

Alert | Government Contracts



August 2025

DOJ Settles Cybersecurity FCA Claims With PE Firm and Government Contractors

On July 31, 2025, the Fraud Section of the U.S. Department of Justice's Commercial Litigation Branch (Fraud Section) announced new settlement agreements with government contractors to resolve their respective False Claims Act (FCA) liabilities arising out of cyber fraud allegations. These settlements mark the Fraud Section's fifth and sixth cyber fraud settlements of 2025, indicating a continued focus on leveraging the FCA's civil tools to ensure government contractors comply with cybersecurity controls.

Recent DOJ False Claims Act Settlements for Cybersecurity Violations

- **Aero Turbine and Gallant Capital Partners** – In coordination with the U.S. Attorney's Office for the Eastern District of California, DOJ announced a **settlement** with defense contractor Aero Turbine Inc. (ATI) and private equity firm Gallant Capital Partners LLC to resolve FCA liability for alleged cybersecurity violations. Gallant owned a controlling stake in ATI during the alleged violations period. There has been no determination of liability under the settlement.
 - **The allegations:** Between January 2018 and February 2020, ATI allegedly failed to implement certain NIST SP 800-171 controls during its performance of a contract with the U.S. Air Force. By way of background, defense contractors must safeguard controlled unclassified information (CUI) according to the cybersecurity standards set forth in DFARS 252.204-7012, including NIST SP 800-171. Instead, ATI had allegedly assumed that its compliance efforts with export controls were sufficient to meet its cybersecurity obligations under NIST SP 800-171, but there was no proper

verification. Additionally, during a two-month period in 2019, ATI and Gallant allegedly failed to safeguard sensitive defense information when they provided files containing protected information to an external software company based in Egypt. The software company and its non-U.S. personnel were not authorized to receive such information under the Air Force contract, but ATI and Gallant allegedly failed to control the flow of CUI and limit access to the controlled information systems to authorized users.

- **The settlement:** ATI and Gallant voluntarily disclosed the alleged violations to the government, cooperated with the subsequent investigation, and took prompt remedial actions. DOJ credited ATI and Gallant for the self-disclosures pursuant to the Justice Manual guidelines, and the parties ultimately agreed to resolve ATI's and Gallant's FCA liability for \$1.75 million.
- **Illumina Inc.** – DOJ announced a multi-million-dollar settlement agreement in coordination with the United States Attorney's Office for the District of Rhode Island to resolve FCA claims arising from a whistleblower complaint regarding cybersecurity violations. This **settlement** alleged false claims by biotechnology company Illumina Inc. in connection with the sale of genomic sequencing systems to various defense and civilian agencies. There has been no determination of liability under the settlement.
 - **The allegations:** From February 2016 to September 2023, Illumina allegedly sold genomic sequencing systems with software that contained cybersecurity vulnerabilities and did not have adequate safeguards in place to address those vulnerabilities. DOJ contended that Illumina failed to properly support its personnel and systems that were responsible for product security, failed to correct known vulnerabilities, and falsely represented to government agencies that its software adhered to required cybersecurity standards. The underlying *qui tam* complaint (captioned *United States ex. rel. Lenore v. Illumina Inc.*, No. 1:23-cv-00372 (D.R.I.)) further alleged that Illumina falsely certified its products that had known cybersecurity vulnerabilities. For example, Illumina's products were scored as critically severe on the Common Vulnerability Scoring System – ranging from 7.4 to 10 – but allegedly continued to market and sell its products with elevated privileges and exposed credentials problems. Illumina also allegedly failed to comply with known cybersecurity standards, such as the FDA's Quality System Regulation controls or the NIST Framework for Improving Critical Infrastructure Cybersecurity. DOJ further contended that Illumina resisted internal efforts to mitigate or remedy known defects, failed to minimize discovered insider threats that date back to 2020, and failed to meaningfully respond to its own vulnerability reports.
 - **The settlement:** DOJ investigated the allegations against Illumina in response to a whistleblower complaint submitted by a former employee who had tried to escalate and address the company's cybersecurity vulnerabilities and was eventually terminated. Nearly two years after the *qui tam* complaint was filed, Illumina and DOJ agreed to resolve the FCA allegations for \$9.8 million (plus interest), of which \$1.9 million will be shared with the whistleblower.

Compliance Considerations from DOJ's Cyber-Fraud Initiative Enforcement Actions

These settlement agreements reflect continued activity by DOJ's **Civil Cyber-Fraud Initiative**, which launched in 2021. The initiative is focused on using enforcement mechanisms to build the cybersecurity of the federal government and its contractor industrial base. While the two matters arose from different allegations and factual postures, there are several lessons and trends that may be observed.

1. Companies may benefit from voluntary disclosures and cooperation with the government. Companies should ensure their ethics hotlines and government contracts compliance programs enable them to identify concerns, initiate investigations, and timely report any noncompliance.

2. The Aero Turbine and Gallant settlement confirms that liability for inadequate cybersecurity controls may extend beyond the government contractor that has privity of contract with the government. Subcontractors and affiliates must also be aware of their responsibilities to protect controlled information.
3. These settlements suggest that DOJ is examining cybersecurity obligations that extend beyond the requirements that the Department of Defense's acquisition regulations impose. Contractors should review all information security and cyber requirements in their government contracts, and ensure they understand the government's expectations surrounding what information must be protected and to what level.
4. Companies must properly identify controlled information, comply with restrictions on distribution, and flow down security controls, including when sharing that information with affiliates and their supply chains.
5. Companies must also have sufficient controls and procedures in place to confirm the accuracy of any representations made to the government.

Authors

This GT Alert was prepared by:

- **Eleanor M. Ross** | +1 202.530.8565 | Eleanor.Ross@gtlaw.com
- **Cassidy Kim** | +1 415.590.5133 | Cassidy.Kim@gtlaw.com
- **Olivia Bellini** | +1 703.903.7514 | Olivia.Bellini@gtlaw.com

Albany. Amsterdam. Atlanta. Austin. Berlin[~]. Boston. Charlotte. Chicago. Dallas. Delaware. Denver. Fort Lauderdale. Houston. Kingdom of Saudi Arabia^{*}. Las Vegas. London^{*}. Long Island. Los Angeles. Mexico City^{*}. Miami. Milan^{*}. Minneapolis. Munich[~]. New Jersey. New York. Northern Virginia. Orange County. Orlando. Philadelphia. Phoenix. Portland. Sacramento. Salt Lake City. San Diego. San Francisco. São Paulo[»]. Seoul[∞]. Shanghai. Silicon Valley. Singapore[~]. Tallahassee. Tampa. Tel Aviv[^]. Tokyo^{*}. United Arab Emirates[<]. Warsaw[~]. Washington, D.C. West Palm Beach. Westchester County.

*This Greenberg Traurig Alert is issued for informational purposes only and is not intended to be construed or used as general legal advice nor as a solicitation of any type. Please contact the author(s) or your Greenberg Traurig contact if you have questions regarding the currency of this information. The hiring of a lawyer is an important decision. Before you decide, ask for written information about the lawyer's legal qualifications and experience. Greenberg Traurig is a service mark and trade name of Greenberg Traurig, LLP and Greenberg Traurig, P.A. ~Greenberg Traurig's Berlin and Munich offices are operated by Greenberg Traurig Germany, LLP, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. *Operates as a separate UK registered legal entity. «Greenberg Traurig operates in the Kingdom of Saudi Arabia through Greenberg Traurig Khalid Al-Thebity Law Firm, a professional limited liability company, licensed to practice law by the Ministry of Justice. +Greenberg Traurig's Mexico City office is operated by Greenberg Traurig, S.C., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's Milan office is operated by Greenberg Traurig Studio Legal Associato, an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. »Greenberg Traurig's São Paulo office is operated by Greenberg Traurig Brazil Consultores em Direito Estrangeiro – Direito Estadunidense, incorporated in Brazil as a foreign legal consulting firm. Attorneys in the São Paulo office do not practice Brazilian law. ∞Operates as Greenberg Traurig LLP Foreign Legal Consultant Office. ~Greenberg Traurig's Singapore office is operated by Greenberg Traurig Singapore LLP which is licensed as a foreign law practice in Singapore. ^Greenberg Traurig's Tel Aviv office is a branch of Greenberg Traurig, P.A., Florida, USA. »Greenberg Traurig's Tokyo Office is operated by GT Tokyo Horitsu Jimusho and Greenberg Traurig Gaikokuhojimubengoshi Jimusho, affiliates of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. <Greenberg Traurig's United Arab Emirates office is operated by Greenberg Traurig Limited. ~Greenberg Traurig's Warsaw office is operated by GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k., an affiliate of Greenberg Traurig, P.A. and Greenberg Traurig, LLP. Certain partners in GREENBERG TRAURIG Nowakowska-Zimoch Wysokiński sp.k. are also shareholders in Greenberg Traurig, P.A. Images in this advertisement do not depict Greenberg Traurig attorneys, clients, staff or facilities. No aspect of this advertisement has been approved by the Supreme Court of New Jersey. ©2025 Greenberg Traurig, LLP. All rights reserved.*