April 2025

Defense Contractor Settlement Underscores Need for Cybersecurity Compliance and Risk Mitigation

Key Notes:

- A Massachusetts defense contractor settled allegations of noncompliance with multiple cybersecurity compliance obligations imposed by its federal contracts.
- The settlement follows a recent increase in *qui tam* actions brought against contractors alleging false claims arising from certifications related to cybersecurity compliance and settlement agreements with the Department of Justice resolving such allegations.
- Contractors need to understand cybersecurity obligations imposed under federal contractors, engage appropriate resources to assess compliance with those obligations and investigate any instances of non-compliance.

A recent settlement agreement involving Massachusetts-based defense contractor MORSECORP Inc. highlights the growing risk of whistleblower claims and government scrutiny over cybersecurity compliance in federal contracts. MORSECORP agreed to pay $4.6 million to the U.S. Department of Justice (DOJ) to resolve allegations of non-compliance with cybersecurity standards. The settlement follows a trend of *qui tam* actions targeting contractors for failing to meet cybersecurity requirements mandated by regulations set forth in government contracts, including a pending action against Georgia Tech. The DOJ has intensified its focus on cybersecurity compliance through its Civil Cyber-Fraud Initiative, using the False Claims Act (FCA) as a mechanism to target contractors who fail to adhere to those requirements.

To mitigate these risks, contractors must fully understand the cybersecurity standards imposed by their federal contracts, implement necessary protocols, and accurately report their compliance efforts.

MORSECORP Inc. Settlement

In January 2023, a former MORSECORP employee filed a *qui tam* action in Massachusetts federal court, alleging that MORSECORP knew its cybersecurity protocols failed to meet federal standards as required under Defense Department (DOD) contracts. The complaint alleged the following cybersecurity failures by MORSECORP:

- From 2018 to 2022, MORSECORP used a third-party email communication provider without requiring and ensuring that the provider satisfied applicable Federal Risk and Authorization Management Program (or FedRAMP) standards imposed by DFARS 252.204-7012.
- From 2018 to 2023, MORSECORP failed to fully implement all cybersecurity controls required under NIST SP 800-171, as mandated by its defense contracts between 2018 and 2023.
- From 2018 to 2021, MORSECORP failed to maintain a consolidated written plan for each of its covered information systems describing system boundaries, operational environments, security implementation, and the relationships with or connections to other systems.
- In 2021, MORSECORP submitted a positive summary-level assessment score to the DOD's Supplier Performance Risk System (SPRS), which was later contradicted by an independent third-party assessment. MORSECORP did not update its score until June 2023.

Following the complaint, the DOJ issued a subpoena to MORSECORP regarding its cybersecurity practices. Under the settlement agreement, MORSECORP paid $4.6 million

to the DOJ with the relator receiving approximately $851,000.

Recent Cybersecurity Non-compliance Claims

The MORSECORP settlement follows increased legal actions brought against contractors and universities alleging failures of cybersecurity compliance as well as DOJ settlements regarding FCA violations related to cybersecurity requirements. In February 2025, Health Net and its parent, Centene Corp., paid $11.25 million to settle allegations of false cybersecurity certifications under a DOD contract. Among Health Net's alleged violations was its failure to follow its system security plan for identifying and addressing network vulnerabilities.

In August 2024, the DOJ intervened in a *qui tam* action against Georgia Tech, alleging cybersecurity lapses in DOD contracts. The university is accused of failing to secure information systems processing, storing, and transmitting controlled unclassified information (CUI). The complaint further alleges that the university failed to submit a summary-level score in SPRS for the information systems utilized by research labs performing DOD contracts and instead knowingly submitted an enterprise summary-level score for the entire Georgia Tech campus to mislead the DOD. Georgia Tech has moved to dismiss the complaint, which remains pending.

Contractor Focus on Cybersecurity Compliance

The MORSECORP settlement and recent related actions underscore the importance of proactive cybersecurity compliance and the risks created by not understanding those compliance requirements and not implementing appropriate protocols to ensure ongoing compliance and reporting. Contractors should take the following actions to reduce the risk of allegations of non-compliance with cybersecurity requirements:

- Review current federal contracts and active solicitations to understand the requirements to process, store, generate, or transmit CUI and the cybersecurity compliance standards and obligations imposed on the contractor. Federal regulations, particularly DOD regulations, establish specific cybersecurity compliance obligations, including the requirement to report NIST SP 800-171 compliance to SPRS. These requirements will continue evolving with the implementation of DOD regulations for its Cybersecurity Maturity Model Certification 2.0 standards.
- Ensure that the information security policies include a robust vendor management process. It is essential for companies to analyze and verify the technical, physical, and administrative security controls of their third-party IT service providers, which may include documentation of third-party cybersecurity audits, attestations, and certifications. This process also includes ensuring any data processing contracts between a company and its service provider memorialize information security requirements and properly allocate the liability and risks between the parties.
- Engage appropriate resources to determine current compliance with applicable cybersecurity standards and implement a program to address existing gaps to achieve necessary compliance. Outside counsel can assist with this assessment process regarding the application of specific regulations and the attachment of legal privilege to the assessment's findings and determinations.
- Where potential non-compliance with applicable cybersecurity standards is identified, engage counsel to assist with an investigation of alleged non-compliance. The increase in *qui tam* actions by current and former employees alleging contractor false claims related to cybersecurity certifications underscores the need to review potential instances of non-compliance and take appropriate actions to address any actual cybersecurity violations.

FOR MORE INFORMATION

For more information, please contact:

Mark J. Cipolletti
Partner, White Collar Defense & Investigations
202.973.2786
Mark.Cipolletti@ThompsonHine.com

Francis E. (Chip) Purcell, Jr.
Partner and Practice Group Leader, Government Contracts
202.263.4118
Chip.Purcell@ThompsonHine.com

Brittain Shaw
Partner, White Collar Defense & Investigations
212.908.3940
Brittain.Shaw@ThompsonHine.com

Steven G. Stransky
Partner and Co-Chair, Privacy & Cybersecurity
216.566.5646
202.263.4126
Steve.Stransky@ThompsonHine.com
Certified Information Privacy Professional/Government (CIPP/G)
Certified Information Privacy Professional/United States (CIPP/US)