THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

THOMSON REUTERS®

Vol. 64, No. 20 **May 18, 2022**

Focus

¶ 147

FEATURE COMMENT: Don't Panic: DOJ Civil Cyber Fraud Initiative And Defense Contractors

Deputy Attorney General Lisa Monaco caused quite a stir in the Government contracting community on October 6 of last year when she announced the Department of Justice's new civil cyber fraud initiative to use the False Claims Act to "combat new and emerging cyber threats to the security of sensitive information and critical systems." See *www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative*. By threatening civil fraud enforcement for noncompliance with constantly changing cybersecurity and information protection rules, DOJ dramatically increased the anxiety levels in many Government contractor legal, compliance, and information technology departments—especially because these departments have already been working overtime in recent years to adjust to new threats and ever increasing information protection rules. But that anxiety can be reduced by understanding (1) where the DOJ announcement fits within the long arc of Government efforts to enhance contractor cybersecurity, and (2) the heavy lift the Government will need to undertake to bring successful cyber fraud FCA cases against Government contractors that expend good faith efforts to comply.

This article focuses on Department of Defense cybersecurity rules in order to discuss the compliance challenges facing contractors, and how those compliance challenges present obstacles to DOJ's efforts to bring FCA cases.

Historical Context—Cybersecurity Requirements in Flux—DOD efforts to improve cybersecurity and information protection have proceeded in fits and starts. Large changes have been proposed, or announced in interim rulemaking, only later to be walked back or significantly modified by subsequent guidance or final rulemaking. This evolution continues today. These inconsistencies are likely to frustrate DOJ efforts to bring successful FCA cases against companies that expend good faith effort towards compliance.

Further, understanding the development of Government contractor cybersecurity rules may permit companies to push back against overly broad, or even incorrect, arguments that the standards were violated. This, in turn, may help contractors defend themselves against FCA investigations, resist DOJ interventions in qui tam whistleblower cases, and move to dismiss filed cases.

A brief summary of some key cybersecurity rules affecting Government contractors follows.

- A critical development in Government contractor cybersecurity requirements issued in 2013 when the Defense Federal Acquisition Regulation Supplement published clause 252.204-7012, Safeguarding Unclassified Controlled Technical Information (Nov. 18, 2013). The "Safeguarding Clause" focused contractors on providing "adequate security" for unclassified but still controlled technical information (CUI). The Safeguarding Clause called for contractors to implement, at a minimum, more than 50 specific security controls then contained within the National Institute of Standards and Technology (NIST) Special Publication 800-53.

Challenges with the NIST controls included their dynamic nature, and appropriately calibrating the controls for the relative threats facing the contractor. The Safeguarding Clause required contractors and their subcontractors to implement dynamic controls to protect CUI and to disclose to DOD certain cyber incidents on an aggressive timeframe.

- But then the requirements changed substantially. On Aug. 26, 2015, an interim rule replaced NIST Special Publication 800-53 with NIST Special Publication 800-171 as the baseline for DOD Safeguarding Clause. NIST Special Publication 800-171 pivoted Government contractors' cybersecurity efforts to complying with more than 100 requirements in more than a dozen control families after the industry had spent years working to comply with Special Publication 800-53's substantial controls. Government contractors were given a limited period of time to implement the new NIST 800-171 controls.
- And then the requirements increased yet again. On Oct. 21, 2016, after a few rounds of interim rulemaking, the Safeguarding clause expanded through a final rule to include "covered defense information" or "CDI" on all covered contractor information systems, and to require that any cloud service providers used to store, process, or transmit CDI must themselves have certain adequate cybersecurity and information protection qualifications. CDI expanded the information that must be protected beyond CUI to include, among other things, critical information relevant to operational security including cybersecurity vulnerabilities, export controlled information, and controlled technical information.
- Recognizing the burden contractors faced in complying with the Government's requirement, a DOD policy document provided some relief. On Sept. 21, 2017, the Office of the Undersecretary of Defense for Acquisition, Technology and Logistics issued a memorandum entitled "Implementation of DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting," which further spelled out DOD policy regarding compliance with the Safeguarding Clause and provided certain safe harbors for noncompliance. See *www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf*.

  The memo made clear that the Safeguarding Clause required compliance with more than 100 additional controls spelled out in NIST Special Publication 800-171, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations," and provided a date for compliance. Specifically, "[c]ontractors, who self-attest to meeting these requirements, have until Dec, 31, 2017, to implement NIST SP 800-171."

  This guidance indicated the dynamic nature of the information protection requirements imposed upon Government contractors, stating "[t]here is no single or prescribed manner in which a contractor may choose to implement the requirements ... or to assess their own compliance. ... [and t]hird party assessments or certifications of compliance are not required, authorized, or recognized by DoD, nor will DoD certify that a contractor is compliant."

  Importantly, the guidance recognized that contractors would have gaps in compliance. System security plans (SSPs) with plans of action and milestones (POAMs) to closing gaps are discussed as methods of reporting shortfalls and working to close them over time.
- In part to move beyond self-assessment of cybersecurity and information protection compliance, in September 2020, DOD announced the creation of the Cybersecurity Maturity Model Certification (CMMC) where a third party would certify a contractor's compliance with five tiers of information protection requirements. The interim rule became effective in November 2020 and established a five-year phased compliance period. See *www.acq.osd.mil/cmmc/about-us.html*. DOD made clear that CMMC compliance would be a gating factor for contractors to be eligible for award. But confusion about the process, timelines, and entities that could certify contractor compliance bogged down CMMC rollout such that, in 2021 after

receiving "more than 850 public comments in response to the interim DFARS rule," DOD issued CMMC 2.0 to streamline and simplify the program. Id.

CMMC 2.0 contains three risk-adjusted levels of protection with assessments that permit DOD to verify implementation of 17 "foundational" practices, 110 "advanced" practices aligned with NIST SP 800-171, and 100+ "expert" practices based on NIST SP 800-172, "Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171." Annual self-assessments are permitted for Level 1/Foundational compliance. Level 2/Advanced compliance requires triennial third-party assessments for "critical national security information" and annual self-assessments for select programs. Level 3/Expert requires triennial Government-led assessments. Rulemaking is ongoing with much left to be finalized.

This brief summary of the evolution of a sample of the cybersecurity requirements facing Government contractors demonstrates just how difficult the effort is. The requirements have not been uniform, and each iteration of the rules has required substantial time, effort, and resources to implement. And a substantial number of contractors funded cybersecurity enhancements on their own. After all, the requirements evolved during the period where DOD was also expending great effort to drive down acquisition costs and squeeze contractor profits (that might otherwise be available to fund cybersecurity improvement) through acquisition methods such as low price, technically acceptable procurement.

Cyber Fraud Initiative—Given the importance of information protection and the increase in cyber threats facing the defense industrial base, it is not surprising that DOJ would want to consider punishing noncompliance. The cyber fraud initiative announced Oct. 6, 2021, seeks to accomplish that goal by utilizing "the False Claims Act to pursue cybersecurity related fraud by Government contractors and grant recipients." The types of violations to be targeted by the cyber fraud initiative include:

- Knowingly providing deficient cybersecurity products or services;
- Knowingly misrepresenting cybersecurity practices or protocols; and
- Knowingly violating obligations to monitor and report cybersecurity incidents and breaches.

And the DOJ press release announcing the initiative emphasized in a quote from Deputy Attorney General Monaco that "[f]or too long, companies have chosen silence under the mistaken belief that it is less risky to hide a breach than to bring it forward and report it." There was no support offered for the sentiment that willful failure to report was commonplace. See *www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative.*

Risks Facing Contractors—DOJ's announcement alarmed Government contractors because of the dynamic and continuously evolving nature of cybersecurity compliance. The prospect of facing FCA liability for perceived noncompliance with an unfixed and continuously changing set of regulatory requirements is indeed unsettling.

Focusing on Deputy Attorney General Monaco's quote, Government contractors can face FCA liability (among other consequences) (1) where the contractor experiences a cyber breach, (2) where leadership knows the company is required to report the breach, and (3) where leadership chooses not to report. But that was true before the establishment of the cyber fraud initiative. So what new risks are present after DOJ's announcement? That answer is less than clear. After all, the FCA elements make bringing a raft of successful cyber fraud cases far more difficult than might appear to be the case from the DOJ press release.

A contractor may be liable for violating the FCA when the contractor "knowingly presents, or causes to be presented, a false or fraudulent claim for payment or approval" to the U.S. 31 USCA § 3729(a)(1)(A). The "knowingly," or scienter, element of the FCA is likely to present difficulties for the Government as it seeks to bring civil FCA cases for cybersecurity violations. After all, the FCA is not an all-purpose antifraud statute nor is it a vehicle for punishing garden-variety breaches of contract or regulatory violations. It has specific requirements, and one is that the contractor must have "knowingly" engaged in misconduct. It is difficult for the Government to allege a knowing violation when cybersecurity and information protection

rules are in flux. An objectively reasonable belief by a contractor that their conduct is appropriate and within the bounds of the law can be enough to defeat FCA liability.

Additionally, Government knowledge of alleged misconduct and resulting Government decisions to continue to pay invoices are strong evidence that the requirements that the contractor is alleged to have violated are not material to the Government. In such cases, the violations are not actionable under the FCA. Given that SSPs and POAMs were encouraged by DOD policy, it follows that the Government likely has knowledge of a substantial number of Government contractor noncompliances, and therefore DOJ will likely struggle to bring FCA cases resulting from these noncompliances.

Risk Avoidance Strategies—Contractors can reduce the risk of being subjected to an FCA investigation—or reduce the duration of any such investigation—by taking some common-sense prophylactic steps:

(1) Conduct a cybersecurity risk assessment;
(2) Assess compliance with cybersecurity and information protection guidelines against contractual and regulatory requirements, with input from the risk assessment;
(3) Memorialize the company's understanding of its compliance and how each requirement is met so an objective third party can understand how the company is in compliance;
(4) Inform the customer of gaps in compliance consistent with existing regulations, and keep them posted on efforts to address the gaps.

If DOJ or other law enforcement components inquire about cybersecurity compliance, the steps identified above can help companies demonstrate their compliance or, at a minimum, their reasonable belief that they were compliant. Disclosure of gaps in routine filings such as through SSPs and POAMs, or other communications, is also important when defending FCA cases. Finally, mapping alleged noncompliance to the specific rules and timelines for compliance may help contractors defend themselves against allegations that the contractor violated cybersecurity rules.

♦

This Feature Comment was written for THE GOVERNMENT CONTRACTOR by Jenner & Block, LLP, partners* David Robbins, Tony Barkow, David Bitkower *and* Aaron Cooper. *David Robbins is a former acting Deputy General Counsel and a former Procurement Fraud Remedies Director of the U.S. Air Force. He co-chairs the firm's Government Contracts Practice. Tony Barkow is a former federal prosecutor in the Southern District of New York and in the District of Columbia, and co-chairs the Investigations, Compliance, and Defense Practice. David Bitkower is a former Principal Deputy Assistant Attorney General for the Criminal Division of the Department of Justice and co-chairs both the Investigations, Compliance, and Defense Practice and the Cybersecurity Practice. Aaron Cooper, a member of the Investigations, Compliance and Defense Practice, is a former lead Senate investigative counsel and Department of Justice cybercrimes prosecutor.

