BRACEWELL

INSIGHTS

DOJ to Federal Contractors: Report Cyberattacks or Face the False Claims Act

October 11, 2021

By: ***Robert J. Wagman Jr.***

The Department of Justice announced a new ***Civil Cyber-Fraud Initiative*** on October 6 – the latest move in a series of federal efforts to address the recent uptick in major cyberattacks. DOJ's Initiative aims to hold contractors and recipients to a higher standard by promising to aggressively enforce cybersecurity compliance—particularly reporting requirements—in federal contracts and grants by way of the False Claims Act's civil fraud and whistleblower provisions.[1]

Cybersecurity obligations for federal contractors stem from FAR 52.204-21, which applies to contracts where Federal contract information may reside in or transition through the contractor's or any tiered subcontractor's information systems. FAR 52.204-21 requires contractors to have in place certain minimum security controls to safeguard covered contractor information systems, including, but not limited to, limiting system access; exercising prudence in using external connections; verifying identities of users and devices; sanitizing media containing federal contract information; timely identifying, reporting, and correcting information and information system flaws; updating malware protection; and performing periodic scans.

Defense contractors are also subject to the enhanced obligations set forth in DFARS 252.204-7012, which establishes standards for system controls as well as a reporting requirement. Covered contractor information systems must comply with the standards listed in NIST SP 800-171, "Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations," in effect at the time the solicitation is issued. In the event of a cyber incident in which a contractor's information system, covered defense information, or the contractor's ability to perform critical duties under the contract are affected, contractors must "rapidly" report the incident to DoD and conduct a comprehensive review for evidence of compromise of covered defense information. Defense contractors are also subject to the additional verification requirements imposed by DoD's Cybersecurity Maturity Model Certification (CMMC) framework, released in January of this year, which builds on the requirements of DFARS 252.204-712.

Federal grant recipients have a lighter burden under 2 C.F.R. § 200.303(e), which requires only "reasonable measures" be taken to safeguard personally identifiable information or other sensitive information.

Under the new Civil Cyber-Fraud Initiative, failures to comply with the above requirements—in particular where the non-compliance is the result of an effort to conceal the occurrence of a cyber incident—will amount not to breach of contract, but to fraud against the government. Such violations are actionable under the False Claims Act by the government and by whistleblowers bringing suit under the Act's *qui tam* provision. In its October 6 press release, the Justice Department not only contemplates *qui tam* suits as a possible component of the Initiative — it actively encourages potential whistleblowers to take part in the Agency's enforcement efforts by reminding them of their right under the Act to share in the government's recovery if successful.

DOJ's Initiative is consistent with recent developments in the cybersecurity space suggesting an interest by the federal government in pushing more organizations towards mandatory reporting of cyberattacks. President Biden's ***May 12 executive order***, a response to the Colonial Pipeline and SolarWinds cyberattacks, mandates major updates to federal information systems and demanded that several agencies take action on the issue. The Senate Homeland Security Committee introduced the Cyber Incident Reporting Act in September, which would require governments, critical infrastructure operators, and businesses with 50 or more employees to report extortion payments as a result of ransomware attacks within 24 hours and for critical infrastructure companies to report cyberattacks to Homeland Security's Cybersecurity and Infrastructure Security Agency within 72 hours. Congress is currently considering combining the language of the Cyber Incident Reporting Act with a similar bill introduced earlier this year by the Senate Intelligence Committee and passing them as part of the annual National Defense Authorization Act, a move for which bipartisan support is expected. ***Recent enforcement actions out of the SEC*** and plans to update Agency guidance on the topic make clear that enforcement of cyber incidents is at the top of the Agency's agenda.

There have been several cases enforcing cybersecurity non-compliance through the False Claims Act. Even though the risks are not new, the DOJ's move formalizing the government's intent to enforce compliance through civil fraud remedies, especially reporting requirements, heightens considerations for all federal contractors and recipients moving forward. Those who do business with the government or receive federal funds will need to consider updating their prepared response materials, drill procedures, and other controls in place to contemplate mandatory reporting obligations that now have more teeth.

---

1. The cybersecurity framework applicable to recipients of federal funds is more cohesive, comprehensive, and onerous than the patchwork of disparate federal and state rules that currently governs private organizations not doing business with the government.