DOJ Continues its Pursuit of Federal Contractors' Cybersecurity Compliance through the False Claims Act

Client Alert
10.3.2023

Celebrating its 20th year, October has been declared National Cybersecurity Awareness Month by the Cybersecurity & Infrastructure Security Agency (CISA).[1] Collaborative efforts by the federal government continue to follow threat actors and cybersecurity incidents, providing guidance to industry leaders on what they can do to avoid being the next big data breach or ransomware attack. Since the issuance of an October 28, 2020 joint cybersecurity alert ("2020 Joint Alert")[2] by CISA, the Federal Bureau of Investigation (FBI) and the Department of Health & Human Services (HHS), the FBI and other federal agencies have continued to provide Joint Alerts, Public Service Announcements (PSAs), Advisories and other guidance "to help cybersecurity professionals and system administrators' guard against the persistent malicious actions of cyber actors."[3] And, as recently as last week, the Government Accountability Office (GAO) issued a Cybersecurity Program Audit Guide, to aid analysts and auditors in evaluating agency cybersecurity programs.

In addition to the valuable resources mentioned above, the federal government has placed particular emphasis on the cybersecurity obligations of federal contractors. In that regard, on October 6, 2021, the Department of Justice (DOJ) announced its Civil Cyber-Fraud Initiative ("CCFI").[4] The CCFI established national cybersecurity as a key enforcement priority by, among other things, signaling to contractors that the False Claims Act ("FCA") would be used to target contractors that misrepresent compliance with the contractual requirements set out in the applicable cybersecurity contract clauses.

Indeed, shortly after rolling out the CCFI, on March 8, 2022, the DOJ announced its first settlement under the CCFI with Comprehensive Health Services, LLC, a medical service contractor to the Department of State ("DoS") and Air Force. The

Related People

Debra A. Geroux
Shareholder

Derek Mullins
Shareholder

Related Services

Cybersecurity and Privacy Specialty Team

CHS Settlement Agreement resolved two separate lawsuits, brought by private parties under the *qui tam* provisions of the FCA. The lawsuits alleged, among other things, that CHS, under an implied certification theory of relief, submitted or caused to be submitted claims for payment to the federal government, while at the same time, failing to disclose CHS's noncompliance with certain contractual obligations, including those requiring it to secure DoS medical records in HIPAA-compliant electronic medical records systems and violations of Federal Drug Administration regulations, including the provision of non-FDA approved medical supplies. While CHS did not admit liability, the cases were resolved for $930,000.

Shortly thereafter, the DOJ announced the second FCA resolution under the CCFI, in which federal contractor Aerojet Rocketdyne Inc. agreed to pay $9 million to resolve a *qui tam* FCA lawsuit brought by a former Aerojet employee that alleged Aerojet misrepresented its compliance with the contractual cybersecurity requirements set forth in the Defense Federal Acquisition Regulation Supplement (DFARS) and NASA-specific clauses contained in certain of its contracts. Of note, the primary DFARS clause at issue, which appears in many DoD contracts (and is required to be flowed down to subcontractors), requires contractors (and subcontractors) to safeguard unclassified "controlled technical information" and to protect the confidentiality, integrity and availability of agency information from unauthorized disclosure.[5]

Most recently, on September 5, 2023, the DOJ announced a third FCA Settlement Agreement pursuant to the CCFI with Verizon Business Network Services LLC. Unlike the two previous settlements that resulted from lawsuits brought by private *qui tam* plaintiffs, the Verizon settlement was the result of Verizon's self-disclosure of its noncompliance to the General Services Administration ("GSA"), regarding potential issues with its implementation and maintenance of required security controls with its Managed Trusted Internet Protocol Services ("MTIPS") utilized by various federal agencies, including the Critical Capabilities set forth in the Department of Homeland Security's Trusted Internet Connections Reference Architecture Document. Due to its self-disclosure of noncompliance and cooperation with the government's investigation, Verizon received credit by way of a reduced penalty enhancement in accordance with the DOJ's Guidelines for Taking Voluntary Disclosure, Cooperation, and Remediation into Account in False Claims Act Matters, Justice Manual § 4-4.112. Specifically, Verizon agreed to pay a total of $4,091,317, of which $2,727,545 was identified as actual restitution. Typically, the FCA imposes treble damages of 3 times the government's damages, or 2 times actual damages in the case of certain voluntary disclosures leading to a settlement.[6] However, the Verizon settlement shows only a 1.5x multiplier—a savings of more than $1.3 million. This reduction should incentivize government contractors to self-disclose instances of non-compliance early and take remedial actions to correct identified deficiencies.

The above settlements are a stark reminder to government contractors of their obligations to ensure the security of government information and the DOJ's focus on enforcing cybersecurity requirements as part of the CCFI. Government contractors should take note of the requirements governing their services to the federal government and ensure not only that they are in compliance upon award of their contracts, but remain compliant throughout the term of services.

Please contact the authors of this Alert or your Butzel attorney for more information.

Debra A. Geroux
248.258.2603
geroux@butzel.com

Derek Mullins
313.983.6944
mullins@butzel.com

[1] See Cybersecurity & Infrastructure Security Agency (CISA) National Cybersecurity Awareness Month (NCSAM), available at: https://www.cisa.gov/national-cyber-security-awareness-month

[2] CISA Alert (AA20-302A), *Ransomware Activity Targeting the Healthcare and Public Health Sector*, issued October 28, 2020 and available at: https://us-cert.cisa.gov/ncas/alerts/aa20-302a

[3] CISA *Stop Ransomware* Official Alerts and Statements available at: https://www.cisa.gov/stopransomware/official-alerts-statements-fbi

[4] Shortly after establishing the CCFI, President Biden signed into law the 2022 Cyber Incident Reporting for Critical Infrastructure Act of 2022 ("CIRCIA"), Pub. L. No. 17-103, 136 Stat. 1038 (2022), which will require certain Critical Infrastructure Covered Entities to notify CISA of cybersecurity incidents within 72 hours once enabling regulations are developed and issued. To date, regulations implementing CIRCIA have yet to be issued.

[5] DFARS 252.204-7012.

[6] 31 U.S.C. § 3729(a)(1)(G)–(a)(2).