COVINGTON

Cybersecurity and Government Contracting: False Claims Act Considerations

By Michael Wagner, Peter B. Hutt II, Susan B. Cassidy and Andrew Guy on January 11, 2021

False Claims Act

As the recent SolarWinds Orion attack makes clear, cybersecurity will be a focus in the coming years for both governmental and non-governmental entities alike. In the federal contracting community, it has long been predicted that the government's increased cybersecurity requirements will eventually lead to a corresponding increase in False Claims Act (FCA) litigation involving cybersecurity compliance. This prediction may soon be proven true, as a December 2020 speech from Deputy Assistant Attorney General Michael Granston specifically identified "cybersecurity related fraud" as an "area where we could see enhanced False Claims Act activity." This article discusses recent efforts to use the FCA to enforce cybersecurity compliance — and, based on those efforts, what government contractors may expect to see in the future.

In recent years, the government and *qui tam* plaintiffs have begun using the FCA to pursue alleged noncompliance with cybersecurity regulations, and some of these efforts have gained traction. For instance, in May 2019, a federal district court in California declined to dismiss a case alleging that a government contractor had falsely asserted its compliance with cybersecurity standards when entering into Department of Defense contracts. And in July 2019, the Department of Justice announced that another contractor had agreed to pay more than $8 million in connection with resolving a *qui tam* suit alleging failure to meet federal cybersecurity standards, marking the first settlement based on FCA allegations related to cybersecurity noncompliance.

More recently, however, at least one court rejected the attempt to build an FCA case out of alleged deviations from cybersecurity regulations. In October 2020, a federal district court in the District of Columbia dismissed a *qui tam* suit alleging that a contractor had failed to disclose a security vulnerability in the computer systems that it sold to the United States. *United States ex rel. Adams v. Dell Computer Corp.*, 15-cv-608 (D.D.C. Oct. 8, 2020). The court's dismissal was based on its conclusion that the whistleblower had failed to show that the noncompliance was "material." As the court noted, "the technology policies referenced . . . do not require defect-free products," and that any applicable security policy could have instead been addressed by "providing the necessary assistance to eliminate or reduce vulnerabilities as they appear."

Going forward, we expect the FCA's strict materiality requirement will continue to present a significant hurdle for plaintiffs in future cases alleging noncompliance with increasingly detailed cybersecurity regulations. As Mr. Granston's recent speech portends, however, the federal

government and *qui tam* plaintiffs are poised to bring suits under the FCA predicated on allegations of cybersecurity noncompliance. While these allegations could take myriad forms, there are two regulatory developments in particular that may provide ammunition to enterprising whistleblowers – and pose FCA risk for unwary contractors. First, under the NIST 800-171 DoD Assessment Methodology, DoD is now requiring that contractors complete a pre-award self-assessment (formally known as a "Basic Assessment") of their compliance with the 110 security controls found in NIST 800-171. That Basic Assessment results in a numerical score that is provided to the government and a date by which the contractor represents it will be in full compliance with all NIST 800-171 controls. Following award, the DoD may decide to complete its own Medium Assessment (via a paper review) or High Assessment (via an in-person review) of a contractor's compliance with the NIST 800-171 security requirements.

This assessment process could give rise to disagreements between the contractor and the government over the extent to which the contractor is complying with the NIST 800-171 security controls. In particular, a large discrepancy between the Basic Assessment's numerical score and the Medium or High Assessment's numerical score could lead to allegations that the contractor failed to accurately represent its cybersecurity requirements, thereby raising the specter of FCA risk.

Second, defense contractors will soon be asked to obtain and provide a Cybersecurity Maturity Model Certification (CMMC) from an accredited CMMC Third Party Assessment Organization. As part of this certification process, contractors will be expected to show their ability to meet the NIST 800-171 security requirements as well as several additional security controls. Allegations of inconsistencies between the self-assessment of compliance with 800-171 and the third party CMMC assessment, may also draw the attention of would-be *qui tam* plaintiffs.

However, it may prove difficult for the government or *qui tam* plaintiffs to establish FCA liability based on allegations of cybersecurity noncompliance. First, and as noted above, FCA liability can only be imposed where the requirement is "material," meaning that the noncompliance would have a "natural tendency to influence, or be capable of influencing" the government's decision to pay the contractor. However, federal contracts often contain cybersecurity requirements among a list of dozens — if not hundreds — of other regulatory obligations. In many cases it is unlikely that the government's decision to pay a contractor would depend on strict compliance with a particular cybersecurity control or set of controls, in which case noncompliance with that control would not be "material."

Second, FCA liability requires a showing that a noncompliance was "knowing," meaning that the contractor actually knew they were not in compliance with a requirement, acted with deliberate ignorance, or acted with reckless disregard. However, many of the cybersecurity requirements are new, and drafted broadly, allowing reasonable differences in technical interpretation. There is substantial case law establishing that a contractor cannot be held liable under the FCA for a reasonable, good-faith reading of unclear regulatory requirements.

Thus, even if the predictions about an uptick in FCA cybersecurity cases come true, there are good reasons for thinking that many such matters will face significant headwinds. Although all cases are different, the standard defenses in such matters will be fully available, including both substantive defenses like those outlined above, and procedural defenses such as the statute's Public Disclosure bar. Nonetheless, the likelihood of an increase in FCA cases underscores the importance of ensuring careful attention to cybersecurity compliance and associated representations.

If you have any questions concerning the material discussed in this client alert, please contact the following members of False Claims Act practice:

Christopher Denig	+1 202 662 5325	cdenig@cov.com
Matt Dunn	+1 202 662 5314	mdunn@cov.com
Sarah Franklin	+1 202 662 5796	sfranklin@cov.com
Geoffrey Hobart	+1 202 662 5281	ghobart@cov.com
Peter Hutt	+1 202 662 5710	phuttjr@cov.com
Fred Levy	+1 202 662 5154	flevy@cov.com
Aaron Lewis	+1 424 332 4754	alewis@cov.com
Matthew O'Connor	+1 202 662 5469	moconnor@cov.com
Mona Patel	+1 202 662 5797	mpatel@cov.com
Ethan Posner	+1 202 662 5317	eposner@cov.com
Daniel Shallman	+1 424 332 4752	dshallman@cov.com
Michael Wagner	+1 202 662 5496	mwagner@cov.com
Shanya Dingle	+1 202 662 5615	sdingle@cov.com
Michael Maya	+1 202 662 5547	mmaya@cov.com
Krysten Rosen Moller	+1 202 662 5899	krosenmoller@cov.com
Sarah Tremont	+1 202 662 5538	stremont@cov.com

This information is not intended as legal advice. Readers should seek specific legal advice before acting with regard to the subjects mentioned herein.

Covington & Burling LLP, an international law firm, provides corporate, litigation and regulatory expertise to enable clients to achieve their goals. This communication is intended to bring relevant developments to our clients and other interested colleagues. Please send an email to unsubscribe@cov.com if you do not wish to receive future emails or electronic alerts.

© 2021 Covington & Burling LLP. All rights reserved.