WINSTON & STRAWN LLP

BLOG

DOJ Launches Civil Cyber-Fraud Initiative to Enforce Federal Contractors' Cyber Security Requirements

OCTOBER 20, 2021

The Biden Administration has signaled that it views national cybersecurity as an important enforcement priority. In May 2021, President Biden signed an Executive Order on Improving the Nation's Cybersecurity, stating that "the Federal Government must bring to bear the full scope of its authorities and resources to protect and secure its computer systems." That same month, Deputy AG Monaco ordered a comprehensive cyber review "aimed at developing actionable recommendations to enhance and expand the Justice Department's efforts against cyber threats." The Civil Cyber-Fraud Initiative arose out of that review.

On October 6, 2021, Deputy Attorney General Lisa O. Monaco announced a new Civil Cyber-Fraud Initiative, by which the Department of Justice (DOJ) will utilize the False Claims Act (FCA) as a tool to enforce cybersecurity standards required of federal contractors and grant recipients. Specifically, the DOJ will target companies and individuals who allegedly misrepresented their cybersecurity practices or protocols to win a federal contract or grant, or knowingly submitted claims to the government for payment while in violation of regulatory or contractual cybersecurity requirements.

The FCA allows the government to recover three times its damages plus penalties up to $23,607 *per claim* against persons who knowingly submit false claims for payment or knowingly make a false statement material to a false or fraudulent claim. The Act incentivizes private citizens to bring "qui tam" (i.e., whistleblower) lawsuits on behalf of the government by allowing the whistleblower to keep between 15% and 30% of the amount recovered by the government. A classic example of a false claim is where a contractor fraudulently requests payment from the government for goods or services it did not actually provide.

There are many sources of cybersecurity obligations for federal contractors, including statutes, agency regulations, and the contractor's written agreement(s) with the government. A contractor also faces potential FCA liability for falsely certifying that it complied with a legal or contractual obligation—even where it provided goods or services in accordance with the contract—if it can be shown that the noncompliance is material to the government's decision whether to pay the claim. The Supreme Court has recognized that false certifications may be express or implied: "the implied false certification theory can be a basis for liability . . . when the defendant submits a claim for payment that makes specific representations about the goods or services provided, but knowingly fails to disclose the defendant's noncompliance with a statutory, regulatory, or contractual requirement." Some courts have specifically

found that an alleged false certification of compliance with cybersecurity protocols required to do business with the government may form the basis for FCA liability.

In an October 13, 2021, speech at the Cybersecurity and Infrastructure Security Agency's National Cybersecurity Summit, Assistant Acting Attorney General for the DOJ Civil Division Brian Boynton described three types of knowing misconduct by federal contractors as "prime candidates" for FCA enforcement under the new initiative:

1. Noncompliance with cybersecurity standards required as a condition for payment under the contract (e.g., measures to protect governmental data or prohibitions on using components made in restricted foreign countries);
2. Misrepresentation of security controls or practices to secure a government contract; and
3. Failure to timely report suspected cybersecurity breaches or incidents.

Boynton stated that the DOJ had secured additional resources, including appointment of a supervisor within the DOJ's Civil Fraud Section to oversee the initiative. The DOJ has signaled that it is serious about using the FCA to act against federal contractors that have fallen short of cybersecurity requirements imposed as a condition for payment by the government. It is critical that federal contractors maintain robust compliance systems to swiftly detect and remediate—and, if necessary, timely report—any cybersecurity failures or breaches.

TIP: Companies that do business with the government—especially those who handle classified or other sensitive information and systems—should engage experienced counsel with expertise in cyber and data security issues to ensure they are aware of and complying with all applicable requirements.
3 Min Read

Author

Chase J. Cooper

Related Locations

Houston

Related Topics

Cyber Security

Related Capabilities

Privacy & Data Security

Government Investigations, Enforcement & Compliance

Government Program Fraud, False Claims Act & Qui Tam Litigation

Related Regions

North America

Related Professionals

Chase J. Cooper

This entry has been created for information and planning purposes. It is not intended to be, nor should it be substituted for, legal advice, which turns on specific facts.