Published on *The National Law Review* https://natlawreview.com

Cybersecurity Compliance on U.S. Government Contracts and Subcontracts

Article By:

Karen R. Harbaugh

Richard J. Gibbon

The U.S. Department of Justice announced late last year that it would utilize the False Claims Act, the U.S. government's primary civil tool to redress false claims for federal funds and property, to bring actions against U.S. government contractors and subcontractors who do not meet the cybersecurity requirements of a particular contract or grant. The U.S. Department of Justice (the "DoJ") certainly was not bluffing. In the past few months, DoJ has announced the settlement of two False Claims Act cases related to cybersecurity deficiencies or misrepresentations, and more are expected.

As such, it is now imperative that companies executing U.S. government contracts and subcontracts proactively assess their compliance with federal cybersecurity requirements.

DoJ's Cyber-Fraud Initiative

In October 2021, Deputy Attorney General Lisa O. Monaco announced the launch by the DoJ of a "Civil Cyber-Fraud Initiative," which she said would hold accountable individuals or entities that put U.S. information or systems at risk by 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. The Civil Cyber-Fraud Initiative would utilize the False Claims Act (the "FCA") to pursue cybersecurity-related cases against government contractors, subcontractors and grant recipients.

The False Claims Act

The FCA is the U.S. federal government's primary civil tool to combat fraud against the government.

It imposes liability on persons and companies (typically federal contractors and subcontractors) who defraud governmental programs, by either improperly receiving payments from, or improperly avoiding payments to, the U.S. federal government. The U.S. government has now recovered more than USD 70 billion under the FCA.

Enforcement Activity

In the past few months, DoJ has announced the settlement of two FCA cases related to cybersecurity deficiencies on the part of government contractors.

- On March 8, 2022, in DoJ's first resolution of an FCA case involving cybersecurity since the launch of the Civil Cyber-Fraud Initiative, DoJ announced that Comprehensive Health Services LLC ("CHS") had agreed to pay almost USD 1 million to resolve allegations that it violated the FCA by falsely representing to the U.S. Department of the State ("State") and the U.S. Air Force ("USAF") that it complied with contract requirements relating to the provision of medical services at State and USAF facilities in Iraq and Afghanistan. Among the violations, CHS, a provider of global medical services that contracted to provide medical support services at the facilities, had submitted claims to State for the cost of a secure electronic medical record ("EMR") system to store all patients' medical records, including the confidential identifying information of U.S. service members, diplomats, officials and contractors working and receiving medical care. However, CHS failed to disclose to State its inconsistent use of the secure EMR system over a seven-year period.

- Then on July 8, 2022, DoJ announced that Aerojet Rocketdyne Inc. ("Aerojet") had agreed to pay USD 9 million to resolve allegations that it violated the FCA by misrepresenting its compliance with cybersecurity requirements in certain federal government contracts requiring defense contractors to safeguard unclassified controlled technical information. Aerojet, which provides propulsion and power systems for launch vehicles, missiles and satellites and other space vehicles to the U.S. Department of Defense, the National Aeronautics and Space Administration ("NASA") and other federal agencies, was found to have induced the government to enter into contracts while knowing that it was not in compliance with Defense Federal Acquisition Regulation 48 C.F.R. § 252.204- 7012 (DFARS) and NASA Federal Acquisition Regulation 48 C.F.R. § 1852.204-76 (NASA FARS), which were both contractual preconditions. For example, one external audit determined that Aerojet was only compliant with 5 of the 59 required controls under DFARS, another identified high-risk deficiencies, while a third was able to penetrate Aerojet's network within a matter of hours.

Additional Considerations

These cases highlight the increased FCA risk that cybersecurity compliance poses for U.S. government contractors and subcontractors.

Importantly, liability need not turn on the government suffering a known loss of data but rather on whether the relevant contractor or subcontractor meets its full suite of contractual obligations to the government, including material cybersecurity requirements. Recklessly misrepresenting compliance to contracting agencies or deliberately agreeing to incorporate certain requirements into a contract but then failing to do so will give rise to liability under the FCA.

In addition to allowing the United States to pursue perpetrators of fraud on its own, the FCA allows private citizens or "relators" (in essence, whistleblowers), with knowledge of past or present frauds committed against the federal government, to file suits on behalf of the government (called *"qui tam"* suits), in return for the chance to participate in ensuing financial settlements. In fact, many of the DoJ Fraud Section's investigations and lawsuits arise from such *qui tam* actions.

Accordingly, contractors and subcontractors should engage with counsel to understand their cybersecurity obligations on existing and future U.S. government contracts and subcontracts, train employees, implement information security controls such as access and network restrictions, devise incident response plans and ransom strategies, and operationalize internal whistleblowing.

National Law Review, Volume XII, Number 262