Cybersecurity Failures Lead to False Claims Act Case Against Government Contractor

Aloke S. Chakravarty, John A. Marty

Published 04/14/2025

In a striking move at the end of March, the U.S. Department of Justice ("DOJ") announced a $4.6 million settlement with MORSE Corp Inc. ("MORSE"), a defense contractor based in Cambridge, Massachusetts, for falsely certifying that the company complied with cybersecurity requirements. The announcement underscores the potentially severe consequences for government contractors that fail to comply strictly with cybersecurity requirements in government contracts. The settlement also serves as a stark reminder of the critical importance of an effective cybersecurity compliance program.

What You Need to Know:

- Government contractor settles with DOJ for $4.6 Million Settlement relating to cybersecurity lapses.
- Whistleblower will receive $851,000 as part of the settlement.
- Settlement highlights the importance of thorough compliance with cybersecurity requirements, accurate reporting, and regular audits to avoid severe penalties.

The settlement, announced by the U.S. Attorney for the District of Massachusetts on March 26, 2025, stemmed from a lawsuit filed under the *qui tam* whistleblower

provisions of the False Claims Act. The relator (*i.e.*, the whistleblower) will receive a $851,000 share of the settlement, further illustrating the powerful incentives for whistleblowers to report on compliance failures, and the importance of company compliance programs preempting and addressing these failures.

What Happened: A Breakdown of Cybersecurity Missteps

MORSE faced serious allegations tied to its cybersecurity practices in contracts with the United States Army and Air Force. Key admissions in the settlement reveal:

- **Inadequate Third-Party Security:** From January 2018 to September 2022, MORSE used a third-party email host without ensuring the host complied with required Federal Risk and Authorization Management Program ("FedRAMP") security standards.
- **Incomplete Implementation of Cybersecurity Controls:** Between January 2018 and February 2023, MORSE failed to fully implement the cybersecurity controls specified in NIST Special Publication 800-171.
- **Lack of Consolidated Security Plans:** MORSE did not maintain a consolidated written system security plan for its information systems from January 2018 to January 2021, despite contractual requirements that it do so.
- **Inaccurate Compliance Reporting:** MORSE submitted an inaccurate cybersecurity compliance score to the U.S. Department of Defense and failed to correct it in a timely manner.

Lessons: Best Practices Based on False Claims Act Enforcement

This settlement is a reminder of what a powerful tool the FCA can be to ensure compliance with government cybersecurity standards. Accordingly, government contractors should review their cybersecurity compliance programs, and consider relevant updates where appropriate, to ensure they include the elements below.

- **Ensure Compliance with specified Cybersecurity Requirements:**
    - Thoroughly review and understand all cybersecurity requirements specified in government contracts.
    - Implement all necessary cybersecurity controls as outlined in applicable standards (e.g., NIST SP 800-171).
- **Use secure third-party services:**

    - Verify that any third-party service providers comply with required security standards, such as FedRAMP Moderate baseline.
    - Maintain documentation of the third-party's compliance with these standards.
- **Maintain accurate and up-to-date security documentation:**
    - Develop and maintain a consolidated written system security plan for all covered information systems.
    - Ensure that the plan describes system boundaries, environments of operation, security requirement implementations, and connections to other systems.
- **Accurate Reporting:**
    - Document and provide accurate cybersecurity compliance scores and updates to the Department of Defense or other relevant agencies.
    - Regularly review and seasonably update compliance scores to reflect the current state of cybersecurity measures.
- **Promptly address deficiencies:**
    - Conduct regular cybersecurity audits and address any identified deficiencies promptly.
    - If notified of any discrepancies or issues by third-party consultants, take immediate action to correct and update relevant reports.
- **Training and Awareness:**
    - Ensure that all employees involved in cybersecurity and compliance are well-trained and aware of the requirements and the importance of adhering to them.
    - Provide a secure confidential internal reporting channel for whistleblowers.
    - Conduct regular training sessions and updates on cybersecurity best practices and compliance obligations.
- **Collaboration with legal and compliance teams:**
    - Collaborate closely with legal and compliance teams to ensure all contractual and regulatory requirements are being met.
    - Regularly consult with these teams to stay updated on any changes in cybersecurity laws and standards.

MORSE's settlement is a cautionary tale about the increasing risks of cybersecurity failures beyond data breaches. In a heightened cyber and national security threat environment, and with DOJ strongly indicating that they intend to use the False Claims Act more aggressively to address cyber failings, this settlement is the latest example of the government leveraging its enforcement options to address contractors' cybersecurity deficiencies. As the MORSE episode demonstrates, adhering to best compliance practices is still worth the investment for government contractors. And to the extent there is any doubt, the MORSE settlement should assist inhouse legal and compliance teams demonstrate the even greater costs of non-compliance.

Further, DOJ's increased vigilance in the area of cybersecurity for contractors is driven in part by the risk that sensitive data may be vulnerable to foreign adversaries; as the recent implementation of the critical national security program to protect Americans' sensitive data from foreign adversaries indicates, companies that process data that would be valuable to foreign adversaries should ensure they are in compliance with all federal cybersecurity standards.

Authors

Aloke S. Chakravarty

Partner

(617) 912-0949 |

View bio

John A. Marty

Associate

(412) 209-2566 |

View bio

Related Services

Cybersecurity & Privacy

White Collar & Government Enforcement