
259. Honeywell's violations were not immaterial or inadvertent technical mistakes in processing paperwork, or simple and honest misunderstanding of the rules, terms and conditions, or certification requirements. Rather, Honeywell knowingly failed to comply with material legal obligations and certifications.

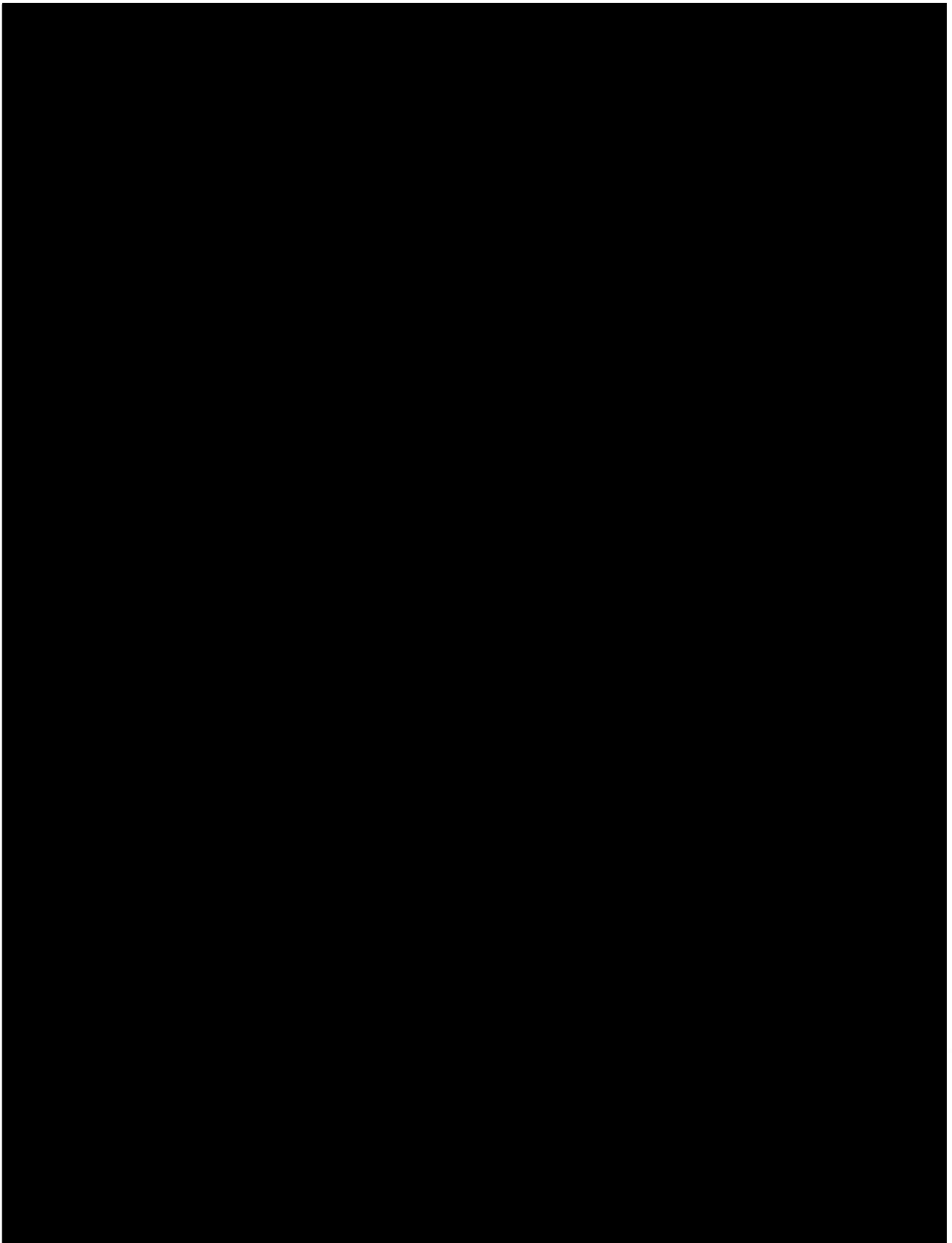
260. Honeywell knew that it was submitting or causing to submit false or fraudulent claims for, and false or fraudulent statements, records in support of claims for government funds, which the government paid.

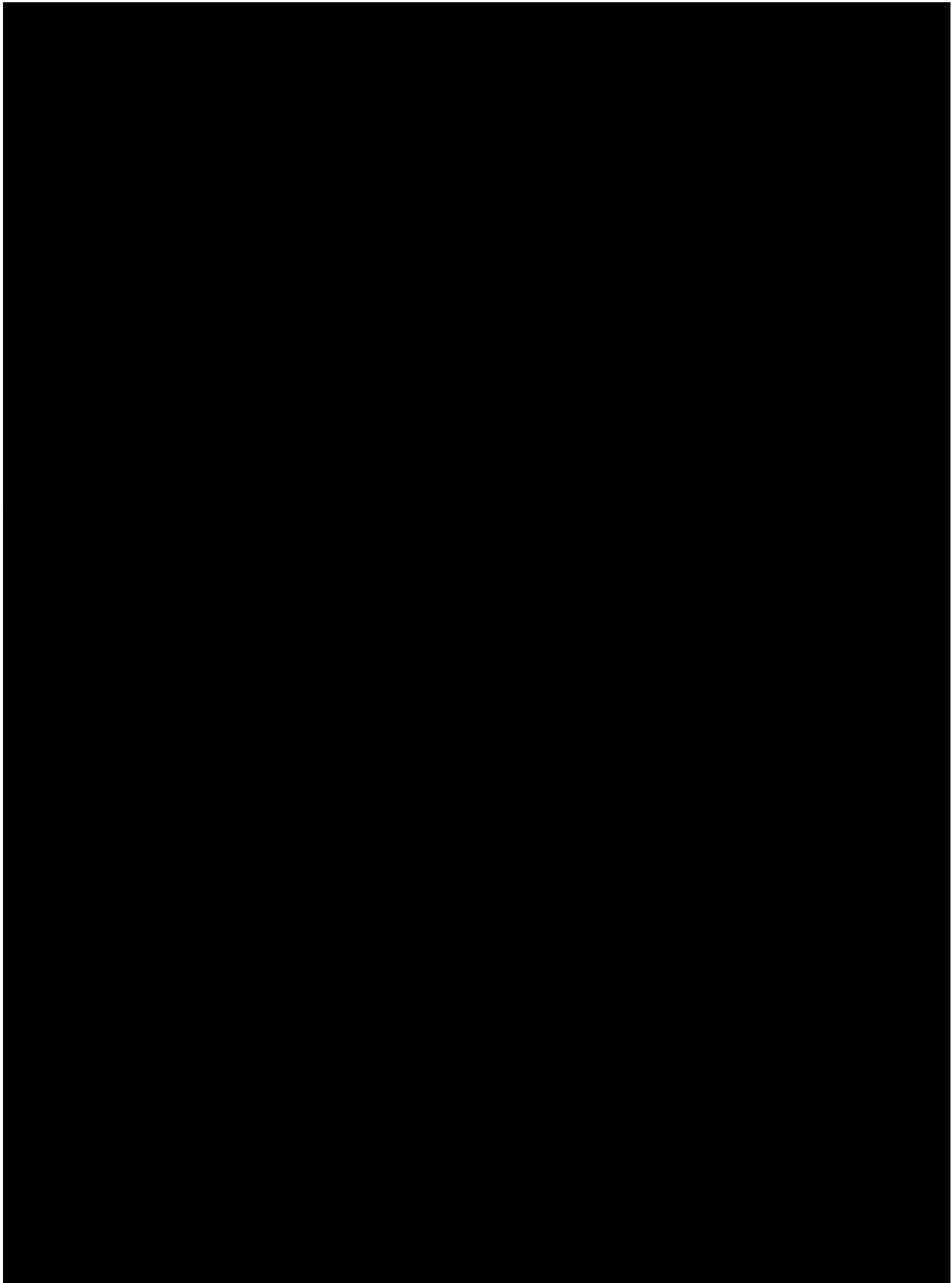
261. In short, there is ample evidence to show that Honeywell knew or should have known that its violations had the natural tendency to influence the

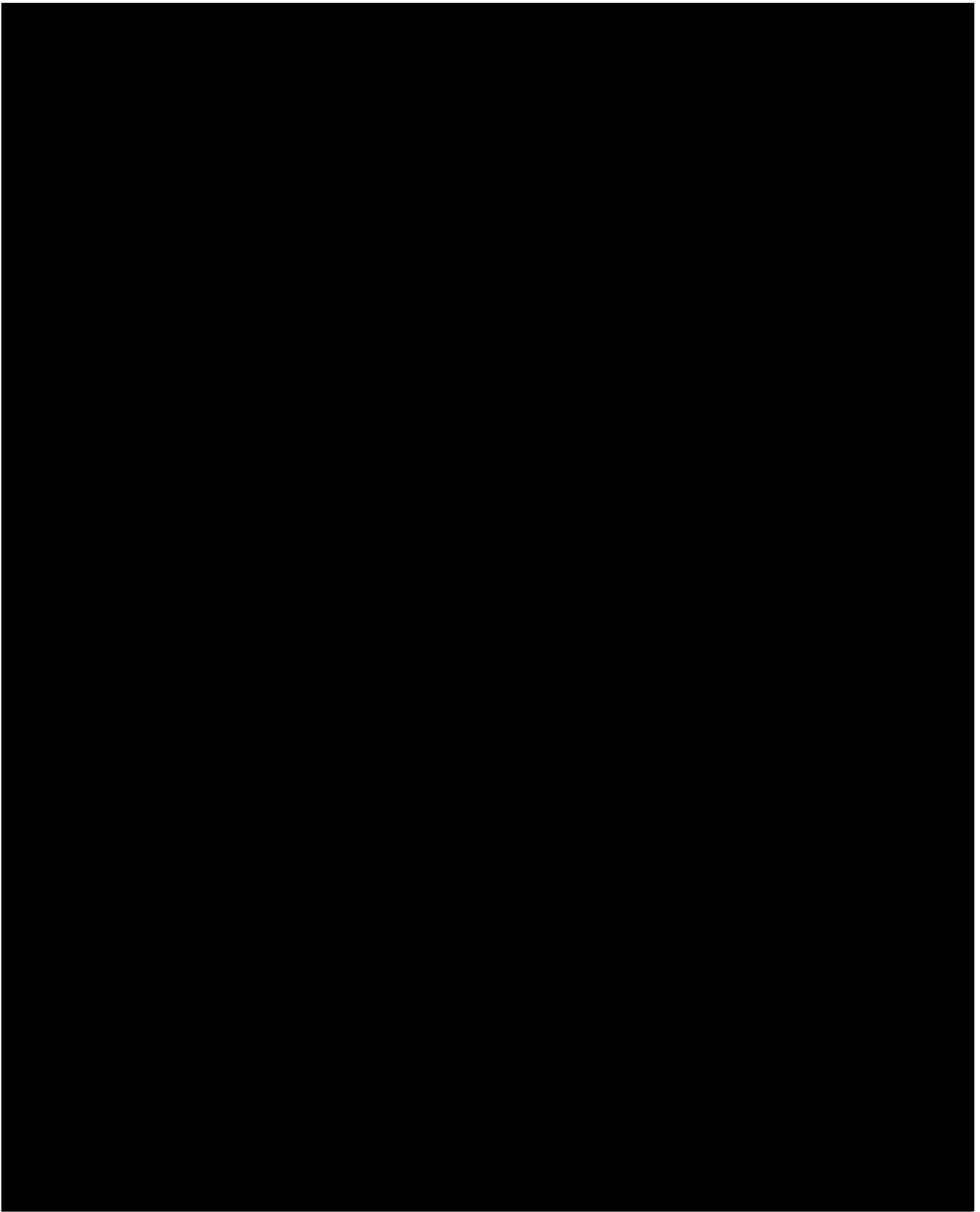
Government's decision to pay the claims under the Quantum Contracts and that any reasonable person would attach importance to its choice of action.

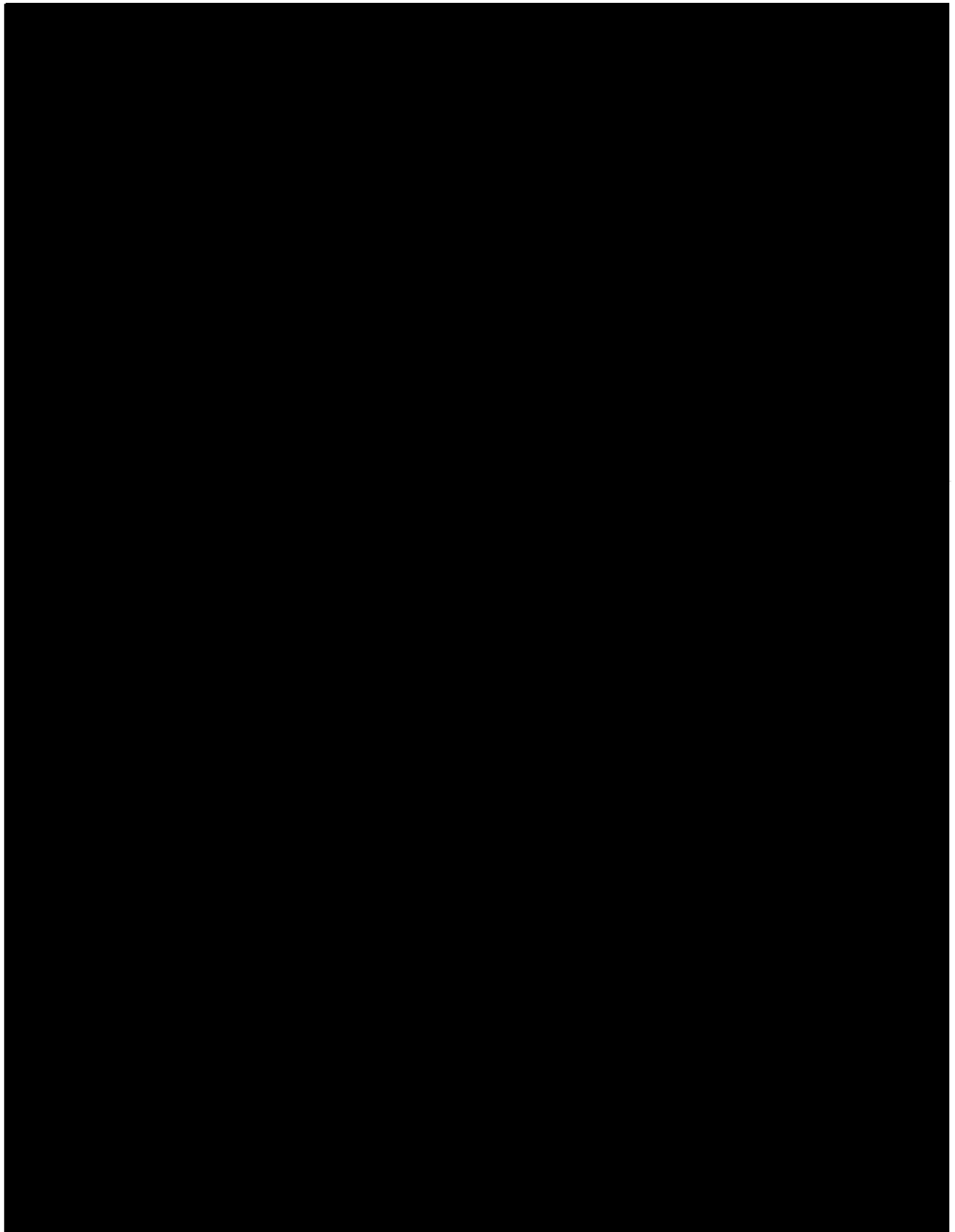


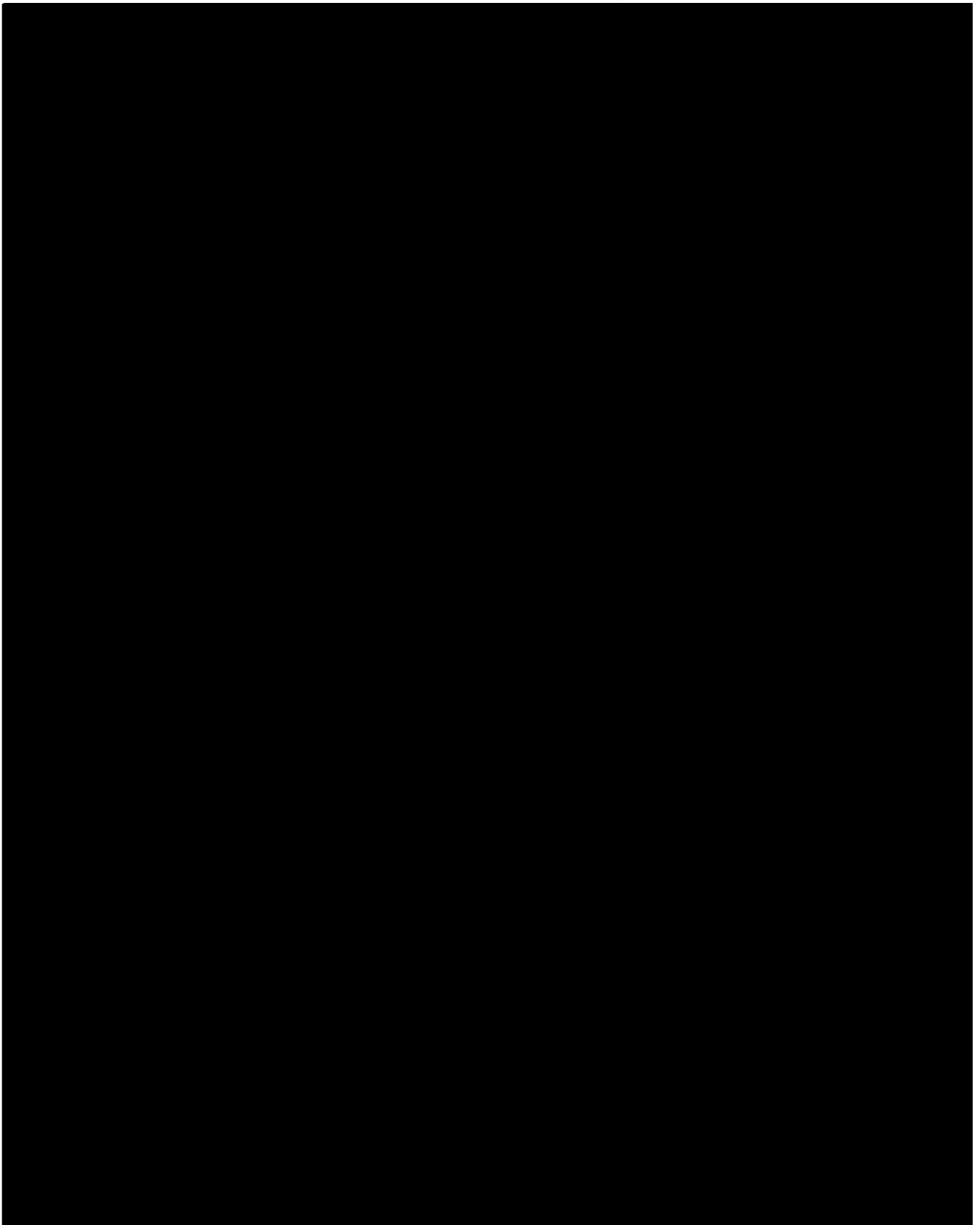


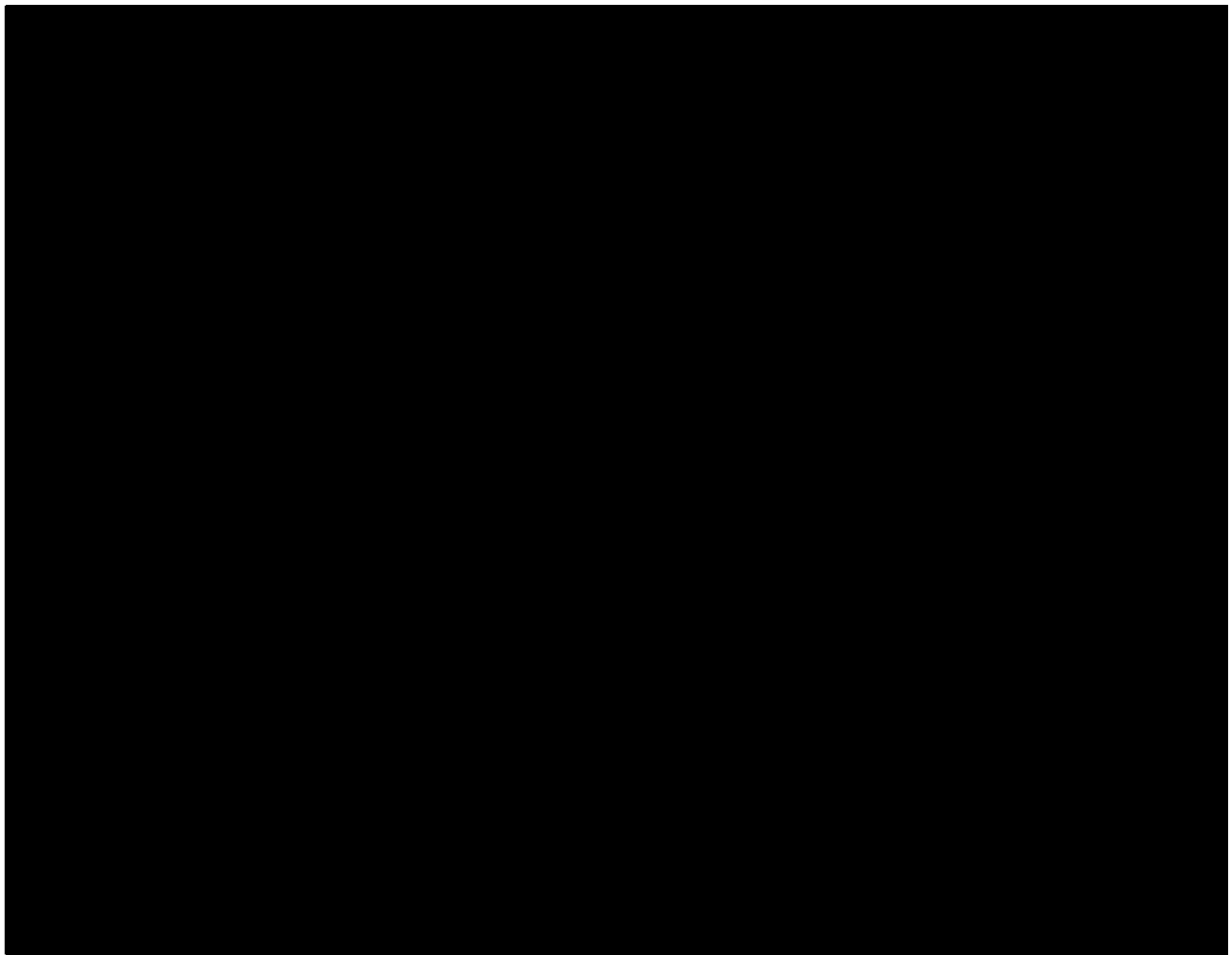












VIII. COUNTS

COUNT I

**Federal False Claims Act:
31 U.S.C. § 3729(a)(1)(A)**

293. The allegations in the preceding paragraphs are incorporated by reference.

294. Defendant knowingly presented or caused to be presented false or fraudulent claims for payment or approval in violation of 31 U.S.C. § 3729(a)(1)(A).

295. The United States paid for claims that otherwise would not have been allowed.

296. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

297. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

COUNT II

Federal False Claims Act: 31 U.S.C. § 3729(a)(1)(B)

298. The allegations in the preceding paragraphs are incorporated by reference.

299. Defendant knowingly made, used or caused to be made or used, false records or statements material to false or fraudulent claims, in violation of 31 U.S.C. § 3729 (a)(1)(B).

300. The United States paid for claims that otherwise would not have been allowed.

301. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus

civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

302. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

COUNT III

Federal False Claims Act: 31 U.S.C. § 3729(a)(1)(G)

303. The allegations in the preceding paragraphs are incorporated by reference.

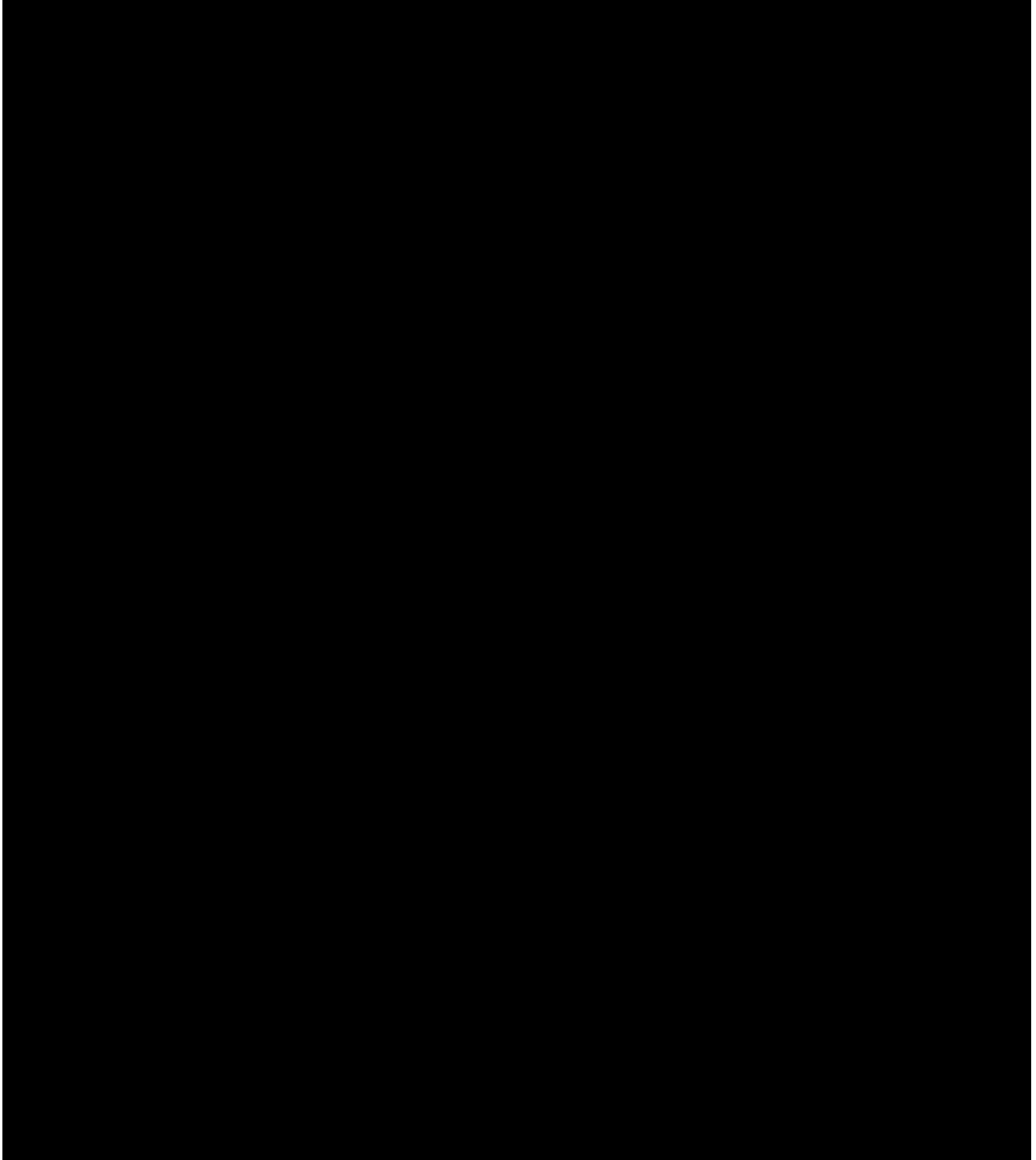
304. Defendant knowingly made, used, or caused to be made or used, false records or statements material to an obligation to pay or transmit money or property to the Government, or knowingly concealed or knowingly and improperly avoided or decreased an obligation to pay or transmit money or property to the Government, in violation of 31 U.S.C. § 3729 (a)(1)(G).

305. The United States paid for claims that otherwise would not have been allowed.

306. Because of these false or fraudulent claims, Defendant is liable to the United States for incurred damages resulting from such false claims, trebled, plus civil penalties for each violation of the Act, and liable for all other relief authorized by the statute.

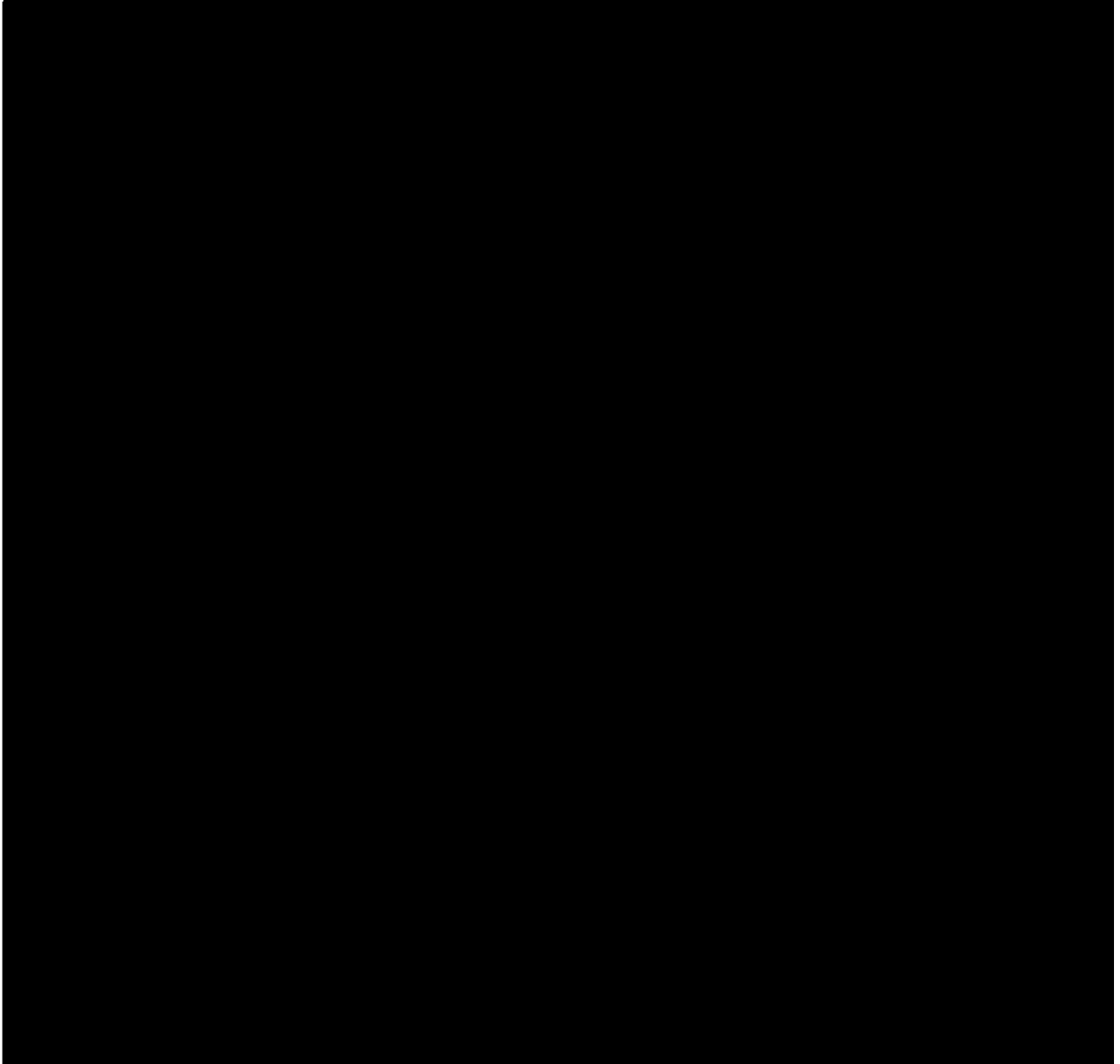
307. As a result of Defendant's violations, the United States has suffered damages in an amount to be determined at trial.

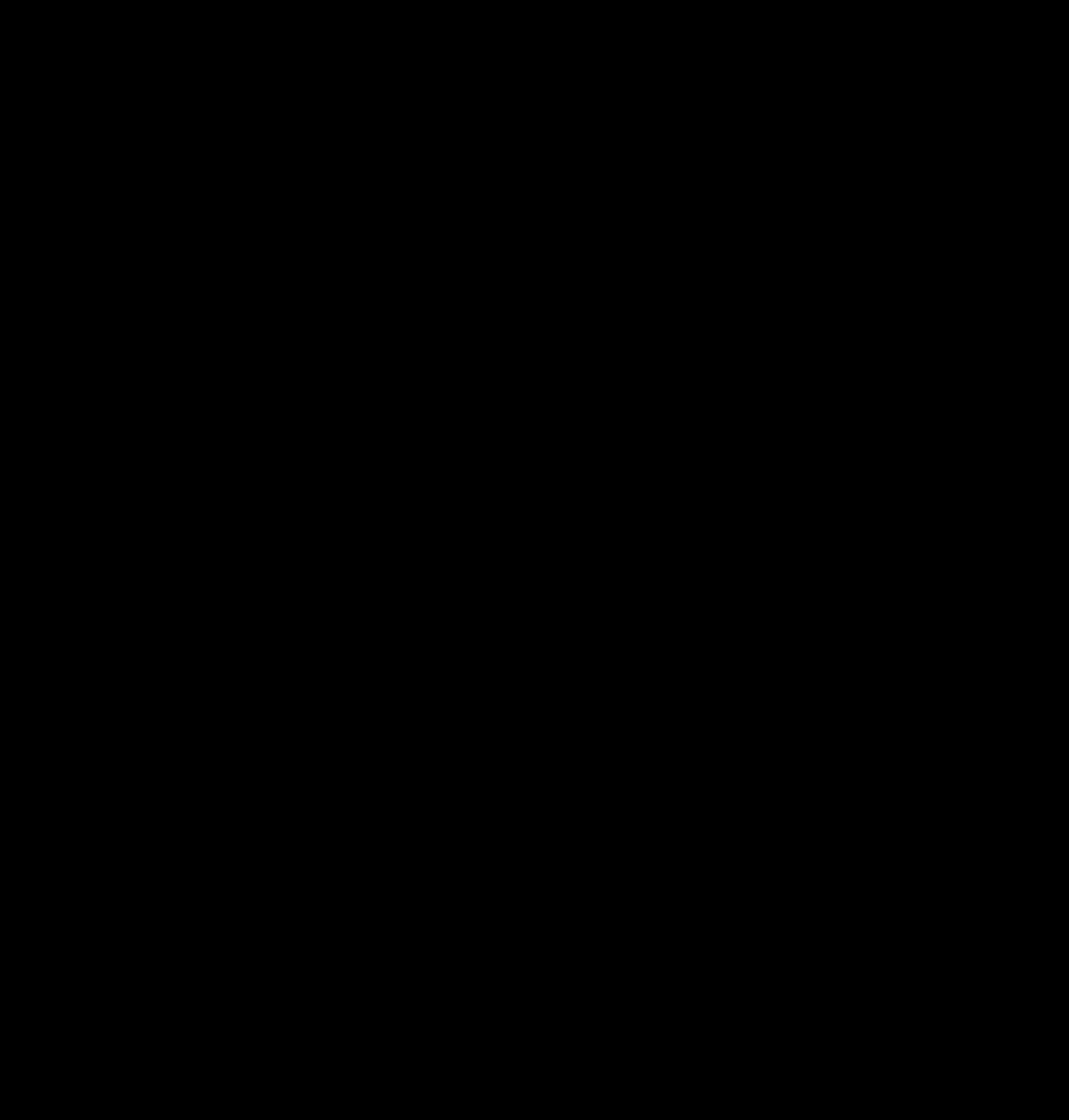
COUNT IV





COUNT V

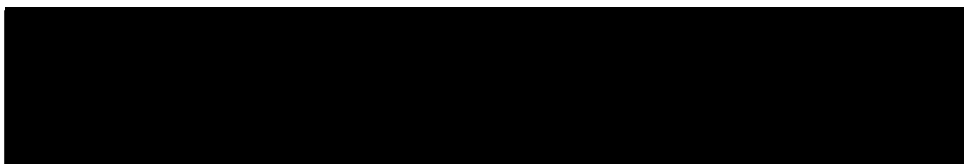


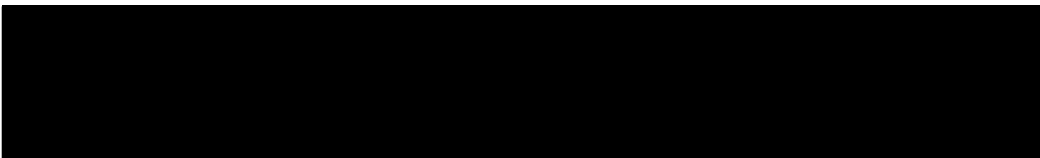


WHEREFORE, Relator, on behalf of Relator and the United States, prays:

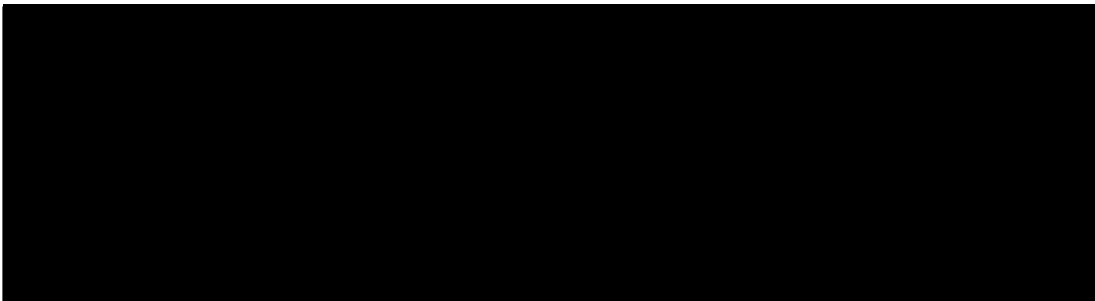
- (a) That the Court enter judgment against Defendant in an amount equal to three times the amount of damages the United States has sustained

because of Defendant's actions, plus a civil penalty of any amount within the applicable statutory ranges, for each violation;

- (b) That Relator be awarded an amount that the Court decides is reasonable for recovering the proceeds of the action, including but not necessarily limited to the civil penalties and damages, on behalf of the United States, which, pursuant to the False Claims Act, shall be at least 15 percent but not more than 25 percent of the proceeds of the action or settlement of the claim if the Government intervenes and proceeds with the action, and not less than 25 percent nor more than 30 percent of the proceeds of the action or settlement of the claim if the Government does not intervene;
- (c) That Relator receives all relief necessary to make Relator whole for Defendant's violations of 31 U.S.C. § 3730(h) and Minnesota Statute 181.932;
- (d) That the Court order Defendant to award Relator front pay in lieu of reinstatement;
- (e) That Relator receives an award of two times back pay, including the value of lost benefits and equity and restoration of service credit;
- (f) 

- 
- (g) That Relator receives an award of punitive damages in an amount sufficient to punish Defendant for its willful and malicious conduct and deter future, similar violations;
 - (h) That Relator be awarded all costs and expenses incurred, including reasonable attorneys' fees;
 - (i) That Relator be awarded all other legal and equitable relief to which Relator may be entitled;

(j)



- (k) That the Court order such other relief as is appropriate.

Trial by jury is hereby requested.

Dated: March 25, 2022

Respectfully submitted,



RENÉE BROOKER
(*Pro Hac Vice* pending)
D.C. Bar No. 430159
EVA GUNASEKERA
D.C. Bar No. 502542
GLENN E. CHAPPELL
D.C. Bar No. 1708506
Tycko & Zavareei LLP
1828 L Street NW
Suite 1000
Washington, DC 20036
(202) 417-3664
(202) 973-0950 (fax)
reneebrooker@tzlegal.com