THE GOVERNMENT CONTRACTOR®

Information and Analysis on Legal Aspects of Procurement

OCTOBER 11, 2023 | VOLUME 65 | ISSUE 37

¶ 273 FEATURE COMMENT: Former CIO's FCA Suit: A Warning For Universities (And Beyond) Over Controlled Unclassified Information Compliance

*David Robbins and Moshe Broder**

In an unusual procedural move, the U.S. District Court for the Eastern District of Pennsylvania recently denied the Government's request to keep under seal a relatively recently filed, information security-related False Claims Act qui tam suit against Pennsylvania State University. FCA investigations often remain sealed for years. Here, however, the Eastern District of Pennsylvania ruled that eight months was long enough. As a result, on Sept. 29, 2023, the Government declined to intervene, but noted that it remained a party in interest and its investigation was ongoing.

The complaint was filed by the former chief information officer of Penn State's Applied Research Laboratory and alleges failures in following Government contracting requirements to safeguard "controlled unclassified information" (CUI). See *www.documentcloud.org/documents/23977827-us-vs-penn-state-false-claims-act*. The complaint takes issue with Penn State's self-assessment and self-certification of its compliance with, among other things, rules governing protection of CUI. Id.

The relator alleges that Penn State submitted knowingly false records and risk assessments—documents that are threshold requirements to be considered for contract award under Defense Federal Acquisition Regulation Supplement clause 252.204-7019. Id. The relator further alleges that despite performing multiple contracts subject to the requirements of DFARS 252.204-7012 and -7019, Penn State did not prepare required system security plans and thus had no ability to meaningfully assess or certify its compliance with applicable cybersecurity requirements. Id. It also details multiple areas of alleged CUI noncompliance, and an effort by Penn State to dilute the internal findings critical of the university's alleged non-compliance. Id. Further complicating the matter, on Sept. 29, 2023, the U.S. informed the Court that it was not intervening "at this time" although its investigation remains active and will

**This Feature Comment was written for* THE GOVERNMENT CONTRACTOR *by* David Robbins *and* Moshe Broder. *David Robbins is the co-Chair of Jenner & Block's Government Contracts practice and a former Deputy General Counsel and Procurement Fraud Remedies Director for the U.S. Air Force. Moshe Broder is resident in the Washington, D.C., office of Jenner & Block and focuses his practice on Government Contracts.*

continue as the Government obtains and reviews information produced in response to Civil Investigative Demands. The U.S. further stated that it may need to take further investigatory action before deciding whether to intervene.

As background, the CUI program was established by a 2010 executive order and was intended to address the inefficient and confusing patchwork of policies and practices surrounding the identification and safeguarding of information that was not classified but required protection due to an existing statute, regulation, or policy. Agencies had previously used a range of markings for such information, including "For Official Use Only" and "Sensitive But Unclassified." Going forward, all agencies would adopt a uniform procedure for identifying and marking such information, and the requirements would increase over time.

Following the enactment of the executive order, the Department of Defense implemented contractual requirements with significant compliance obligations for safeguarding CUI. Most significantly, under DFARS clause 252.204-7012, where CUI is present in certain "covered contractor information systems," the contractor must provide "adequate security" which includes, at a minimum, implementing the security controls set forth in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. In addition to this requirement to safeguard CUI, DOD regularly requires contractors to comply more broadly with the CUI program—including the marking requirements—by inserting a requirement into a contract's security classification guide.

More recently, DOD issued DFARS clauses 252.204-7019 and -7020. These clauses require, as a threshold condition of contract award, that a contractor conduct a formal assessment of their compliance with the requirements set forth in NIST SP 800-171 (for all "covered contractor information systems") and submit a score to DOD reflecting the current state of maturity of their compliance. This is notable because the -7012 clause discussed above did not require an affirmative attestation of compliance or a representation regarding the extent of compliance. And as mentioned above, the relator in the Penn State case alleged that the university prepared basic assessments that were knowingly inaccurate and submitted them to DOD, so the university could remain eligible for contract award.

As experienced FCA defense lawyers, we know well that complaints can exaggerate facts and the truth is not always as colorful. Nevertheless, this complaint highlights the complexity of compliance with difficult and highly technical cybersecurity requirements. The difficulty extends to the Government customer as well, as shown in a DOD Inspector General audit report published earlier this year, which faulted the Government for failing to ensure proper contractor CUI training, and for failing to properly mark data requiring CUI protections. See *www.dodig.mil/reports.html/Article/3413433/audit-of-the-dods-implementation-and-oversight-of-the-controlled-unclassified-i/*. While contractors have made notable progress in safeguarding CUI in recent years, allegations of falsifying cybersecurity assessments are likely to continue as these requirements come under increasing scrutiny.

Additionally, CUI protection is within the ambit of the Department of Justice Civil Cyber Fraud Initiative announced in 2021. See *www.justice.gov/opa/pr/deputy-attorney-general-lisa-o-monaco-announces-new-civil-cyber-fraud-initiative*. The initiative began slowly but there have been a number of settlements after the Department of Justice began actively seeking referrals including from motivated relators seeking a share of eventual recoveries. As such, universities (and recipients of federal funds more generally) are well advised to treat Government inquiries regarding CUI compliance as a prelude to potential enforcement actions.

Whether or not the Government ultimately chooses to intervene in the Penn State case, the complaint serves as an important reminder to universities in receipt of Defense Department dollars to remain in compliance with the full range of (ever evolving) cybersecurity standards, to include CUI protection.