Hogan Lovells

Aerospace & Defense Insights

DOJ's civil cyber-fraud initiative intensifies scrutiny of cybersecurity practices

Stacy Hadeka, Paul Otto, Michael Scheimer, Michael Mason, Peter Marta, Jonathan Diesenhaus, Michael Theis, and Rebecca Umhoffer

Through Aerospace & Defense Insights, we share with you the top legal and political issues affecting the aerospace and defense (A&D) industry. Our A&D industry team monitors the latest developments to help our clients stay in front of issues before they become problems, and seize opportunities in a timely manner.

On 6 October 2021 Deputy Attorney General Lisa Monaco announced a "Civil Cyber-Fraud Initiative," through which the Department of Justice (DOJ) will use the False Claims Act (FCA) to target cybersecurity related fraud by government contractors and grant recipients.

The stated goals of the initiative include holding entities and individuals accountable for:

- 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.

This initiative follows the 2020 SolarWinds supply chain cyberattack, which impacted multiple federal agencies and is part of a department-wide comprehensive cyber review ordered by Monaco in May. Monaco has also called for federal legislation to establish a national standard for reporting significant cyber incidents that affect critical infrastructure and their supply chains, including ransomware. The DOJ's actions accompany several other government efforts, including Executive Order (EO) 14028 issued 12 May 2021, to improve the nation's cybersecurity and specifically to harden the government's information technology (IT) supply chain.

The initiative itself does not impose new regulatory or legal requirements, but it signals a new focus and prioritization of resources by DOJ to improve cybersecurity across the government, the public sector, and at key "industry partners." The initiative also expressly aims to secure FCA recoveries to reimburse the government and taxpayers for losses incurred "when companies fail to satisfy their cybersecurity obligations." Aerospace & Defense (A&D) companies, and other government contractors, should expect increased scrutiny of their compliance with cybersecurity requirements and an increase in FCA complaints on the horizon.

Who is looking over your shoulder with more focus than ever?

Several recent, headline-grabbing FCA claims against government contractors have been based on an alleged failure to comply with contract and regulatory cybersecurity requirements or on alleged misrepresentation of such compliance. The DOJ settled its first such case in 2019.[1] That suit, like the majority of FCA claims, was initiated by a whistleblower. Moreover, there has been other FCA litigation alleging false certification of compliance with applicable cybersecurity requirements, which has also put A&D companies and other government contractors on notice that the threat of FCA litigation for non-compliance with cybersecurity measures is real.[2]

Although A&D companies have long been a prime target for FCA whistleblowers, this new DOJ initiative may increase scrutiny of cybersecurity-related practices of A&D companies.[3] First, the initiative suggests the DOJ may be more prone to intervene in such cases in the future, and this fact may incentivize more whistleblowers to come forward. It may also cause some would-be whistleblowers to more closely examine companies' cybersecurity obligations and practices. In addition, the initiative could draw government scrutiny not just from DOJ, but also from inspectors general at numerous government agencies. In response to this initiative, those agencies could choose to audit or otherwise examine the cyber practices of their contractors and grant recipients, and potentially refer cases to DOJ based on their findings.

What cybersecurity obligations could give rise to a claim?

A&D companies are frequent targets for cyberattacks due to their propensity to store sensitive technical data as well as other high-value government information. In recognition of this fact, the federal government has imposed a framework of cybersecurity requirements that typically requires A&D companies to make substantial investments in infrastructure that meets certain data safeguarding standards.

Although FCA claims relating to cybersecurity obligations could take many forms, two recently modified regulatory requirements are noteworthy.

First, in addition to the safeguarding and cyber incident reporting requirements in Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012, the Department of Defense (DoD) now requires contractors (through DFARS 252.204-7020) to complete a pre-award assessment of their compliance with cybersecurity controls identified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171.[4] This self-assessment is referred to as a "Basic Assessment." It results in a numerical score and must also identify a date by which the contractor will be fully compliant with NIST SP 800-171. Should the validity of a contractor's self-assessment be later questioned, a whistleblower could claim that false or reckless representations made in the self-assessment caused false claims to be made.

Significantly, a Basic Assessment may be followed by a government-led assessment—either a "Medium Assessment" or a "High Assessment"—after award. This could lead to disagreements about the degree to which the contractor is compliant with NIST SP 800-171, and such disagreements could give rise to FCA allegations.

Finally, the DoD anticipates eventually moving toward a system that will require defense contractors to obtain Cybersecurity Maturity Model Certification (CMMC) from an accredited third party. When such certification begins, it is also possible that third party certifiers may uncover inconsistencies between their own assessment of the contractor's security controls and the contractor's earlier Basic Assessment. Whistleblowers could point to such inconsistencies to allege a contractor caused false claims to be made by misrepresenting its security controls in order to win the contract.

1. Joseph Marks, Cisco to Pay US$8.6 Million Fine for Selling Government Hackable Surveillance Technology, Wash. Post (31 July 2019) available here.
2. *See, e.g., United States ex rel. Adams v. Dell Computer Corp.*, No. 15-CV-608 (TFH), 2020 WL 5970677 (D.C. Cir. 8 Oct. 2020); *United States v. Aerojet Rocketdyne Holdings, Inc.*, 381 F. Supp. 3d 1240 (E.D. Cal. 2019).
3. *See* DOJ expects whistleblowers to play 'significant role' in False Claims Act cases against contractors, FEDScoop (13 Oct. 2021), https://www.fedscoop.com/doj-expects-whistleblowers-to-play-significant-role-in-false-claims-act-cases-against-contractors/.
4. NIST SP 800-171 Rev. 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations (Feb. 2020), available here.

The above DFARS clauses apply only to Controlled Unclassified Information (CUI) within the DoD supply chain. However, numerous government contracts contain contract-specific cybersecurity requirements, and noncompliance with these requirements could also give rise to FCA claims. Furthermore, the Federal Acquisition Regulation (FAR), AR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems, requires all contractors and subcontractors to apply specified safeguarding requirements when processing, storing, or transmitting Federal Contract Information (FCI) in or from covered contractor information systems. We have previously written about these requirements here.

Finally, we expect additional government-wide cybersecurity standards and reporting requirements to be issued pursuant to EO 14028. New cybersecurity standards and reporting requirements will increase the avenues for potential FCA claims. In addition, there is new legislation and regulation actively under consideration across the government that would impose new or heightened mandatory cyber reporting requirements, which create further avenues for the government to learn of cyber incidents.

Subcontractors must also take note

The FCA not only imposes liability on a prime contractor or direct grant recipient, but it applies to any entity, including subcontractors, whose conduct induces the government to pay a false claim. Thus, although prime contractors or grant recipients typically submit direct claims for payment to the government on behalf of their subcontractors, a subcontractor that causes a prime contractor or recipient to present a false claim for payment can become subject to FCA liability.[5]

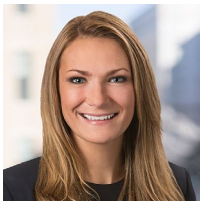
What's next

The Supreme Court has noted that the FCA is not a "vehicle for punishing garden-variety breaches of contract or regulatory violations."[6] It remains to be seen, however, to what degree FCA claims that allege a failure to comply with fast-developing cybersecurity requirements will be successful. For example, if general post-cyberattack litigation and regulatory enforcement is any guide, whistleblowers and the government may seek to use the fact of an incident or breach as evidence that cybersecurity measures were insufficient or non-compliant.

A key factor will likely be whether the specific requirement at issue in any given case is deemed "material." The Supreme Court has emphasized that the materiality requirement is "demanding" and "rigorous."[7] The government's intent to bolster security of its IT supply chain is clear, but federal contracts and grants can include dozens of regulatory requirements, and strict compliance with any single one may not be deemed material in every case. In addition, any lack of clarity in new regulations could protect contractors who make a good faith effort at compliance because the FCA also requires a knowing falsehood.

Despite questions about the strength of future FCA claims based on alleged non-compliance with cybersecurity requirements, companies that contract with the government or receive grants should carefully track fast-evolving cybersecurity rules and regulations and prioritize related compliance efforts.

5. *See e.g., United States v. Bornstein*, 423 U.S. 303, 309 (1976) ("It is settled that the [False Claims] Act ... gives the United States a cause of action against a subcontractor who causes a prime contractor to submit a false claim to the Government."); *United States ex rel. Keaveney v. SRA International, Inc.*, 219 F.Supp.3d 129 (D.D.C. 2016) citing Toyobo, 811 F.Supp.2d 37, 45 (D.D.C. 2011) (A subcontractor may be liable under the statute "even when it did not itself present any false claims to the government if it engaged in a fraudulent scheme that induced the government to pay claims submitted by the contractor."); *United States v. Honeywell Int'l Inc.*, 798 F. Supp. 2d 12, 24 (D.D.C. 2011) (A subcontractor may be liable for causing false claims to be submitted under the FCA "if the subcontractor submits a false statement to the prime contractor intending for the statement to be used by the prime contractor to get the government to pay its claim.").
6. *Universal Health Services., Inc. v. United States*, 136 S. Ct. 1989, 2003 (2016).
7. *Universal Health Services, Inc. v. United States* ex rel. Escobar, 136 S. Ct. 1989, 2003, 2004 n.6 (2016)



Stacy Hadeka
Senior Associate | Washington, D.C.
T: +1 202 637 3678
E: stacy.hadeka@hoganlovells.com

Paul Otto
Partner | Washington, D.C.
T: +1 202 637 5887
E: paul.otto@hoganlovells.com

Michael Scheimer
Counsel | Washington, D.C.
T: +1 202 637 6584
E: michael.scheimer@hoganlovells.com

Michael Mason
Partner | Washington, D.C.
T: +1 202 637 5499
E: mike.mason@hoganlovells.com

Peter Marta
Partner | New York
T: +1 212 918 3528
E: peter.marta@hoganlovells.com

Jonathan Diesenhaus
Partner | Washington, D.C.
T: +1 202 637 5416
E: jonathan.diesenhaus@hoganlovells.com

Michael Theis
Partner | Denver
T: +1 303 899 7327
E: michael.theis@hoganlovells.com

Rebecca Umhofer
Senior Knowledge Lawyer | Washington, D.C.
T: +1 202 637 6938
E: rebecca.umhofer@hoganlovells.com

Alicante
Amsterdam
Baltimore
Beijing
Birmingham
Boston
Brussels
Budapest*
Colorado Springs
Denver
Dubai
Dublin
Dusseldorf
Frankfurt
Hamburg
Hanoi
Ho Chi Minh City
Hong Kong
Houston
Jakarta*
Johannesburg
London
Los Angeles
Louisville
Luxembourg
Madrid
Mexico City
Miami
Milan
Minneapolis
Monterrey
Moscow
Munich
New York
Northern Virginia
Paris
Perth
Philadelphia
Riyadh*
Rome
San Francisco
São Paulo
Shanghai
Shanghai FTZ*
Silicon Valley
Singapore
Sydney
Tokyo
Ulaanbaatar*
Warsaw
Washington, D.C.

*Our associated offices
Legal Services Center: Berlin

www.hoganlovells.com