BLANKROME
CELEBRATING 75 YEARS

Privacy, Security & Data Protection and Government Contracts

OCTOBER 2021 • NO. 2

Department of Justice to Prioritize Cybersecurity Fraud through New Civil Cyber-Fraud Initiative

On October 6, 2021, the U.S. Department of Justice ("DOJ") announced a new Civil Cyber-Fraud Initiative to pursue cybersecurity fraud matters using the enforcement mechanisms of the False Claims Act ("FCA").

This initiative follows DOJ's four-month effort to review its cybersecurity strategy and reflects the government's increased focus on contractor data security. Led by the Civil Division's Commercial Litigation Branch, Fraud Section—*i.e.,* the DOJ Section responsible for investigating and litigating FCA matters—the initiative targets government contractors and grant recipients that "put U.S. information or systems at risk" by "knowingly":

- providing deficient cybersecurity products or services;
- misrepresenting the company's cybersecurity practices or protocols; or
- violating their obligations to monitor and report cybersecurity incidents and breaches.

We discuss below the cybersecurity landscape preceding the new initiative, possible impacts and focus areas of the initiative, and how contractors should prepare for potential enforcement.

1. The Recent Increase in FCA Cybersecurity Enforcement

DOJ's initiative is an outgrowth of the government's objective to enhance cybersecurity in light of some of the well-publicized data compromises (*e.g.,* SolarWinds) to both government agency and contractor systems resulting from the actions of foreign adversaries and other bad actors. The Department of Defense ("DOD") estimates an annual loss of over $600 billion due to these cyberattacks, underscoring the importance of increasing security.

DOJ's Deputy Assistant Attorney Michael Granston predicted in December 2020 that "cybersecurity related fraud" was an "area where we could see enhanced False Claims Act activity." A number of recent cases also foreshadow the FCA as a key tool in enforcing cybersecurity compliance:

- In 2019, a California federal district court suggested that noncompliance with DOD cybersecurity requirements in DFARS 252.204-7012 may form the basis of an actionable FCA claim. The court refused to dismiss a complaint alleging that a contractor had entered contracts with the government despite knowing it did not meet minimum cybersecurity standards. *See United States ex rel. Markus v. Aerojet Rocketdyne Hldgs., Inc.,* 381 F. Supp. 3d 1240 (E.D. Cal. 2019).

- That same year, Cisco Systems settled an FCA suit for $8.6 million to resolve allegations that its video surveillance software contained security vulnerabilities potentially allowing a third party to manipulate security cameras and recorded footage. *U.S. ex rel. Glenn v. Cisco Systems, Inc.,* No. 1:11-cv-00400 (W.D.N.Y. 2019).

- More recently, the D.C. federal district court dismissed a relator's *qui tam* suit alleging Dell Computer sold millions of dollars of computer systems to the government with undisclosed security vulnerabilities. The court held that the alleged vulnerabilities were not material under the FCA because the government's cybersecurity policies did not require defect-free products, but rather systems with limited vulnerabilities. *United States ex rel. Adams v. Dell Computer Corp.,* 496 F. Supp. 3d 91 (D.D.C. Oct. 8, 2020).

Parallel with these FCA cases, the federal government has been actively developing new cyber standards and regulations, many of which are yet to be finalized. On May 12, 2021, President Biden cut to the chase in issuing Executive Order 14028, "Improving the Nation's Cybersecurity" (discussed here) ("EO"). The EO contains aggressive timelines for sweeping cybersecurity changes intended to bolster agency and contractor practices, with a focus on cyber reporting obligations, improving the security and integrity of "critical" software, and standardizing cybersecurity contractual requirements. The EO also dictates revisions to the Federal Acquisition Regulation ("FAR") to require civilian contractors to promptly report cyber incidents.

Congress has also jumped into the fray. Legislation introduced in both the Senate and House would require ransomware victims to report payments to hackers within 48 hours of payment.

DOD, which has had cyber reporting regulations in place for a number of years, continues to work toward rolling out its Cybersecurity Maturity Model Certification ("CMMC"), which implements a tiered system for evaluating and certifying a contractor's systems against a rigorous set of cybersecurity criteria based on the National Institute of Standards and Technology ("NIST") 800-171.

2. DOJ's Cyber-Fraud Initiative

As contractors become subject to an increasing body of cyber standards, DOJ's cyber-fraud initiative seeks to target contractors who fall short of the minimum regulatory or contractual requirements. In announcing the initiative, U.S. Deputy Attorney General Monaco explained that, "For 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 report it. Well that changes today…[W]e will use our civil enforcement tools to pursue companies…[when they fail to follow required cybersecurity standards—because we know that puts all of us at risk."

The initiative anticipates close coordination between DOJ and other federal agencies, subject matter experts, and law enforcement partners. The initiative's stated goals are to build resiliency against cybersecurity intrusions; hold contractors and grantees to their commitments to protect government information and infrastructure; ensure companies "follow the rules" by investing in cybersecurity; and improve overall cybersecurity practices.

3. Potential Risk Areas in Cybersecurity

As DOJ gears up for cybersecurity fraud enforcement, government contractors should be aware of the following areas of potential risk—and the still-outstanding question on whether cybersecurity noncompliance can give rise to FCA liability:

- **Reporting failures:** DOJ's announcement suggests that it will pay particular attention to companies that fail to fully and timely report cyber incidents. For DOD contractors, the existing DFARS clause requires reporting of cyber incidents within 72 hours of "discovery," potentially raising questions about *when* a contractor knew or should have known about a breach. Contractors should also be sure that any disclosures or certifications made to the government are accurate, complete, and not misleading by omission. The *Aerodyne* decision from 2019 suggests that FCA liability could attach if a contractor does not fully disclose all relevant facts.

- **Contractor basic assessments:** As of October 2020, DOD contractors must complete a pre-award self-assessment of their compliance with NIST 800-171. A failure to properly assess relevant systems could result in an inflated self-assessment score. An erroneous or misleading self-assessment could become evident through a government review or when that contractor can achieve only a low CMMC level.

- **Increase in whistleblower lawsuits:** As the government embraces the FCA as a tool to combat cybersecurity fraud, contractors should expect an increase in *qui tam* suits—particularly by employees involved in the company's information technology.

- **Overlap with supply chain requirements:** Cybersecurity fraud cases may also implicate recent supply chain bans, including the Section 889 ban on covered Chinese telecommunications equipment (discussed here, here, and here). Section 889 is intended to rid the supply chain of Chinese technologies used as a back door to infiltrate contractor systems. Contractors must certify that they do not sell or use these covered equipment/services, and an inaccurate certification could subject a contractor to FCA liability.

- **Outstanding questions of materiality:** Though DOJ has clearly made cybersecurity compliance a priority for its investigation and enforcement efforts, one challenge that the government (and whistleblowers) will need to address is whether a contractor's compliance in any particular circumstance was *material* to the government's payment decision. As the Court noted in the *Dell* case, compliance does not necessarily mean "defect-free products," suggesting certain gaps or imperfections in a company's cybersecurity structure may not necessarily impart FCA liability.

- **Evolving cybersecurity standards and requirements:** Both the government and contractors will need to be aware of and track legislative, regulatory, and contractual cybersecurity standards as they develop and change on the federal and state levels. As the pace of government requirements and oversight activity increases, contractors face the danger that DOJ and whistleblowers will evaluate yesterday's conduct by current standards. By the same token, in this environment, contractors cannot afford to rest on their laurels and assume that compliance yesterday assures them of compliance tomorrow. As the proposed CMMC framework suggests, companies should be working towards systems of controls that are "mature" enough to respond, adapt to, and anticipate where possible the ever-changing methods of cyberattacks and threats.

As always, a government contractor's best defense to an FCA enforcement action is to actively and affirmatively assess and address its compliance obligations. In the context of cybersecurity, a company's ability to establish secure, compliant systems will not only help it defend its own business and safeguard any government data that may be in play, but could protect the company from time-consuming and often costly enforcement actions.

For additional information, please contact:

PRIVACY, SECURITY & DATA PROTECTION

Sharon R. Klein
949.812.6010 | sharon.klein@blankrome.com

GOVERNMENT CONTRACTS

Jennifer A. Short
202.420.2698 | jennifer.short@blankrome.com

Robyn Burrows
202.420.2268 | robyn.burrows@blankrome.com