



LOGZONE Marks a First in FCA Cyber Enforcement

By Mark Coakley, Cybersecurity and AI Law Report

The DOJ's June 17, 2026, [settlement](#) with defense contractor LOGZONE signals that government contractors can face False Claims Act (FCA) liability for cybersecurity compliance failures even without a whistleblower complaint, voluntary self-disclosure (VSD) or data breach, making accurate compliance assessments more critical than ever. LOGZONE agreed to pay \$507,144 to resolve allegations that it knowingly failed to comply with cybersecurity requirements in contracts with the Department of the Navy (Navy). The company had earned \$682,193 from these contracts.

"Government contractors that obtain sensitive defense information in administering their contracts must follow required cybersecurity standards," Assistant AG Brett Shumate of the DOJ's Civil Division said in the [press release](#) announcing the settlement. "The Justice Department will continue to investigate potential violations of these cybersecurity requirements in order to protect this critical information from external threats."

"The cybersecurity provisions of federal contracts are critical to protecting sensitive information that may be transmitted in carrying out the mission of the contracts," Navy Vice Admiral Stephen Tedford, director of the Defense Contract Management Agency (DCMA), said in the press release. "DCMA will continue to ensure that contractors are fulfilling these obligations."

This article explores the implications of the settlement, with compliance lessons from partners at Joseph Greenwald & Laake, Foley & Lardner, Parker Poe and Crowell & Moring.

See "[What to Know \(and Do\) About DOJ's Efforts to Identify and Prosecute Cybersecurity Fraud Under the False Claims Act](#)" (Oct. 30, 2024).

Basis for the DOJ's FCA Claims

The settlement resolved DOJ allegations under the FCA that LOGZONE had knowingly submitted false or fraudulent claims for payment on two Navy con-

tracts for which LOGZONE had not complied with the contracts' cybersecurity requirements.

The Contracts

The contracts were awarded in March 2021 and November 2022. In October 2021, LOGZONE submitted to the Department of Defense (DoD) a perfect self-assessment score of 110 for its implementation of National Institute of Standards and Technology Special Publication 800-171 security controls (NIST 800-171). NIST 800-171 constitutes the specific cybersecurity standard mandated for all contractors handling Controlled Unclassified Information (CUI) on their networks and the DoD explicitly incorporates it in several cybersecurity clauses in the Defense Federal Acquisition Regulation Supplement, a set of rules used by the DoD for buying goods and services, Kate Growley, a partner at Crowell & Moring, told the Cybersecurity and AI Law Report.

Alleged Failure to Comply With NIST

From May 2021 to March 2025, LOGZONE allegedly failed to implement certain aspects of NIST 800-171 that, if not implemented, could lead to exploitation of the system or the exfiltration of sensitive defense information.

These issues were identified in February 2024 when the DCMA assessed LOGZONE's implementation of NIST 800-171, which resulted in LOGZONE receiving a score of -170, at the low end of the possible score range of -203 to 110. The DCMA score was 280 points lower than that assessed by LOGZONE previously.

The DOJ maintains that if a company committed in a contract to implement certain cybersecurity measures and the U.S. government believes that the company knowingly fell short of those commitments but was nonetheless paid for the contract by the U.S. government, that is considered a false claim, Growley explained.

Coordinated Settlement Efforts

The settlement resulted from a coordinated effort involving the DOJ's Civil Division, Commercial Litigation Branch, Fraud Section and the U.S. Attorney's Office for the Northern District of Alabama, with assistance from the Navy's Office of the General Counsel, the Naval Criminal Investigative Service, the Department of the Army Criminal Investigation Division and the Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC). The latter is the DoD organization that is responsible for auditing and evaluating defense contractors' cybersecurity compliance.

See "[Navigating DoD's Final Cybersecurity Maturity Model Certification Program Rules](#)" (Oct. 1, 2025).

Settlement Implications

Companies like LOGZONE that end up settling with the DOJ suffer reputational damage and may find it harder to get future government contracts, several of the experts noted.

Growing Role of Audits in FCA Investigations

Most past FCA settlements were initiated by a whistleblower complaint, Growley noted. The LOGZONE case is different because the government's own assessment revealed a stark discrepancy between the contractor's reported compliance score and its actual score, providing evidence of a potential knowing contract violation. That is important, she added, as the DIBCAC audit mechanism is "one that a lot of contractors often overlook, until they receive notice that DIBCAC would like to do an audit of their NIST 800-171 implementation." An assessment requirement in a government contract is "not just a compliance mechanism, it could also be an enforcement tool as well," she said.

It is also notable that the public settlement materials do not describe the issues involving LOGZONE as having been voluntarily self-disclosed to the government, as they were in Verizon's 2023 FCA settlement, William Kirkwood, a partner at Parker Poe, told the Cybersecurity and AI Law Report.

The LOGZONE case further demonstrates that a breach is not a prerequisite to potential FCA exposure based on alleged contractual cybersecurity noncompliance, Kirkwood noted.

It is unclear what initially drew the government's attention to LOGZONE, and the public record does not disclose what prompted DIBCAC's Medium Assessment of the company, Kirkwood noted. The case highlights how audits and assessments can be important in FCA investigations, he said.

Potential for Significant Exposure

The \$507,144 settlement, which came to "a little over one third of the total contract value," illustrates the potentially significant FCA exposure that can result from cybersecurity noncompliance, Growley noted. The figure included restitution, which was subject to multipliers. Similar calculations could produce much larger settlements for contractors with larger government contracts. "This is a data point to look to when trying to anticipate what a settlement figure could look like for other contractors that are in the midst of an investigation," she said.

The settlement also highlights the uncertainty surrounding FCA damages in cases involving no data breach or other obvious harm, Growley continued. The government has suggested that, because cybersecurity is considered fundamental to the performance of any contract, especially with the DoD, any short-

comings could undermine the value of the entire contract. That theory remains largely untested and is often a point of negotiation during FCA investigations. The issue is particularly noteworthy in the LOGZONE case because the company was not providing cybersecurity products or services, she pointed out.

Score Discrepancies Can Invite Scrutiny

The government decided to make an example out of LOGZONE, at least in part because of the 280-point gap between its self-assessed score and the score determined by DIBCAC, Veronica Nannis, a partner at Joseph Greenwald & Laake, told the Cybersecurity and AI Law Report. The large gap suggested that the company had knowingly presented false information. Other companies with such large gaps may also risk being made an example by the government. If LOGZONE had produced a more honest score and presented a plan for improvement, the government may not have gone forward with enforcement.

The gap in scores is important under the FCA because it is evidence of materiality, a key element to a prosecution under the FCA, Nannis explained. The government clearly would not have paid under the contracts had it known that the assessment score gap was so large, making the misrepresentation material. A smaller gap, by contrast, may have been immaterial if it would not have affected the government's payment decision.

It is an oversimplification to say that the size of a score gap correlates to the risk of being investigated, but there is an element of truth to that correlation, Nannis said.

The 280-point gap between LOGZONE's reported self-assessment score of 110 and DIBCAC's subsequent assessment score of -170 was prominently identified in the government's settlement materials, but it would not be wise to try to set a numerical threshold for what makes a company safe or unsafe in terms of representations to the government, as there can be many different reasons why there are problems with self-assessed scores, Kirkwood cautioned. There is no numerical safe zone: even a small discrepancy can warrant scrutiny if a representation was inaccurate. But FCA exposure remains fact-specific and does not automatically follow from any score difference.

Enforcement Risk Not Limited to Large Contracts

There is a misconception that a contractor must be large and handle large dollar contracts to attract FCA attention, Kirkwood said. The settlement identifies \$682,193.37 in payments under the two Navy contracts at issue, and LOGZONE is not among the largest prime contractors in the federal market ranked in the Washington Technology Top 100.

See "[Understanding and Implementing DoD's Cybersecurity Requirements](#)" (Aug. 17, 2022).

Practical Lessons

There are several compliance lessons to be learned from the LOGZONE settlement, the experts agreed.

Understand Contractual Obligations Before Signing

When pursuing an opportunity, government contractors should closely examine the contract and understand exactly what it requires, regardless of the size of the contract, Kirkwood advised. Contract review should be conducted by a team of both lawyers and “program people, quality people, cybersecurity and IT personnel, and various other subject matter experts.” AI tools can be helpful with contract review but should not be completely trusted due to the risk of mistakes and hallucinations, he cautioned.

Be Diligent in Self-Assessment

Companies must be diligent about how they self-assess contractual cybersecurity compliance scores before posting them, Growley instructed. They should ensure that they evaluate such self-assessments in accordance with the [DoD's assessment methodology](#).

Companies have to make sure that they are complying with everything in U.S. government contracts – not just hoping to comply in the future – while also being transparent with the government, Nannis said.

Settle Early

The financial penalty for LOGZONE would have been higher if it had not settled before litigation, Nannis emphasized. “The best time to settle is during the investigation phase. The government will negotiate” then and will usually not demand full restitution or the full punitive payments available under the FCA, she explained.

Conduct a Privileged Internal Investigation

If a government contractor determines that its cybersecurity program may be deficient, it should promptly conduct a privileged internal investigation, Joseph Swanson, a partner at Foley & Lardner, recommended. The investigation should include interviews with key stakeholders and a review of contracts and the cybersecurity program to determine whether any government contracting or other regulatory violations occurred, he told the Cybersecurity and AI Law Report.

To help maximize privilege, counsel – ideally, outside counsel – should direct and oversee the investigation so that the work supports the provision of legal

advice, Swanson continued. Companies also should limit dissemination of investigation findings and carefully manage the work product generated during the investigation. If privilege is not maintained, those materials could provide regulators or plaintiffs' attorneys with a roadmap to the underlying issues and remediation efforts, he cautioned.

See "[FirstEnergy: Best Practices for Preserving Privilege in Internal Investigations](#)" (Jan. 21, 2026).

Consider Voluntary Self-Disclosure

If an internal investigation raises concerns about breaches of government contracts or other regulatory violations, a company should consider making a VSD to the DOJ or the contracting agency, Swanson advised. Although the consequences of a VSD can be difficult to predict, various programs encourage companies to promptly disclose cybersecurity compliance failures. A company's disclosure and remediation efforts may influence whether an enforcement action is initiated or mitigate any resulting penalties, he said.

The appropriate recipient of a VSD could depend on the contract wording, agency and nature of the potential violation, Swanson continued. Some agencies, including the DoD, have their own self-disclosure procedures, while the DOJ maintains separate self-disclosure programs. For a self-report to the DOJ, companies also must determine whether to disclose to Main Justice or to a local U.S. Attorney's Office based on the issues involved and available reporting mechanisms, he added.

Maintain a Strong Cybersecurity Compliance Program

A good compliance program exists in reality, not just on paper, Swanson said. Robust compliance programs include an independent compliance officer with authority to act and a mechanism, such as a hotline or email address, for reporting compliance concerns. The reporting mechanism should be monitored, and concerns should be pursued in a way that maximizes privilege, he advised.

Cybersecurity compliance programs should include data mapping, regular internal audits, gap assessments and solid documentation practices, Kirkwood recommended.

A sound compliance program provides independent oversight free from revenue or operational pressures that may create a conflict of interest, Nannis said. GCs should be seasoned, independent, empowered to address noncompliance, and report directly to the CEO and board or solely to the board.

Effectively Share Responsibilities

Legal departments, compliance teams and CISOs should not operate in silos, Swanson advised. They should communicate regularly to foster an apprecia-

tion of each department's role and responsibilities, although budget constraints and lack of engagement may present challenges. One of the best ways to encourage collaboration is through informal interactions, which could include "going to lunch regularly," he recommended.

Regularly Verify Representations

Companies should periodically verify that representations made in government contracts remain accurate, Swanson suggested. Quarterly or annual certifications based on internal compliance reviews, analogous to how public companies report financial statements, can help achieve that goal, he said.

To support that process, companies can maintain a centralized register of material representations made to the government, Kirkwood recommended. The register should include review dates and a mechanism for updates whenever contract modifications change applicable requirements.

Create and Preserve Documentation

Companies should create and preserve documentation of their contractual compliance efforts, Kirkwood advised, including self-assessment records, and the underlying methodology, scope, supporting evidence, remediation records and approvals.

Employee training also should be documented, Swanson suggested.

As part of the broader documentation effort, companies should maintain a system security plan documenting how they satisfy each NIST cybersecurity requirement, including supporting evidence and identifying any gaps, Growley recommended. A plan of action and milestones (POA&M) should document how the company intends to address identified gaps, including its remediation plan and timeline. The system security plan should explain how the company assessed compliance, including whom it consulted, the documents it reviewed and any screenshots or other evidence demonstrating that controls were in place at the time of the assessment, she elaborated. Such evidence "will be very useful in demonstrating the reasonableness of how a company reached that control and how, if there were mistakes, they were honest ones and are less likely to rise to the level of false claims exposure," she said.

Consider an Assessment Appeal

DIBCAC often comes up with scores with which companies do not agree, Growley noted. If a company does not agree with a score, it has the right to submit a reclama, which is an interim appeal. "It is not a light lift to submit a reclama. It requires careful consideration from both the cybersecurity and legal teams. But it gives a company the opportunity to ensure that it can set the record straight and avoid an unnecessarily low DIBCAC score," she said.

Enforcement Priorities

The U.S. government's focus on cybersecurity enforcement began in earnest in late 2021 under the Biden administration and remained in full force under Trump 2.0, Nannis noted, adding that this will likely continue regardless of which party controls Congress or wins the White House in 2028.

According to anecdotal evidence, there has been an increase in the number of DIBCAC assessments in 2026, Growley observed.

Continued Focus on Defense Contractors

Although the LOGZONE case was brought by the DOJ, the DoD started the investigation and was the DOJ's client, Nannis emphasized. In cases like this, the client agencies are "ultimately the ones that are going to drive whether or not something gets prosecuted and enforced," she noted.

The settlement shows that the DOJ continues to have a significant interest in cybersecurity compliance when it comes to federal government contractors, Swanson warned. "We can expect continued enforcement activity in this space." Compliance officers, GCs and CISOs are "wise to pay attention to this area, especially if their organization has any kind of federal government contract and particularly if they do any contracting work with the Department of Defense where the standards are even more rigorous" than those required by many other agencies.

LOGZONE is an example of how the Civil Cyber-Fraud Initiative continues to be focused on the compliance with NIST 800-171 and "aggressively pursuing" violations, Growley highlighted. There have been "several settlements under the DOJ Civil Cyber-Fraud Initiative that have turned on allegations that contractors misrepresented the degree of compliance with that standard," she noted.

The LOGZONE settlement underscores that FCA cyber enforcement is not limited to big defense contractors, Nannis said. Instead, the government is sending a broader message that companies must comply with the cybersecurity requirements in their federal contracts. LOGZONE-style enforcement is not confined to Navy contractors, she added. "It is for any government contract that has cybersecurity requirements in it. This case is a warning."

Civilian Contractors Also Under Scrutiny

The LOGZONE settlement is instructive of the similar potential risk that federal contractors face in the civilian space, according to Growley. "There have been other settlements that turned on contracts with civilian agencies. One great example is the Illumina settlement that was announced in 2025 and was based on contracts with a multitude of agencies across the civilian sector."

Government contractors should understand that the government is likely to continue focusing on cybersecurity compliance beyond DoD contracts, Kirkwood said. Civilian contracts and assistance instruments – including certain grants and loans – may contain cybersecurity requirements. Their terms and enforcement mechanisms may differ materially from DFARS 252.204-7012 and NIST SP 800-171, but companies should identify and comply with the requirements applicable to their particular award and ensure that their representations to the government are accurate.

© 2026 Mergermarket Limited. All rights reserved.