PRATT'S GOVERNMENT CONTRACTING LAW REPORT

VOLUME 10 **NUMBER 4** **April 2024**

LexisNexis®

QUESTIONS ABOUT THIS PUBLICATION?

For questions about the **Editorial Content** appearing in these volumes or reprint permission, please call or email:

Heidi A. Litman at 516-771-2169
Email: ..... heidi.a.litman@lexisnexis.com

For assistance with replacement pages, shipments, billing or other customer service matters, please call:

Customer Services Department at . . . . . (800) 833-9844
Outside the United States and Canada, please call . . . . . (518) 487-3385
Fax Number . . . . . (800) 828-8341
LexisNexis® Support Center . . . . . https://supportcenter.lexisnexis.com/app/home/

For information on other Matthew Bender publications, please call

Your account manager or . . . . . (800) 223-1940
Outside the United States and Canada, please call . . . . . (518) 487-3385

Library of Congress Card Number:

ISBN: 978-1-6328-2705-0 (print)
ISSN: 2688-7290

Cite this publication as:

[author name], [article title], [vol. no.] PRATT'S GOVERNMENT CONTRACTING LAW REPORT [page number] (LexisNexis A.S. Pratt).
Michelle E. Litteken, GAO Holds NASA Exceeded Its Discretion in Protest of FSS Task Order, 1 PRATT'S GOVERNMENT CONTRACTING LAW REPORT 30 (LexisNexis A.S. Pratt)

Because the section you are citing may be revised in a later release, you may wish to photocopy or print out the section for convenient future reference.

Editorial Office
230 Park Ave., 7th Floor, New York, NY 10169 (800) 543-6862
www.lexisnexis.com

MATTHEW BENDER

(2024–Pub.4938)

Editor-in-Chief, Editor & Board of Editors

Pratt's Government Contracting Law Report is published 12 times a year by Matthew Bender & Company, Inc. For customer support, please contact LexisNexis Matthew Bender, 9443 Springboro Pike, Miamisburg, OH 45342 or call Customer Support at 1-800-833-9844. Direct any editorial inquiries and send any material for publication to Steven A. Meyerowitz, Editor-in-Chief, Meyerowitz Communications Inc., 26910 Grand Central Parkway Suite 18R, Floral Park, New York 11005, smeyerowitz@meyerowitzcommunications.com, 631.291.5541. Material for publication is welcomed—articles, decisions, or other items of interest to lawyers and law firms, in-house counsel, government lawyers, senior business executives, and anyone interested in privacy and cybersecurity related issues and legal developments. This publication is designed to be accurate and authoritative, but neither the publisher nor the authors are rendering legal, accounting, or other professional services in this publication. If legal or other expert advice is desired, retain the services of an appropriate professional. The articles and columns reflect only the present considerations and views of the authors and do not necessarily reflect those of the firms or organizations with which they are affiliated, any of the former or present clients of the authors or their firms or organizations, or the editors or publisher.

POSTMASTER: Send address changes to *Pratt's Government Contracting Law Report*, LexisNexis Matthew Bender, 230 Park Ave. 7th Floor, New York NY 10169.

Government Contractors Beware: New Cybersecurity Rules and False Claims Act Enforcement Actions on the Rise

By Michelle A. Reed, Michael J. Vernick, Elizabeth D. Scott, Angela B. Styles, Natasha G. Kohne, Rachel Claire Kurzweil and Joseph Hold*

In this article, the authors explain what government-contracted tech companies and other organizations receiving government funds should understand about how regulators and private whistleblowers alike are using the False Claims Act to enforce required cybersecurity standards.

Somewhat more than two years after the Department of Justice (DOJ) established its Civil-Cyber Fraud Initiative, there has been a recent uptick in enforcement and regulatory activity related to cybersecurity. September opened with the unsealing of a qui tam action under the False Claims Act (FCA) against Penn State University, alleging the school failed to comply with the Department of Defense's (DoD) cybersecurity requirements.[1] Only a few days later, the DOJ announced[2] a $4 million settlement with Verizon Business Network Services LLC (Verizon) to resolve claims that the telecom giant failed to meet cybersecurity requirements in its provision of secure public internet connections to federal agencies. And in early October, the Federal Acquisition Regulatory Council published two proposed rules increasing cybersecurity requirements for government contractors, which may open many companies up to new or increased FCA liability.

Amid this rising cyber-related FCA activity, government-contracted tech companies and other organizations receiving government funds must understand how regulators and private whistleblowers alike are using the FCA to enforce required cybersecurity standards.

---

* The authors, attorneys with Akin Gump Strauss Hauer & Feld LLP, may be contacted at mreed@akingump.com, mvernick@akingump.com, edscott@akingump.com, astyles@akingump.com, nkohne@akingump.com, rkurzweil@akingump.com, and jhold@akingump.com, respectively.

[1] https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[2] https://www.justice.gov/opa/pr/cooperating-federal-contractor-resolves-liability-alleged-false-claims-caused-failure-fully.

BACKGROUND

The FCA is the primary tool for combatting allegations of fraud in the government contracts space.[3] In October 2021, DOJ introduced the Civil Cyber-Fraud Initiative, harnessing the FCA to curtail cybersecurity-related fraud by government contractors and federal grant recipients that knowingly provide deficient cybersecurity products, misrepresent their cybersecurity practices or status, or violate breach reporting requirements.

Since then, federal agencies have continued to issue new cybersecurity requirements and reporting obligations in government contracts and funding agreements—which may bring yet more vigorous efforts by DOJ and related agencies to pursue alleged fraud, waste and abuse in government spending under the FCA. The FCA also features a qui tam provision, which permits whistleblowers (relators) to bring claims in the government's name against alleged fraudsters and to share in any recoveries.

On March 8, 2022, DOJ announced the first settlement under the Civil Cyber-Fraud Initiative involving Florida-based healthcare provider Comprehensive Health Services LLC, which agreed to pay $930,000 to resolve FCA violations stemming from its alleged misrepresentations to the United States Air Force and State Department that it complied with security contract requirements concerning medical services.[4]

Just a few months later, on July 8, 2022, DOJ announced another cybersecurity-related FCA settlement involving defense and space sector contractor Aerojet Rocketdyne, Inc., which agreed to a $9 million settlement to resolve allegations made in a qui tam suit that it misrepresented its compliance with DoD regulations to safeguard covered defense information, which includes controlled unclassified information, and with a National Aeronautics and Space Administration (NASA) rule for protecting sensitive information.[5]

On March 14, 2023, DOJ announced yet another cybersecurity related FCA settlement with Jelly Bean Communications Designs LLC (along with com-

---

[3] S. Rep. No. 99-345, at 2 (1986) ("This growing pervasiveness of fraud necessitates modernization of the Government's primary litigative tool for combatting fraud; the False Claims Act").

[4] Dept. of Justice, Press Release, Medical Services Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan (March 8, 2022) available at https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical.

[5] Dept. of Justice, Press Release, Aerojet Rocketdyne Agrees to Pay $9 Million to Resolve False Claims Act Allegations of Cybersecurity Violations in Federal Government Contracts (July 8, 2022), available at https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity.

pany co-owner and manager Jeremy Spinks), which agreed to pay nearly $300,000 to resolve allegations that the company and Spinks violated the FCA by failing to patch, update and maintain the federally funded children's health insurance website they created and hosted, leaving personal information vulnerable to attack.[6]

The Penn State University and Verizon cases reflect this continuing pattern of focus on cybersecurity compliance as a potential hook for FCA liability. This line of cases and settlements indicates additional cyber-related FCA actions are likely on the horizon as regulators and whistleblowers alike seek to identify potential fraudulent claims for federal funds and encourage government contractors to place greater emphasis on meeting cybersecurity requirements, thereby protecting the federal infrastructure from dangerous cybersecurity intrusions.

PENN STATE WHISTLEBLOWER CASE

On September 1, 2023, the U.S. District Court for the Eastern District of Pennsylvania unsealed an FCA qui tam suit alleging Penn State University failed to provide adequate security for covered defense information.[7] Under the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, contractors must implement certain cybersecurity controls, including, at a minimum, adequate security for covered defense information, which requires implementing the 110 cybersecurity controls from NIST SP 800-171. DoD contractors are then required to conduct a self-assessment of their compliance with those 110 controls and submit their score to the DoD.[8]

Whistleblower Matthew Decker, Penn State University's former Chief Information Officer for its Applied Research Laboratory, brought the suit on behalf of the government. The suit alleges that Penn State University falsely certified its compliance with the NIST SP 800-171 self-assessment and never actually achieved DFARS compliance. The complaint also alleges that the university's leadership repeatedly ignored certification concerns and that sensitive information was at risk during data migration to commercial cloud

---

[6] Dept. of Justice, Press Release, Jelly Bean Communications Design and its Manager Settle False Claims Act Liability for Cybersecurity Failures on Florida Medicaid Enrollment Website (March 14, 2023), available at https://www.justice.gov/opa/pr/jelly-bean-communications-design-and-its-manager-settle-false-claims-act-liability.

[7] United States ex rel. Matthew Decker v. Pennsylvania State University, No. 2:22-cv-03895-PD (E.D. Pa. January 1, 2023).

[8] This is a self-attestation of compliance rather than an official audit procedure.

storage.[9] While DOJ declined to intervene in the case, the department's investigation into the claims is ongoing, and it may opt to intervene at a later time.

This case highlights the litigation and enforcement risk that government contractors now face from the expansive checklist of cybersecurity controls they must meet to obtain and keep their contracts. Government contractors should closely examine their self-attestations and be responsive to internal complaints to ensure they are in full compliance with these mandatory requirements.

VERIZON CIVIL-CYBER FRAUD INITIATIVE SETTLEMENT

Verizon agreed to pay approximately $4 million to resolve FCA allegations that it failed to satisfy certain cybersecurity requirements related to information technology services provided to federal agencies.[10] According to the September 5, 2023, settlement agreement with DOJ, the allegations concerned Verizon's Managed Trusted Internet Protocol Service (MTIPS), which is designed to provide federal agencies with secure connections to the public internet and other external networks.[11] The settlement resolved allegations that the MTIPS solution did not satisfy the cybersecurity controls required for Trusted Internet Connections for General Services Administration (GSA) contracts from 2017–2021.[12]

Additionally, the settlement followed Verizon's self-disclosure of the issue and implementation of remedial measures. For instance, Verizon initiated its own independent investigation and compliance review, provided detailed supplemental written disclosures, and cooperated with the government's investigation, including by identifying individuals responsible for the issues, preserving relevant documents and providing rolling disclosures of relevant information.[13] Verizon also worked to update the MTIPS system security plan and take other remedial steps to fulfill its contractual requirements.

The settlement agreement states that $2.7 million of the settlement was allocated as restitution, leaving about $1.3 million from the government's application of a multiplier. Under the FCA, the government may seek up to treble damages plus statutory penalties, meaning Verizon likely avoided a much greater total penalty by self-disclosing.

---

[9] Id. at 14.

[10] Dept. of Justice, Press Release, Cooperating Federal Contractor Resolves Liability for Alleged False Claims Caused by Failure to Fully Implement Cybersecurity Controls (September 5, 2023) available at https://www.justice.gov/opa/pr/cooperating-federal-contractor-resolves-liability-alleged-false-claims-caused-failure-fully.

[11] Id.

[12] Id.

[13] Id.

FEDERAL ACQUISITION REGULATORY (FAR) COUNCIL'S PROPOSED CYBER RULES

Amid this heightened FCA interest, the FAR Council recently proposed two sweeping rules to increase cybersecurity requirements for federal contractors. The first proposed rule[14] would standardize contractual cyber requirements for "unclassified federal information systems."[15]

The second proposed rule[16] would require contractors to share information on cyber threats and report cyber incidents to the government within eight hours of discovery.[17] These broad proposals would apply to the majority of federal contractors, including organizations otherwise exempt from many government contracting rules and will require precise and timely incident response to comply.

Both of these proposed rules additionally explicitly state that cybersecurity obligations and cyber incident reporting are material to government contract eligibility and payment,[18] thereby setting the stage for potential future FCA liability for noncompliance. The wider net these proposed rules cast, alongside recent increased cybersecurity-related FCA activity, could have potentially serious implications for contractor compliance efforts.

LESSONS FOR FEDERAL CONTRACTORS

Cybersecurity practice and policy will only continue to grow in importance for organizations performing government contracts. Federal contractors, universities and other federal grant recipients should begin reevaluating their compliance with cybersecurity requirements, paying particular attention to the accuracy of their self-evaluations. The cybersecurity compliance landscape is evolving rapidly and requires continuous internal monitoring, as well as a system for handling internal complaints. Outside counsel can be instrumental in ensuring complaints receive the necessary evaluation in light of the company's cybersecurity obligations. Additional training and team evaluations

---

[14] https://www.federalregister.gov/documents/2023/10/03/2023-21327/federal-acquisition-regulation-standardizing-cybersecurity-requirements-for-unclassified-federal.

[15] Federal Acquisition Regulation: Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems, Proposed Rule, 88 FR 68402 (October 3, 2023) [hereinafter, Proposed Rule 1].

[16] https://www.federalregister.gov/documents/2023/10/03/2023-21328/federal-acquisition-regulation-cyber-threat-and-incident-reporting-and-information-sharing.

[17] Federal Acquisition Regulation: Cyber Threat and Incident Reporting and Information Sharing, Proposed Rule, 88 FR 68055 (October 3, 2023) [hereinafter, Proposed Rule 2].

[18] Proposed Rule 1 at 7; Proposed Rule 2 at 4.

may also help contractors tackle the growing and increasingly complicated web of cybersecurity requirements contractors face.

Contractors can expect to see many more enforcement actions in the near future, from both the government and whistleblowers and should therefore take the opportunity now to bolster their compliance efforts.