Akin Gump
STRAUSS HAUER & FELD LLP

Cyber Security Update:
False Claims Act Risks for IT Contractors

SUMMARY: Federal contracts impose significant information security requirements on IT contractors. A contractor's noncompliance with cybersecurity requirements can heighten the risk of whistleblower lawsuits under the False Claims Act (FCA) and fraud investigations by law enforcement. Three main areas of risk are (1) data access by users not in the United States, (2) mismanagement of secure shell keys and (3) ineffective monitoring of employees. A robust compliance review and continuous monitoring are effective ways to mitigate the risk of FCA liability.

I. Background

The National Institute of Standards and Technology (NIST) publishes guidance for federal information systems to ensure that sensitive information remains confidential when stored outside of federal systems. Security standards in NIST 800-53 (updated 2013) were government-specific and were passed from agencies to contractors through contract clauses. Security standards in NIST 800-171 (updated 2015) are contractor-specific and apply to components of nonfederal information systems that process, store or transmit sensitive information.

II. Breaches of Cybersecurity Contract Terms May Create FCA Liability Risks

The FCA imposes civil liability on any person who knowingly presents a false claim to the government for payment or approval. IT contractors should be aware that a breach of cybersecurity requirements may create FCA liability risks. Under a hotly debated legal theory labeled "implied certification" (currently before the U.S. Supreme Court), some courts have concluded that the act of submitting a claim for reimbursement under a federal contract itself might, under certain circumstances, imply compliance with applicable regulations and contract provisions, including cybersecurity rules. Under this theory, relators may attempt to argue that FCA liability can stem from failing to meet cybersecurity obligations in a manner that can be characterized as "reckless."

III. Common Operational Practices May Cause Compliance Risks

IT contractors face the challenge of providing effective and efficient services to the government while also trying to avoid cybersecurity risks. There are three main areas of concern:

- **Data access by users not in the United States**. To provide the best service at reasonable rates, IT contractors often delegate responsibilities to lower-cost employees and contractors located overseas. However, providing overseas developers with the access they need to complete system development or maintenance tasks can inadvertently compromise the security of highly sensitive data. Granting access to systems with confidential information to noncitizens without security clearances may violate the terms and conditions contained in telecommunications contracts.
- **Mismanagement of secure shell keys**. More than half of all websites use a version of the secure shell data-in-transit protocol when maintaining their systems, making it a ubiquitous tool among IT contractors. However, mismanagement of secure shell keys can create data "backdoors." Failure to

rotate keys, to restrict the use of root access keys, or to monitor the use of keys may violate NIST standards and place the contractor at risk.

- **Ineffective monitoring of employees**. Most experienced IT contractors have adopted sophisticated measures to protect highly sensitive data, such as controlling physical access to the data center, establishing secure zones in the network and using appropriate encryption tools. However, corporate policies are effective only when they are followed closely by employees. Ineffective monitoring of employees to ensure compliance can lead to allegations that a contractor “recklessly disregarded” its obligations under an IT contract.

CONCLUSION: In this rapidly changing technological landscape, managing risk and ensuring compliance are effective ways to mitigate the risk of FCA liability.