King & Spalding

Client Alert

Special Matters & Government Investigations

FEBRUARY 24, 2025

For more information, contact:

Brandt Leibe
+1 202 626 8983
bleibe@kslaw.com

Sumon Dantiki
+1 202 626 5591
sdantiki@kslaw.com

Michael Galdo
+1 512 457 2081
adavey@kslaw.com

Alexander Davey (Alex)
+1 713 276 7376
adavey@kslaw.com

King & Spalding

Houston
1100 Louisiana Street
Suite 4100
Houston, TX 77002
T. +1 713 751 3200

DOJ Continues Cybersecurity False Claims Act Enforcement in New Administration

KEY TAKEAWAYS FOR FEDERAL CONTRACTORS

The Department of Justice (DOJ) recently announced an $11.3 million settlement of False Claims Act allegations against a Department of Defense (DOD) contractor administering its TRICARE health insurance program that allegedly falsely certified compliance with DOD cybersecurity contract requirements between 2015 and 2018. The settlement underscores the government's continued focus on using the False Claims Act (FCA) to enforce cybersecurity-related requirements against companies that contract with the federal government.

ONGOING FCA CYBER ENFORCEMENT

DOJ's press release announcing the settlement does not refer to DOJ's Civil Cyber Fraud Initiative, but it emphasizes DOJ's "ongoing efforts" to enforce FCA liability in cybersecurity cases. This suggests that DOJ is committed to using the FCA as a powerful tool to enforce cybersecurity standards and hold government contractors responsible for failures to live up to federal cybersecurity standards.

The press release includes a pointed statement from Brett Shumate, who is currently the acting head of DOJ's Civil Division and has been nominated for the permanent role, emphasizing that "the Justice Department will continue to pursue federal contractors that place [government] data at risk by failing to meet material cybersecurity requirements in their contracts."

Even if DOJ's enforcement priorities shifted in the coming months, a single employee with knowledge of where an IT system for a government contractor falls short of federal cybersecurity standards may file a lawsuit under the FCA's qui tam provision. These qui tam suits can go forward with or without DOJ involvement in the case. This empowers private

whistleblowers to file lawsuits alleging fraud against the government, with these private actors eligible to reap as much as 30 percent of the total amount recovered.

AFCA MAY FURTHER INCREASE SCRUTINY OF CYBERSECURITY LAPSES

The recently passed Administrative False Claims Act (AFCA) may also prove to be a potent weapon for the government in enforcing contractual cybersecurity obligations. Passed in December 2024, the AFCA updates the existing law that permit federal agencies to pursue claims against government contractors on their own, without a FCA lawsuit. The AFCA increases the cap on damages from $150,000 to $1,000,000, streamlines the enforcement procedures, and allows agencies to recoup the costs of investigating and prosecuting AFCA matters.

These changes give agencies, including DOD, added incentive and additional tools to pursue smaller cybersecurity lapses that may not meet DOJ thresholds for FCA suits or attract attention from whistleblowers. Importantly, AFCA investigations also involve investigatory subpoenas and retain the ability to refer matters to DOJ for criminal and civil investigation if additional evidence is discovered during the investigation.

ROLE OF DOD AUTHORITIES IN CYBER-FOCUSED FCA INVESTIGATIONS

This case also highlights the involvement of two components of the Department of Defense:

- Defense Criminal Investigative Service (DCIS). While DCIS has a smaller cyber investigative team than large law enforcement agencies like the FBI or components of the Department of Homeland Security, it is highly skilled and has worked closely with those law enforcement entities in recent high-profile cyber initiatives.
- The Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). DIBCAC assesses DOD contractor's cyber risk mitigation efforts and their compliance with the applicable cybersecurity standards.

Combining DIBCAC's auditing infrastructure with DCIS's cyber expertise could result in heightened scrutiny for DOD contractors.

DOD's Cybersecurity Maturity Model Certification (CMMC) Program will be phased in throughout 2025, implementing cybersecurity rules in all DOD contracts through changes to the Defense Federal Acquisition Regulation Supplement (DFARS). The changes include third-party verification and additional cybersecurity assessment requirements to be added as an express condition of contracts with DOD.

The combination of additional regulations plus heightened scrutiny from expert DOD oversight entities, means that DOD contractors should carefully prepare for cybersecurity enforcement changes in the coming months.

THE LONG TAIL OF COMPLIANCE FAILURES

This settlement is another reminder that cybersecurity noncompliance can have a long tail. The alleged false certifications in this case occurred between 2015 and 2018, yet enforcement action is only now resulting in financial penalties. The gap between the underlying conduct and the finalized settlement underscores the extended risk horizon for federal contractors, reinforcing the need for ongoing compliance monitoring and proactive remediation of past cybersecurity lapses.

RISKS OF INHERITING CYBERSECURITY LIABILITY

The contractor in this case was acquired in March 2016. The alleged false certifications with cybersecurity requirements[i] were made annually, from November 2015 to November 2017. This highlights the need to assess cybersecurity risks in pre-acquisition diligence and conduct post-acquisition remediation, particularly where the acquisition target has government contracts.

DEBARMENT STILL IN PLAY?

The settlement does not prevent the federal government from pursuing suspension and debarment of the contractor, which, depending on how reliant an entity is on government contract revenue, can cause lasting damage to a contractors' future business.

WHAT THIS MEANS FOR YOUR ORGANIZATION

This settlement is the latest in a growing trend of cybersecurity-related FCA enforcement and part of a continued focus on cybersecurity compliance that will only grow as the government begins to utilize the new AFCA. Companies that have contracts with the federal government should consider proactive steps to assess and mitigate risk under privilege.

Special Matters & Government Investigations Partners

Gary Adamson
New York
+1 212 556 2113
gadamson@kslaw.com

Adam Baker
New York
+1 212 556 2376
abaker@kslaw.com

J.C. Boggs
Washington, DC
+1 202 626 2383
jboggs@kslaw.com

Christopher C. Burris
Atlanta
+1 404 572 4708
cburris@kslaw.com

Craig Carpenito
New York
+1 212 556 2142
ccarpenito@kslaw.com

Steve Cave
Northern Virginia
+1 703 245 1017
scave@kslaw.com

Michael J. Ciatti
Washington, DC
+1 202 661 7828
mciatti@kslaw.com

Daniel R. Coats
Washington, DC
+1 202 626 2642
dcoats@kslaw.com

Patrick M. Collins
Chicago
+1 312 764 6901
pcollins@kslaw.com

Ander M. Crenshaw
Washington, DC
+1 202 626 8996
acrenshaw@kslaw.com

Sumon Dantiki
Washington, DC
+1 202 626 5591
sdantiki@kslaw.com

Dan Donovan
Washington, DC
+1 202 626 7815
ddonovan@kslaw.com

Robert L. Ehrlich, Jr.
Washington, DC
+1 202 626 9710
rehrlich@kslaw.com

David Farber
Washington, DC
+1 202 626 2941
dfarber@kslaw.com

Zachary Fardon
Chicago
+1 312 764 6960
zfardon@kslaw.com

Lucas Fields
Washington, DC
+1 202 626 2399
lfields@kslaw.com

Emily Gordy
Washington, DC
+1 202 626 8974
egordy@kslaw.com

Leah B. Grossi
Washington, DC
+1 202 626 5511
lgrossi@kslaw.com

Ehren Halse
San Francisco
+1 415 318 1216
ehalse@kslaw.com

Max Hill, K.C.
London
+44 20 7551 2130
mhill@kslaw.com

Amy Schuller Hitchcock
Sacramento/San Francisco
+1 916 321 4819
ahitchcock@kslaw.com

John A. Horn
Atlanta
+1 404 572 2816
jhorn@kslaw.com

Andrew C. Hruska
New York
+1 212 556 2278
ahruska@kslaw.com

Rob Hur
Washington, DC
+1 202 383 8969
rhur@kslaw.com

Mark A. Jensen
Washington, DC
+1 202 626 5526
mjensen@kslaw.com

Dixie L. Johnson
Washington, DC
+1 202 626 8984
djohnson@kslaw.com

William Johnson
New York
+1 212 556 2125
wjohnson@kslaw.com

Barry Kamar
Miami
+1 305 462 6044
bkamar@kslaw.com

Allison F. Kassir
Washington, DC
+1 202 626 5600
akassir@kslaw.com

M. Alexander (Alec) Koch
Washington, DC
+1 202 626 8982
akoch@kslaw.com

Yelena Kotlarsky
New York
+1 212 556 2207
ykotlarsky@kslaw.com

Steve Kupka
Washington, DC
+1 202 626 5518
skupka@kslaw.com

Jade R. Lambert
Chicago
+1 312 764 6902
jlambert@kslaw.com

Jamie Allyson Lang
Los Angeles
+1 213 443 4325
jlang@kslaw.com

Raphael Larson
Washington, DC
+1 202 626 5440
rlarson@kslaw.com

Carmen Lawrence
New York
+1 212 556 2193
clawrence@kslaw.com

Brandt Leibe
Houston
+1 713 751 3235
bleibe@kslaw.com

Aaron W. Lipson
Atlanta
+1 404 572 2447
alipson@kslaw.com

Daniel E. Lungren
Washington, DC
+1 202 626 9120
dlungren@kslaw.com

William S. McClintock
Washington, DC
+1 202 626 2922
wmcclintock@kslaw.com

Amelia Medina
Atlanta
+1 404 572 2747
amedina@kslaw.com

Kendrick B. Meek
Washington, DC
+212 626 5613
kmeek@kslaw.com

Andrew Michaelson
New York
+212 790 5358
amichaelson@kslaw.com

Nema Milaninia
Washington, DC
+202 626 9273
nmilaninia@kslaw.com

Jim C. Miller III
Washington, DC
+1 202 626 5580
jmiller@kslaw.com

Patrick Montgomery
Washington, DC
+1 202 626 5444
pmontgomery@kslaw.com

Paul B. Murphy
Atlanta/Washington, DC
+1 404 572 4730
pbmurphy@kslaw.com

Grant W. Nichols
Austin/Washington, DC
+1 512 457 2006
gnichols@kslaw.com

Alicia O'Brien
Washington, DC
+1 202 626 5548
aobrien@kslaw.com

Patrick Otlewski
Chicago
+1 312 764 6908
potlewski@kslaw.com

Michael R. Pauzé
Washington, DC
+1 202 626 3732
mpauze@kslaw.com

Michael A. Plotnick
Washington, DC
+1 202 626 3736
mplotnick@kslaw.com

Olivia Radin
New York
+1 212 556 2138
oradin@kslaw.com

John C. Richter
Washington, DC
+1 202 626 5617
jrichter@kslaw.com

Rod J. Rosenstein
Washington, DC
+1 202 626 9220
rrosenstein@kslaw.com

Daniel C. Sale
Washington, DC
+1 202 626 2900
dsale@kslaw.com

Heather Saul
Atlanta
+1 404 572 2704
hsaul@kslaw.com

Greg Scott
Sacramento/San Francisco
+1 916 321 4818
mscott@kslaw.com

Richard Sharpe
Singapore
+65 6303 6079
rsharpe@kslaw.com

Kyle Sheahen
New York
+1 212 556 2234
ksheahen@kslaw.com

Michael Shepard
San Francisco
+1 415 318 1221
mshepard@kslaw.com

Thomas Spulak
Miami
+1 305 462 6023
tspulak@kslaw.com

Aaron Stephens
London
+44 20 7551 2179
astephens@kslaw.com

Cliff Stricklin
Denver
+1 720 535 2327
cstricklin@kslaw.com

Jean Tamalet
Paris
+33 1 7300 3987
jtamalet@kslaw.com

Courtney D. Trombly
Washington, DC
+1 202 626 2935
ctrombly@kslaw.com

Rick Vacura
Northern Virginia
+1 703 245 1018
rvacura@kslaw.com

Anthony A. Williams
Washington, DC
+1 202 626 3730
awilliams@kslaw.com

David K. Willingham
Los Angeles
+1 213 218 4005
dwillingham@kslaw.com

David Wulfert
Washington, DC
+1 202 626 5570
dwulfert@kslaw.com

Sally Q. Yates
Atlanta/Washington, DC
+1 404 572 2723
syates@kslaw.com

Joseph Zales
New York
+1 212 827 4087
jzales@kslaw.com

[i] Alleged failures in this case, which were denied by contractor and contractor's parent company, included a failure to timely scan for and remediate known vulnerabilities on contractor's network and systems; ignoring reports of numerous cybersecurity risks raised by third party auditors and contractor's internal audit department. The settlement agreement did not contain an admission of fault by either contractor or contractors' parent company.