How Contractors Can Avoid Cybersecurity FCA Violations

By **Benjamin Powell, Elizabeth D'Aunno and Shannon Mercer** (September 27, 2022)

Benjamin Powell

Elizabeth D'Aunno

Shannon Mercer

Speaking about the U.S. Department of Justice's enforcement priorities on Sept. 12 at the American Bar Association's annual Civil False Claims Act and Qui Tam Enforcement Institute conference, the principal deputy assistant attorney general in the DOJ's Civil Division, Brian Boynton, provided important insights into the DOJ's investigation and prosecution of contractors for noncompliance with cybersecurity requirements.

Announced last October, the DOJ's Civil Cyber-Fraud Initiative seeks to hold contractors liable under the False Claims Act, or FCA, for

> 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.[1]

The DOJ has since announced two recoveries under the initiative.

One was in March involving allegations that Comprehensive Health Services LLC, a contractor operating in Iraq and Afghanistan, did not consistently store patient records exclusively on a secure electronic record system.[2]

The other was in July, involving allegations that Aerojet Rocketdyne Holdings Inc. misrepresented its compliance with cybersecurity requirements in certain federal government contracts.[3]

In his remarks on Sept. 12, Boynton confirmed that the DOJ has opened numerous other investigations into suspected cyber fraud. Some investigations were opened based on agency referrals and others arose from qui tam filings.

As investigations like these take time to develop, the full sweep of the Cyber-Fraud Initiative may only be felt in the coming months and years.

The Cyber-Fraud Initiative took pride of place as the first key enforcement priority discussed in Boynton's opening remarks at the FCA conference.

The DOJ doubled down on a key theme from the statement of interest it filed in United States ex rel. Markus v. Aerojet Rocketdyne Holdings Inc. last year,[4] asserting that the government is damaged when cybersecurity requirements are not followed, even when a contractor delivers a functional product that otherwise meets specifications, and regardless of whether there was a known loss of data or other cybersecurity breach.

In the DOJ's view, noncompliance with bargained for cybersecurity requirements, in and of itself, damages the U.S. Further, the DOJ asserted that a breach can diminish or even eliminate the value of a contractor's performance.

Such an exacting standard for cybersecurity compliance puts government contractors in a tough spot.

Cybersecurity requirements imposed on federal contractors are expensive and extremely difficult to meet. Defense contractors in particular may be targeted by sophisticated, evolving adversaries.

Even those with industry-leading cybersecurity compliance programs are likely to experience a significant cyber event. And when one inevitably occurs, even those that engage top-tier, third-party forensics providers may need weeks or months to fully investigate a cyber event, and the root cause of such event may never be uncovered.

Moreover, the enormous scale of operations can make it difficult, even impossible, to disclose certain cybersecurity compliance issues with specificity.

Of course, not every instance of cybersecurity noncompliance satisfies the elements of an FCA violation. There are many points contractors can marshal in defense of FCA claims, such as government payment of a particular claim in full despite its actual knowledge that certain requirements were violated.

But that may be cold comfort when there remains tremendous uncertainty as to what constitutes knowing provision of deficient cybersecurity products or services,[5] and merely responding to a government inquiry into potential fraud, even if the inquiry ultimately does not establish liability, can cost companies dearly — in legal fees, disruption to business operations and reputational damage with key government customers.

To be sure, contractors must abide by applicable regulations and agency requirements governing reporting of cyber incidents, including the timing and means of such reports.

For example, most U.S. Department of Defense contracts require contractors who discover a cyber incident that "affects a covered contractor information system or the covered defense information therein, or that affects the contractor's ability to perform the requirements of the contract that are designated as operationally critical support and identified in the contract," to rapidly report — within 72 hours of discovery — the incident to the DOD Cyber Crime Center.[6]

Contractors should also stay apprised of evolving regulations, particularly in light of heightened regulator attention to cybersecurity.

There are other steps contractors can take to help minimize the risk of cybersecurity noncompliance, aside from timely incident reporting.

Invest the resources needed to accomplish the company's cybersecurity plans of action and milestones.

Contractors should take care not to put goals in the plans of action and milestones, or POA&M, as defined by the National Institute of Standards and Technology, without intent and a reasonable plan to accomplish them.

They should also maintain oversight and accountability over progress toward POA&M goals. To this end, contractors should set clear leadership responsibilities and implement detection and escalation mechanisms.

Determine which cybersecurity requirements apply to the company's systems.

For example, contractors should consider whether the company is contractually or otherwise obligated to comply with specific agency requirements, or security requirements beyond NIST Special Publication (SP) 800-171, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, such as:

- FIPS 200, Minimum Security Requirements for Federal Information and Information Systems;
- NIST SP 800-37, Risk Management Framework for Information Systems and Organizations; or
- NIST 800-53, Security and Privacy Controls for Information Systems and Organizations.

Develop a cyber incident response plan and practice it regularly.

Incidents require urgent and immediate coordinated efforts to contain, remediate, investigate, and undertake regulatory and law enforcement communications and obligations.

A good cyber incident response plan will enable an organization to manage the multiple work streams necessary to responsibly handle a cyber incident, including data breaches.

Just as critical is the frequency and quality with which an organization practices executing its incident response plan. Tabletop exercises and other trainings help a company iterate on the plan and build capabilities among key players.

Conduct periodic risk assessments consistent with regulatory requirements and best practices.

Contractors should conduct regular network monitoring and penetration testing.

Take steps to ensure service provider and subcontractor cybersecurity.

Contractors should conduct due diligence on providers' cybersecurity, incorporate cybersecurity requirements into contracts and subcontracts, and follow up to confirm that providers are adhering to appropriate practices.

They should also undertake meaningful auditing and maintain careful record of disposition of audit findings, even those the company may consider relatively low risk, and ensure the auditing function is adequately resourced.

Establish a rapport with regulators and customers.

Contractors should brief regulators and customers on the company's cybersecurity systems, practices and compliance program.

They should also consider disclosing to the contracting officer the types of events that are regularly identified and redressed through the normal course of monitoring, and building a preexisting relationship can facilitate more productive dialogue if, and more likely when, a cyber event occurs.

Similarly, be responsive to employee reports or concerns.

Contractors should provide cybersecurity training to employees so they have the knowledge and means to constructively interpret and report cybersecurity concerns.

This includes setting up clear, well-advertised and well-monitored avenues for internal reporting of concerns, offering an anonymous reporting hotline and emphasizing the company's policy of nonretaliation. Contractors should also investigate and respond to internal reports in a timely manner.

Contractors should also ensure there is a feedback loop among privacy officers, those involved in information security, cybersecurity and incident response, and those with responsibility for ensuring compliance with the company's representations and certifications.

Conclusion

Time will tell what instances of cybersecurity noncompliance are more likely to come under government scrutiny, but the Cyber-Fraud Initiative settlements to date and Boynton's remarks on Sept. 12 underscore that the risk will not rise and fall exclusively on a breach or loss of data.

Contractors need to make decisions about cybersecurity compliance measures accordingly.

Benjamin A. Powell is a partner, Elizabeth D'Aunno is counsel and Shannon Togawa Mercer is a senior associate at WilmerHale.

[1] https://www.wilmerhale.com/en/insights/client-alerts/20211013-doj-launches-civil-cyber-fraud-initiative-to-use-the-false-claims-act [alternate cite: Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative, (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.]" target="_blank" rel="noopener noreferrer">https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative].

[2] Press Release, U.S. Dep't of Justice, Medical Services Contractor Pays $930,000 to Settle False Claims Act Allegations Relating to Medical Services Contracts at State Department and Air Force Facilities in Iraq and Afghanistan (Mar. 8, 2022), https://www.justice.gov/opa/pr/medical-services-contractor-pays-930000-settle-false-claims-act-allegations-relating-medical.

[3] https://www.wilmerhale.com/en/insights/blogs/WilmerHale-Privacy-and-Cybersecurity-Law/20220728-aerojet-rocketdyne-agrees-to-pay-9-million [alternate cite: https://www.justice.gov/opa/pr/aerojet-rocketdyne-agrees-pay-9-million-resolve-false-claims-act-allegations-cybersecurity.

[4] United States' Statement of Interest in Connection with Defendants' Summary Judgment

Motion, United States ex rel. Markus v. Aerojet RocketDyne Holdings, Inc., No. 2:15-cv-02245 (E.D. Cal. Oct. 20, 2021), Docket No. 135.

[5] See Press Release, U.S. Dep't of Justice, Deputy Attorney General Lisa O. Monaco Announces New Civil Cyber-Fraud Initiative, (Oct. 6, 2021), https://www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.

[6] DFARS 252.204-7012(a), (c).