Cybersecurity obligations for government contractors – focus on them before the government focuses on you

Government Contracts Alert

22 September 2021

By: Dawn E. Stern | Courtney Gilligan Saleski | Thomas E. Daley

Over the past several years, the government has increasingly focused on the cybersecurity requirements applicable to federal government contractors and contractor's compliance with those regulations. With these additional compliance obligations comes an increased risk of cybersecurity-related False Claims Act liability. It is critical that contractors understand their obligations and consider taking appropriate steps.

According to the Department of Justice, "[w]here [cybersecurity] protections are a material requirement of payment or participation under a government program or contract, the knowing failure to include such protections could give rise to False Claims Act liability."[1]

As noted in our previous publication, at least one district court has concluded that a company's failure to comply with cybersecurity requirements, including National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, could be material under the False Claims Act. As new cybersecurity requirements are implemented as part of the Department of Defense Cybersecurity Maturity Model Certification (CMMC) program, and in response to the Executive Order on Improving the Nation's Cybersecurity , many contractors may be required to comply with new cybersecurity requirements that could be deemed material under the False Claims Act.

Given this environment, it is critical that contractors understand their obligations and consider taking appropriate steps in the following areas:

- President Biden's Executive Order on Improving the Nation's Cybersecurity contemplates a number of new, cybersecurity-related obligations that are receiving significant attention from the government. Thus, contractors will want to closely monitor developments under the Executive Order and ensure compliance. For example:
  - There will be a number of new Federal Acquisition Regulation (FAR) and Defense Federal Acquisition Regulation Supplement (DFARS) provisions and contract clauses that relate to collecting and preserving data, reporting and sharing data related to cyber incidents, and collaborating with federal agencies when investigating cyber incidents. Contractors should understand their contract requirements and take steps to ensure timely implementation, including performing appropriate tabletop exercises – do not wait until a cyber incident occurs to first evaluate your relevant obligations.
  - We anticipate that information and technology service contractors will be required to "promptly" report cyber incidents involving a software product or service being provided to an agency. Thus, even those companies that are not subject to reporting requirements under the existing DFARS framework (DFARS 252.204-7012) may have onerous reporting obligations. Companies impacted by this requirement should consider how it will impact their compliance programs and contracts throughout their supply chains. For example, once this requirement is finalized, contractors will want to consider whether they need to amend any subcontracts to address such reporting.
  - Providers of "critical software" will be required to ensure that the critical software complies with NIST requirements. Once again, this requirement may extend to companies that are not currently subject to the cybersecurity requirements set forth in DFARS 252.204-7012. Thus, companies impacted by these requirements should consider their impact throughout the supply chain.

- While currently undergoing review (and likely alteration) from the Biden Administration, the Department of Defense's Cybersecurity Maturity Model Certification (CMMC) program, once implemented, has the potential to create areas of False Claims Act liability:
  - Contractors must ensure that they have the requisite certification level before bidding on a contract and have achieved that certification level from an approved auditor.
  - Contractors must ensure that companies within their supply chain have achieved the requisite certification level. This is not as easy as it sounds because companies within the supply chain may require different certification levels, and the requisite levels are unlikely to be delineated in the solicitation or contract. Thus, ascertaining which level is required for each subcontractor will likely require coordination with the contracting officer and subcontractors, as well as an understanding of how electronic information will flow during performance of the contract.

- Other agencies are closely watching the development of CMMC and may implement it in various forms. Thus, even non-DoD contractors should be monitoring CMMC developments.
- Given the long lead time associated with the roll-out of CMMC as well as the inconsistent implementation of the existing DoD cybersecurity requirements (ie, implementation of the NIST SP 800-171 controls pursuant to DFARS 252.204-7012), DoD enacted a self-assessment and reporting requirement. Specifically, DFARS 252.204-7020, which applies generally to contractors and subcontractors that process, store, or transmit covered defense information (CDI), requires the performance of a self-assessment and the reporting of the results of that assessment to DoD. This new reporting requirement, as with other cybersecurity developments, comes with the potential for False Claims Act liability. To minimize risk, the self-assessment and subsequent reporting ideally should be conducted by an interdisciplinary team that includes IT, business, legal, and compliance, with a focus on accurate and complete reporting.

Contractors should take note of these risks because liability under the False Claims Act can be financially debilitating, particularly for small and mid-size contractors. Under the False Claims Act, contractors may face both criminal and civil liability, including civil penalties for each false claim and treble damages. Additionally, the knowing failure to comply with applicable cybersecurity requirements could lead to other issues, such as suspension or debarment from federal contracting.

We will continue to monitor developments in this area. If you have any questions, please contact the authors or your DLA Piper relationship attorney.

[1]*Remarks of Deputy Assistant Attorney General Michael D. Granston at the ABA Civil False Claims Act and Qui Tam Enforcement Institute*, US Department Of Justice, https://www.justice.gov/opa/speech/remarks-deputy-assistant-attorney-general-michael-d-granston-aba-civil-false-claims-act (Dec. 2, 2020)

AUTHORS

Dawn E. Stern
Partner
Washington, DC | T: +1 202 799 4000
dawn.stern@dlapiper.com

Courtney Gilligan Saleski
Partner
Philadelphia | T: +1 215 656 3300
Washington, DC | T: +1 202 799 4000
courtney.saleski@dlapiper.com

Thomas E. Daley
Associate
Washington, DC | T: +1 202 799 4000
tom.daley@dlapiper.com