Bloomberg Law

The United States Law Week

INSIGHT: Defending Cybersecurity False Claims Act Allegations

By David Robbins, Jason Crawford, Kate Growley, and Michael Gruden Sept. 18, 2019

False Claims Act whistleblower lawsuits are being filed against government contractors for cybersecurity issues. Crowell & Moring attorneys lay out lessons from an FCA settlement involving Cisco Systems and offer tips for mitigating risk and defending FCA allegations.

President Abraham Lincoln signed the False Claims Act into law in 1863 to combat the sale of sick mules and shoddy uniforms to the Union Army. Who knew that in 2019, the law would be deployed on the cybersecurity battlefield.

A recent FCA settlement makes clear that government contractors have no choice but to understand FCA risks associated with cybersecurity noncompliance.

Cisco Systems recently agreed to pay $8.6 million to settle allegations that it violated the FCA by selling video surveillance systems to state and federal agencies that contained software flaws enabling those agencies to be hacked.

An employee of one of Cisco's resellers filed the whistleblower lawsuit in 2011 after discovering an alleged security weakness that could permit a cyber intruder to obtain administrative access to the software that managed video feeds. Although United States, ex rel. Glenn v. Cisco Sys. Inc. marks the first time a cybersecurity-related qui tam has resulted in a settlement or judgment (and the company makes clear there was no evidence the flaws were actually exploited), it is a likely harbinger of increased FCA activity in the years to come.

Given the FCA's specter of treble damages and penalties of $11,463 to $22,927 per claim, government contractors would be well-served to understand their cybersecurity obligations on federal contracts, as well as the potential liability for failure to comply.

The Growing FCA Risk

If a contractor falls short of cybersecurity requirements, but is paid under a contract containing FAR 52.204-21 or DFARS 252.204-7012, these clauses could provide a qui tam relator or the Department of Justice with a contractual hook to bring an FCA case.

In the aftermath of the Office of Personnel Management data breach, many civilian agencies are now also including contract clauses that are intended to safeguard personally identifiable information, providing more potential triggers for FCA liability.

FCA lawsuits alleging cybersecurity noncompliance are likely to be framed as "fraudulent inducement" causes of action or brought under the implied certification theory of liability that the Supreme Court recognized in *Universal Health Servs. Inc. v. U.S. ex rel. Escobar*. Under this theory, a contractor can face FCA liability if it bills the government with knowledge that the contractor is out of compliance with a statutory, regulatory, or contractual requirement that is material to the government's decision to pay a claim.

Determining whether compliance with a particular cybersecurity requirement is material to payment is a fact-dependent exercise that may depend, in part, on the nature of the goods or services that the contractor is providing. Also, from a technical perspective, there can be divergent views as to what is required under the notably vague "NIST SP 800-171" security controls that form the basis of many contractual requirements.

Moreover, the Department of Defense (DoD) has seemingly back-peddled regarding contractor compliance with the full suite of NIST SP 800-171 requirements. At an Industry Information Day held on June 23, 2017, to gather and respond to industry feedback regarding the DFARS 252.204-7012, DoD clarified what "implementation" required.

Specifically, the DoD announced that "implementation" of NIST SP 800-171, as required in the clause's text, may be done through completion of two documents known as a system security plan (SSP) and a plan of action and milestones (POAM). Further, contractors could document in their SSPs what security controls they had completed, and then document in their POAMs what controls still needed work.

Combined, these two documents would be sufficient to have "implemented" NIST SP 800-171 by the clause's Dec. 31, 2017, deadline, even if some security controls remained outstanding on that date. As such, the argument that the government has regularly excepted contractors from full compliance with the DFARS Safeguarding Rule may help establish that implementation of a particular control was not material to payment.

Mitigating Risk and Defending Against FCA Actions

Contractors should be prepared for the possibility that a disgruntled former employee or an enterprising hacker could seek to capitalize on a contractor's noncompliance with cybersecurity requirements.

There are, however, certain steps a contractor can take to mitigate against the risk of an FCA action based on noncompliance with cybersecurity requirements:

1. Document Compliance Efforts: Companies should document good faith efforts to meet the relevant requirements. Written plans and policies (including SSPs and POAMs) are important in that regard. Written policies and procedures (including an incident response plan) and training records will also help demonstrate the contractor's efforts at compliance.

2. Monitor Compliance and Address Gaps Quickly: Because cybersecurity standards are constantly evolving, contractors can benefit from internal compliance programs staffed with a cross-functional team that identifies compliance gaps and provides continuous feedback that a contractor can use to implement improvements. This helps demonstrate that the contractor did not act with deliberate ignorance or reckless disregard as to its cybersecurity noncompliance.

3. Listen to Internal Concerns: Notably, almost all of the cybersecurity FCA cases that have been unsealed to date were filed by former IT managers, computer security experts, or cybersecurity directors. This trend is not surprising considering that such employees are often in the best position to assess and understand a contractor's security weaknesses. This trend also underscores the importance of listening to internal concerns, addressing security gaps, and making clear to employees that the contractor understands its obligations under the DFARS 252.204-7012 and is making a good faith effort to comply with the NIST standards.

4. Disclose Noncompliance or Seek Exception: Where a contractor falls short of the relevant cybersecurity standards, POAM documentation can be helpful. Well-written POAMs clearly document the steps necessary to complete an outstanding control and the timelines in which those steps will be completed. That can put the government on notice of any alleged deficiency and, to the extent a contract is awarded anyway or no government objection is made, the contractor may have defenses to future FCA actions.

Separately, the DFARS 252.204-7012 contains language that permits contractors to proactively seek exceptions from or propose alternative measures that the DoD chief information officer can approve before a bid is made and a contract awarded. If the government was aware that a contractor was not fully compliant with the required controls but still paid the contractor, it will be a much tougher row to hoe for an FCA plaintiff to establish materiality.

This column does not necessarily reflect the opinion of The Bureau of National Affairs, Inc. or its owners.

Author Information

David Robbins is a partner in Crowell & Moring's Washington, D.C., office. He ran the U.S. Air Force's global Procurement Fraud Remedies Office and served, among other roles, as deputy general counsel (contractor responsibility). Robbins regularly conducts internal investigations, defends FCA cases, and provides general ethics and compliance advice to contractors of all sizes.

Jason Crawford practices in Crowell & Moring's Washington, D.C., office and has an active litigation and counseling practice focused on FCA litigation, government investigations, mandatory and voluntary disclosures to the government, and internal investigations. He is the co-host of the Let's Talk FCA podcast which covers legal and policy developments involving the FCA.

Kate Growley (CIPP/US, CIPP/G) is a counsel in Crowell & Moring's Washington, D.C., office. She is a member of the Steering Committee for the firm's Privacy & Cybersecurity Group, and her practice covers a wide range of information security counseling and litigation engagements, including cybersecurity compliance, incident response, regulatory investigations, and disputes surrounding data breaches and trade secrets.

Michael Gruden (CIPP/G) is an associate in Crowell & Moring's Washington, D.C., office where he is a member of the firm's Government Contracts and Privacy & Cybersecurity groups. He previously worked as a contracting officer at both the DoD and the Department of Homeland Security in the security sector and the information technology, research and development sector for nearly 15 years.