October 30, 2023

Skadden

Privacy & Cybersecurity Update

If you have any questions regarding the matters discussed in this memorandum, please contact the following attorneys or call your regular Skadden contact.

William Ridgway
Partner / Chicago
312.407.0449
william.ridgway@skadden.com

David A. Simon
Partner / Washington, D.C.
202.371.7120
david.simon@skadden.com

Emma Hlavin
Law Clerk / Chicago
312.407.0610
emma.hlavin@skadden.com

One Manhattan West
New York, NY 10001
212.735.3000

Cyber Fraud Alleged by Former CIO for Purported Noncompliance With DoD Cyber Requirements

A recently unsealed case against Pennsylvania State University:

- Serves as yet another example of the increased use of the False Claims Act (FCA) in cybersecurity enforcement.
- Underscores the need for companies with government contracts to scrutinize their cybersecurity and reporting policies and procedures to avoid FCA exposure.
- Is especially relevant for Department of Defense (DoD) contractors and requirements to safeguard "controlled unclassified information" (CUI) under Defense Federal Acquisition Regulation Supplement (DFARS) clause 252.204-7012.

Background

In October 2021, Department of Justice (DOJ) launched its Civil Cyber-Fraud Initiative, which utilizes the FCA to enforce cybersecurity standards required of federal contractors and grant recipients. Importantly, the FCA includes a whistleblower provision that allows private parties to identify fraudulent conduct and share in recovery. DOJ signaled its intent to target companies that knowingly:

- Provide deficient cybersecurity products or services.
- Misrepresent their cybersecurity practices or protocols.
- Violate obligations to monitor and report cybersecurity incidents and breaches.

As part of the initiative, DOJ clarified that CUI compliance is a prioritized area of enforcement. Following a slow start, the initiative secured a number of settlements after the department actively started seeking referrals, including from whistleblowers. To date, DOJ has publicized three resolutions of cases brought as part of the initiative, two of which relate to the cybersecurity of health information. The Penn State investigation is the latest outgrowth of the DOJ's initiative.

Penn State

In October 2022, Penn State was sued by a former chief information officer (CIO) for allegedly failing to safeguard CUI as contractually required and knowingly submitting false security compliance reports.

Cyber Fraud Alleged by Former CIO for Purported Noncompliance With DoD Cyber Requirements

Significantly, DFARS clause 252.204-7012 requires DoD contractors to provide "adequate security" to protect CUI, which at a minimum includes implementing the security controls set forth in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171. Although the -7012 clause does not require an affirmative attestation, the recently issued DFARS clauses 252.204-7019 and -7020 compel a contractor to conduct a self-assessment and self-certification of its compliance with the requirements of NIST SP 800-171.

Penn State's former CIO alleges that the university prepared basic assessments that were knowingly inaccurate to dilute the internal findings critical of the university's alleged CUI noncompliance, and then submitted them to DoD to remain eligible for contract award. Although the government recently declined to take over the lawsuit, a DoD probe and the whistleblower litigation remain ongoing.

Takeaways

The Penn State case demonstrates the whistleblower exposure that comes from potential FCA liability for cybersecurity-related fraud. Companies with any involvement in government contracting should consider assessing, and taking steps to implement controls that may help mitigate against, this potential exposure. For example, companies should contemplate:

- Evaluating the accuracy of any representations regarding the cybersecurity of products and services.
- Retaining contemporaneous documentation that supports the accuracy of representations.
- Staying abreast of cybersecurity regulatory developments and ensuring that company policies and procedures continue to meet regulatory requirements and industry best practices.
- Adopting whistleblower best practices, including a reporting structure that facilitates the reporting of potential cybersecurity gaps and failures within the company.