Updates
August 08, 2022
Recent Settlement Highlights Cybersecurity Whistleblower Risk for Government Contractors

The U.S. Department of Justice's (DOJ) Civil Cyber-Fraud Initiative, announced last October, is designed to leverage existing whistleblower incentives for employees, or other persons with inside knowledge, to identify lapses in federal contractors' cybersecurity and privacy practices. We gave that issue in-depth treatment here, with particular focus on the U.S. District Court for the Eastern District of California's opinion in *United States ex. rel. Markus v. Aerojet Rocketdyne Holdings, Inc.*, No. 2:15-cv-02245 WBS AC, 2022 WL 297093 (E.D. Cal. Feb. 1, 2022), denying the defendant's motions for summary judgment on a majority of the relator's False Claims Act (FCA) claims.

Last month, DOJ announced that Aerojet Rocketdyne Holdings Inc. (Aerojet) "has agreed to pay $9 million to resolve allegations that it violated the False Claims Act by misrepresenting its compliance with cybersecurity requirements in certain federal government contracts." The relator—Markus, a former cybersecurity professional at Aerojet—will receive $2.61 million as recovery for bringing the qui tam action. Given that the *Markus* case presents a clear incentive for cybersecurity professionals across the federal supply chain to bring a whistleblower claim, as well as the DOJ's stated intention of pursuing such claims as a matter of protecting our nation's cybersecurity, we provide some high-level, practical considerations for contractors to consider.

What Is a Company's Risk?

The following questions are designed to help businesses consider the potential breadth of their cybersecurity whistleblower risk:

- **What percentage of the company's revenue is sourced from government contracts?** The size of a potential claim under the FCA can be up to triple the amount of the contract value.
- **How siloed is the company's process for assessing contractual representations to the government from its information security functions/organizations?** The more siloed the process, the more likely it is that there are not entirely accurate representations or certifications that a potential whistleblower can use in a complaint.
- **Are the company's processes for assessing representations made to the government limited to identifying affirmative evidence of a particular process or control?** If so, then it is essential to actively identify and review other sources of information within the organization that could be inconsistent with such representations.
- **Is incident response handling and reporting, and the results of the same, internalized into the company's process for ensuring that contractual obligations with the government are met?** One way for whistleblowers to identify a misrepresentation to the government is failure to disclose cybersecurity incidents pursuant to contractual obligations.
- **Does the organization have a process for handling cybersecurity issues raised by employees, and are such concerns routed to the appropriate internal functions (necessarily including legal)?** Understanding the source of a complaint early is an effective way to mitigate the whistleblower risk, as significant issues can be addressed and mitigated if engaged by the right resources in a timely fashion.

Asking these questions will likely give organizations a better sense of how ready it is to address and mitigate cybersecurity whistleblower risk. We discuss our recommendation as to how to practically address that risk below.

Conduct a Legal Risk Assessment Under Privilege

To address cybersecurity whistleblower risk, it is important to take a holistic approach in reviewing sources of information that may otherwise end up in whistleblower complaints. Additionally, it makes sense to conduct that review with outside counsel and under privilege to help address any curative disclosures that need to be made and to assist in the event of an actual litigation or governmental inquiry.

There is a good chance that the portion of an organization that assesses its cybersecurity against contractual representations made to federal agencies does so by looking for *affirmative* evidence that the representations are accurate. What is much less likely, is that the organization comprehensively analyzes the various records, documents, and statements available to its cybersecurity (or other) professionals that may be *inconsistent* with those representations. However, as seen in the *Markus* summary judgment opinion, it is that material that will make it difficult for a court to rule in a defendant's favor ahead of a trial because there are genuine issues of material fact.

The scope of material that can drive whistleblower risk is fairly large. Consider all of the language that may show up in reports (risk assessment, audit, forensic, incident response, penetration test, Service Organization Control or SOC 2, etc.), company resources (incident response platforms, risk registers, the System Security Plan, etc.), and communications (emails, texts, enterprise instant messaging environments, etc.) that a plaintiff's attorney can use to reflect inconsistent representations. It is far too common for issues to be identified in the course of normal business conduct aimed at maintaining an organization's security posture and then either go unaddressed or more likely be addressed but not memorialized. These issues can present the very real risk, for an

organization with reasonable cybersecurity procedures, of having to weigh the unknowns of going to trial against a multimillion-dollar settlement with a whistleblower and the federal government.

Authors

Explore more in

Privacy & Security Government Contracts Data Security Counseling and Breach Response

Related insights

Update

HHS Proposal To Strengthen HIPAA Security Rule

Update

California Court of Appeal Casts Doubt on Legality of Municipality's Voter ID Law