Investigations, Compliance, and Defense
Government Contracts
Data Privacy and Cybersecurity

New Civil Cyber-Fraud Initiative Uses False Claims Act to Enforce Cybersecurity Requirements

By: Moshe Broder, David Bitkower, Brandon D. Fox, Shoba Pillay, and David B. Robbins

The Department of Justice (DOJ) announced yesterday a new Civil Cyber-Fraud initiative which will use the False Claims Act (FCA) to enforce government contract cybersecurity requirements. The initiative will be led by the Fraud Section of the DOJ Civil Division's Commercial Litigation Branch. DOJ believes it can bring its experience and resources from its civil fraud enforcement, procurement, and cybersecurity focused attorneys to make this a successful initiative.

In remarks coinciding with the launch of this initiative, Deputy Attorney General Lisa Monaco emphasized that DOJ will seek to impose "very hefty fines" on contractors or grant recipients who fail to comply with their obligations under cybersecurity standards. For example, while contractors are required to "rapidly report" (defined as reporting within 72 hours) "cyber incidents" to the Department of Defense under Defense Federal Acquisition Regulation Supplement 252.204-7012, Monaco suggested that contractors are falling short in meeting those reporting requirements. In particular, she stated that "[f]or too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and to report it. Well that changes today."

Although enforcement practices and other details of this initiative remain to be seen, DOJ described the focus of the enforcement efforts as seeking to "hold accountable entities or individuals that put U.S. information or systems at risk." DOJ said it would target those: (1) providing deficient cybersecurity products or services, (2) misrepresenting their cybersecurity practices or protocols, or (3) violating obligations to monitor and report cybersecurity incidents and breaches. DOJ also noted the applicability of the FCA's whistleblower protection provision, highlighting the risk to contractors from qui tam suits alleging noncompliance with cybersecurity requirements. This announcement comes during a surge in FCA and other procurement fraud investigations, as we previously reported here.

The DOJ initiative also comes at a time when government contractor cybersecurity compliance and enforcement remains a high priority due to increasing cyber threats, including ransomware and other sophisticated attacks. Through standard government contract clauses implemented by an Interim Rule issued in September 2020,[1] many Department of Defense (DoD) contractors are required to perform a "Basic Assessment" of their implementation of National Institute of Standards and Technology controls for protecting controlled unclassified information.[2] Performing a Basic Assessment (and submitting a score to the Supplier Performance Risk System) can be a condition for contract award, exercise of an option period, and/or extending a contract's period of performance.

The same Interim Rule introduced another standard government contracts clause[3] that is intended to incorporate Cybersecurity Maturity Model Certification (CMMC) requirements into contracts. CMMC represents a paradigm shift from permitting self-attestation of compliance with contractual cybersecurity requirements to requiring third-party certification as a condition of contract award. CMMC requirements have not yet been rolled out in solicitations and contracts, and media reports indicate that the CMMC initiative is undergoing a programmatic review with a range of possible changes under consideration.

Taken together, however, the CMMC initiative reflects DoD's push toward requiring widespread compliance with minimum cybersecurity standards, while DOJ's Civil Cyber-Fraud initiative signals increasing enforcement resources directed at government contractors who knowingly misrepresent their cybersecurity practices or fail to monitor and report cyber incidents.

The new Initiative has the potential to carry significant risk for government contractors. First and foremost, understanding the scope of a cyber attack and determining whether reporting obligations have been triggered within the 72 hour rapid reporting period can be challenging and may require close coordination with forensic investigators and counsel. Second, DOJ has announced that the fact (and presumably the completeness of) the reporting will be subject to FCA enforcement. More than ever, government contractors should ensure they understand their contractual cybersecurity requirements, and the representations they are making about their compliance with those requirements. Contractors should also consider conducting tabletop exercises that game out how to respond to a cyber attack and ensure their internal policies, including timely reporting pursuant to federal regulations, are up to date.

Jenner & Block will continue to monitor these and other cybersecurity developments impacting government contractors. If you have any questions, please feel free to contact: Moshe Broder, David Bitkower, Brandon D. Fox, Shoba Pillay, or David B. Robbins.

---

[1] DFARS 252.204-7019 and DFARS 252.204-7020. *See* 85 Fed Reg. 61505 (Sept. 29, 2020), *available at* https://www.federalregister.gov/documents/2020/09/29/2020-21123/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of.

[2] NIST Special Publication ("SP") 800-171.

[3] DFARS 252.204-7021.

Contact Us

Moshe Broder

mbroder@jenner.com | Download V-Card

David Bitkower

dbitkower@jenner.com | Download V-Card

Brandon D. Fox

bfox@jenner.com | Download V-Card

Shoba Pillay

spillay@jenner.com | Download V-Card

David B. Robbins

drobbins@jenner.com | Download V-Card

Meet Our Investigations, Compliance, and Defense Team

Meet Our Government Contracts Team

Meet Our Data Privacy and Cybersecurity Team

Practice Leaders

Anthony S. Barkow
Investigations, Compliance, and Defense Co-Chair
abarkow@jenner.com
Download V-Card

Christine Braamskamp
Investigations, Compliance, and Defense Co-Chair
cbraamskamp@jenner.com
Download V-Card

Brandon D. Fox
Investigations, Compliance, and Defense Co-Chair
bfox@jenner.com
Download V-Card

Erin R. Schrantz
Investigations, Compliance, and Defense Co-Chair
eschrantz@jenner.com
Download V-Card

David Bitkower
Investigations, Compliance, and Defense and Data Privacy and Cybersecurity Co-Chair
dbitkower@jenner.com
Download V-Card

Madeleine V. Findley
Data Privacy and Cybersecurity Co-Chair
mfindley@jenner.com
Download V-Card

Marc A. Van Allen
Government Contracts Co-Chair
mvanallen@jenner.com
Download V-Card

David B. Robbins
Government Contracts Co-Chair
drobbins@jenner.com
Download V-Card