Bracing For Rising Cyber-Related False Claims Act Scrutiny

By **Townsend Bourne and Nikole Snyder** (September 18, 2023)

Townsend Bourne

Nikole Snyder

In recent weeks, there has been an uptick in news of cyber-related False Claims Act activity. For example, on Sept. 1, the U.S. District Court for the Eastern District of Pennsylvania unsealed a qui tam lawsuit against Pennsylvania State University relating to allegations of noncompliance with U.S. Department of Defense cybersecurity obligations.

Separately, on Sept. 5, the U.S. Department of Justice announced a multimillion-dollar FCA settlement with Verizon Business Network Services LLC under its Civil-Cyber Fraud Initiative, which focuses on leveraging the FCA to pursue cybersecurity-related fraud by government contractors and grant recipients.[1].

These and other cases suggest — as many had been speculating — that the number of enforcement actions and the publicity associated with previously sealed qui tam cases will continue to increase. They also signal that contractors and universities should brace for additional scrutiny and potential whistleblower claims in this area.

Whistleblower Allegations Relating to DFARS Cybersecurity Compliance

On Sept. 1, the Eastern District of Pennsylvania unsealed Decker v. Pennsylvania State University, a qui tam FCA lawsuit originally filed on Oct. 5, 2022, alleging Penn State University failed to provide adequate security for covered defense information, as is contractually required by Defense Federal Acquisition Regulation Supplement 252.204-7012.

Under this clause, "adequate security" is defined as at least implementing all 110 controls outlined in the National Institute of Standards and Technology Special Publication 800-171.[2] Moreover, federal regulations require DOD contractors to conduct a self-assessment of compliance with those 110 controls and report a compliance score, out of 110, in the DOD's supplier performance risk system.

Among other things, the lawsuit alleges Penn State falsified at least 20 documents related to its NIST SP 800-171 self-assessment and other self-attestations.

In particular, the lawsuit alleges that despite never reaching DFARS compliance, the university "had been falsely attesting to compliance since January 1, 2018." The lawsuit also alleges sensitive information was put at risk when the university migrated some of its data to a commercial cloud-storage service.

The relator in the case, Matthew Decker, served as the interim chief information officer at Penn State's Applied Research Laboratory in 2015 and was part of a team assigned to evaluate the university's compliance in early 2022. The DOJ has not yet intervened and must notify the court by Sept. 29 if it intends to intervene in the case.

This FCA whistleblower lawsuit is significant for at least two reasons.

First, it reinforces that DOD contractors and subcontractors are easy targets for whistleblowers — especially when they have exceedingly long lists of actions, such as the 110 controls here, for which they regularly attest.

As such, it is critical that contractors and subcontractors take steps to ensure that self-attestations and representations are accurate, and that they facilitate a culture of collaboration, transparency and accountability when it comes to cybersecurity to lower the likelihood that an employee will become a whistleblower.

Second, universities and institutes of higher education with government contracts are not shielded from cyber-related FCA claims and must ensure they understand and comply with government cybersecurity regulations.

DOJ Civil-Cyber Fraud Initiative Settlement

On Sept. 5, the DOJ announced its latest cyberfraud-related settlement under the Civil-Cyber Fraud Initiative.[3] Per the settlement agreement, Verizon has agreed to pay $4,091,317 to resolve FCA allegations that it failed to completely satisfy certain cybersecurity controls in connection with an information technology service provided to federal agencies.[4]

In particular, the settlement relates to Verizon's Managed Trusted Internet Protocol Service, which is designed to provide federal agencies with secure connections to the public internet and other external networks. The DOJ alleged that Verizon's MTIPS solution did not completely satisfy three required cybersecurity controls for Trusted Internet Connections with respect to General Services Administration contracts from 2017 to 2021.

In resolving the allegations, the DOJ explained that Verizon received significant credit because Verizon self-disclosed the issue, initiated an independent investigation and compliance review of the issues, and provided supplemental written disclosures. Verizon also cooperated with the government's investigation and took prompt and substantial remedial measures.

The settlement agreement clarifies that $2.7 million of the settlement amount is restitution, which means approximately $1.3 million is due to the government's application of a multiplier — under the FCA, the government can seek up to treble damages, plus certain statutory penalties.

Here, the total settlement amount appears to be about 1.5 times the restitution amount. This is fairly common in instances where contractors self-disclose noncompliance, as Verizon did here.

This DOJ settlement highlights the importance of robust contractor compliance systems and a culture that facilitates internal reviews to identify issues, self-disclosure of issues, internal investigations and cooperation with the government.

Key Takeaways for Federal Contractors and Universities

Review and confirm your understanding of cybersecurity obligations and practices.

Now is a good time for contractors and universities to reexamine their cybersecurity posture and ensure compliance efforts are well underway, and that any self-attestations and representations are accurate and defensible.

Government contractor cybersecurity obligations are complicated and can be confusing. Ensure your team has a good understanding of the requirements and, if not, provide training and instruction.

Build a strong compliance, and audit and monitoring function.

Contractors and universities must understand cybersecurity obligations, follow the required standards and implement strong policies, procedures and controls. Continuous internal reviews are critical to identifying and resolving any potential gaps in compliance.

Promptly investigate internal complaints.

Internal complaints can be tricky, especially as the compliance landscape with respect to cybersecurity requirements is complex and rapidly evolving in real time. Internal complaints may very well be legitimate. But, it also is possible that employees may not fully understand the company's true compliance obligations.

Companies should take all internal complaints seriously, and ensure that complaints are adequately investigated against the company's actual compliance obligations and that corrections are made as necessary.

Additionally, as our colleague David Douglass recently wrote, respecting employees' concerns, understanding those concerns and keeping employees in the loop during internal investigations result in a stronger organization.[5]

Recent enforcement actions are just the beginning.

The focus on this area will not fade any time soon. As such, we expect to see significant increases in enforcement actions, both government-initiated and whistleblower-initiated. If cybersecurity compliance has not been at the top of your list, it is likely past time to move it up.

Townsend Bourne is a partner and leader of the government business group at Sheppard Mullin Richter & Hampton LLP.

Nikole Snyder is an associate at the firm.

[1] We previously discussed this here: https://www.governmentcontractslawblog.com/2021/10/articles/cybersecurity/doj-announces-civil-cyber-fraud-initiative/.

[2] https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf.

[3] https://www.justice.gov/opa/pr/cooperating-federal-contractor-resolves-liability-alleged-false-claims-caused-failure-fully.

[4] https://www.justice.gov/media/1313011/dl?inline.

[5] https://www.organizationalintegrity.com/2022/07/short-guide-responding-to-employee-concerns-about-your-organizations-actions-and-mission-vision-and-values/.