Updates
October 11, 2021

DOJ’s Civil Cyber-Fraud Initiative Highlights False Claims Act Cybersecurity Risks for Government Contractors

On October 6, 2021, the U.S. Department of Justice (DOJ) announced an initiative to pursue civil False Claims Act (FCA) enforcement actions against government contractors that knowingly fail to follow required cybersecurity standards and reporting requirements—the latest indication of the heightened risks of noncompliance with cybersecurity-related obligations for contractors.

According to Deputy Attorney General (AG) Lisa Monaco's announcement, the DOJ's new Civil Cyber-Fraud Initiative will combine the DOJ's expertise in civil fraud enforcement, government procurement, and cybersecurity "to combat new and emerging cyber threats to the security of sensitive information and critical systems." Under the initiative, the DOJ will utilize the FCA—the government's primary remedy to redress fraud against the government—to "hold accountable" entities or individuals that put U.S. information or systems at risk by knowingly (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.

The DOJ's initiative comes amid a flurry of regulatory and legislative activity related to cybersecurity and government supply chain risks. Agencies are in the process of implementing President Biden's broad May 12, 2021, *Executive Order on Improving the Nation's Cybersecurity* (EO 14028), which calls for new requirements for information technology contractors to share information about potential cyber threats, among other things. Meanwhile, the U.S. Department of Defense (DoD) is conducting a review of its Cybersecurity Maturity Model Certification (CMMC) program, whereby nearly all defense contractors will have to undergo third-party assessments and certifications of their compliance as a condition of receiving a contract.

This update provides an overview of DOJ's initiative, which highlights the role of the FCA in prosecuting companies and individuals that knowingly violate cybersecurity requirements.

CMMC and Other Cybersecurity Developments

Under the basic safeguarding clause set forth at Federal Acquisition Regulation (FAR) 52.204-21, contractors are required to apply basic requirements and procedures to protect their information systems that process nonpublic but unclassified contract information against cyber intrusions. Defense contractors are subject to additional requirements under Defense FAR Supplement (DFARS) clauses 252.204-7012, -7019, -7020, and -7021. Defense contractors that receive or process so-called covered defense information are required to implement, at a minimum, the 110 cybersecurity controls set forth in the National Institute of Standards and Technology's (NIST) Special Publication (SP) 800-171. They also must report certain cyber incidents to the DoD within 72 hours. And under an interim rule that took effect in September 2020, defense contractors must carry out Basic Assessments of their compliance with NIST SP 800-171 and submit their scores to the DoD as a condition of receiving a defense contract, and also can be subject to Medium and High Assessments of compliance performed by the DoD. The interim rule also provides for CMMC to be rolled out to nearly all contractors (there is a narrow exception for commercial off-the-shelf suppliers) gradually until October 2025.

Recent cyber-related attacks such as the SolarWinds incident have generated a flurry of government activity focused on protecting unclassified government information in the possession of government contractors and their suppliers against increasingly sophisticated cyber threats. Several regulatory efforts are underway. Under EO 14028, contractors should expect new requirements to be issued in the coming year in areas such as cyber threat information-sharing and software security (see our analysis of the EO here). The DoD has been reviewing CMMC, with the open issues including the program's impact on small businesses.

Congress is also examining legislation to tighten cyber reporting requirements. The Cyber Incident Notification Act of 2021, introduced in July 2021, would require contractors to report breaches of their systems within 24 hours of discovery, while also providing them immunity. Under the Ransomware Disclosure Act, introduced on October 5, 2021, victims of ransomware attacks would have to report payments made to hackers to the government within 48 hours.

DOJ's Civil Cyber-Fraud Initiative

The DOJ's Civil Cyber-Fraud Initiative underscores the role that enforcement of the FCA will play in this evolving regulatory and enforcement landscape. The FCA prohibits, among other things, the knowing submission of a false or fraudulent claim for payment to the government. FCA cases can be initiated by *qui tam* whistleblowers (relators) seeking a portion of any recovery as well as by the government on its own. The statute imposes treble damages and penalties on violators. Liability under the FCA can be premised upon an express or implied false certification of compliance with a material statutory, regulatory, or contractual obligation.

There have been signs in recent years that cybersecurity is an area for potential FCA investigations and litigation, including *qui tam* cases brought by whistleblowers. During public remarks in February 2021, Bryan Boynton, Acting Assistant Attorney General of DOJ's Civil Division, described cybersecurity-related fraud as an area of potentially "enhanced False Claims Act activity," citing the growing threat of cyberattacks.

According to the DOJ, its Civil Cyber-Fraud Initiative will be led by the Civil Division's Commercial Litigation Branch, Fraud Section. The initiative is a result of the DOJ's ongoing comprehensive cyber review ordered by Deputy AG Monaco.

In announcing the DOJ's initiative during the Aspen Institute Cyber Summit on October 6, 2021, Deputy AG Monaco reportedly stated: "For too long, companies have chosen silence under the mistaken belief that it's less risky to hide a breach than to bring it forward and report it." She added, "Well, that changes today." Deputy AG Monaco also reportedly stated that companies that "fail to follow required cybersecurity standards" will face "very hefty fines."

The DOJ's announcement cites numerous objectives, including building resiliency against cybersecurity intrusions across the government, the public sector, and key industry partners; holding contractors and grantees to their commitments to protect government infrastructure and information, and ensuring that companies that "follow the rules" related to cybersecurity are "not a competitive disadvantage." The DOJ will work on its initiative with other federal agencies, subject matter experts, and law enforcement partners, according to its announcement.

Takeaways

The DOJ's initiative makes clear that government contractors, grant recipients, as well as individuals may be exposed to potential enforcement under the FCA if they knowingly provide deficient cybersecurity products or services, misrepresent their compliance with cybersecurity requirements, or fail to monitor or report cyber incidents or breaches where required. Several practical issues can be considered.

- Having compliant cybersecurity policies and procedures in place is increasingly essential for government contractors. Companies should review and regularly update their cybersecurity controls, conduct gap analyses that identify areas requiring further actions, and be prepared to update their programs as new requirements are issued. Inattention to cybersecurity also threatens to put contractors at a competitive disadvantage.
- The DOJ's announcement specifically calls out the FCA's protections for whistleblowers against retaliation and encourages people to report cyber-related fraud to the DOJ. Having internal reporting requirements and ethics hotlines in place can help companies mitigate the risks of whistleblower suits and respond to complaints in a timely manner.
- The DOJ's initiative highlights the risks of failing to disclose cyber breaches where required. Although the legislative and regulatory changes are in a state of change, it appears that contractors will likely soon be required to disclose information to law enforcement agencies about potential cyber threats to their systems, and under tight timeframes. Companies should anticipate ultimately being subject to more stringent reporting rules.
- Contractors' representations to the government about the nature of their goods and services—and their compliance with material cybersecurity requirements—can present FCA risks if not properly handled. Defense contractors should be particularly attuned to such risks when submitting their Basic Assessments to the DoD reflecting the extent to which they have implemented controls under NIST SP 800-171. Inaccurate or unsubstantiated self-assessed scores could expose a company to potential FCA liability.
- Cybersecurity FCA cases will likely raise legal issues that have arisen in FCA cases in other contexts. One such issue is whether a particular cybersecurity requirement is material to the government's payment decision. Another issue is the role of guidance documents in FCA cases. In a July 1, 2021, memorandum, Attorney General Merrick Garland rescinded a 2018 DOJ policy memorandum, known as the Brand Memo, that restricted the role of agency guidance in FCA cases. AG Garland's memo offers principles for the DOJ to follow related to the use of guidance documents in enforcement actions.

Authors

Alexander O. Canizares

Partner
ACanizares@perkinscoie.com 202.654.1769

Richard W. Oehler

Partner
ROehler@perkinscoie.com 206.359.8419

Julia M. Fox

Counsel
JuliaFox@perkinscoie.com

Explore more in

Government Contracts White Collar & Investigations

Related insights

Update

Ninth Circuit Rejects Mass-Arbitration Rules, Backs California Class Actions

Update

CFPB Finalizes Proposed Open Banking Rule on Personal Financial Data Rights