Shumaker

SEPTEMBER 8, 2026 | PUBLICATION

DOJ's $2 Million Honeywell Settlement Reinforces Cybersecurity as a False Claims Act Risk

For government contractors, cybersecurity compliance is no longer solely an information-security issue. Increasingly, it is also a question of contractual accuracy, corporate governance, and potential False Claims Act liability.

INDUSTRY SECTOR

Technology

SERVICE LINE

Data Privacy
Technology

RELATED PROFESSIONALS

C. Jade Davis

MEDIA CONTACT

Wendy M. Byrne
wbyrne@shumaker.com

The U.S. Department of Justice (DOJ) announced on September 1, 2026, that Honeywell Aerospace Inc. agreed to pay $2,042,518 to resolve allegations that a business unit failed to comply with cybersecurity requirements applicable to a Department of Defense (DoD) contract. Honeywell Aerospace, headquartered in Phoenix, Arizona, provides aerospace products and solutions to government and commercial customers; prior to June 29, 2026, when it became a standalone public company, it operated as a business segment of Honeywell International Inc., of Charlotte, North Carolina.

The settlement adds to a growing body of cybersecurity-related False Claims Act "FCA) enforcement actions. In fiscal year 2025 alone, DOJ recovered more than $52 million across nine cybersecurity-related FCA settlements as part of a record-shattering $6.8 billion in total FCA recoveries. The Honeywell matter provides an important warning for companies doing business with the federal government: a cybersecurity representation that does not match the organization's actual security environment can create legal exposure even when the government does not allege that a data breach occurred.

What DOJ Alleged

According to DOJ, from April 2020 through December 2023, a business unit of Honeywell International Inc. allegedly submitted claims for payment while failing to comply with cybersecurity requirements specified in National Institute of Standards and Technology Special Publication 800-171 (NIST SP 800-171) with respect to one of its networks. Those cybersecurity requirements were incorporated into the applicable DoD contract and regulations.

NIST SP 800-171 establishes safeguards designed to protect Controlled Unclassified Information (CUI) in nonfederal information systems. For DoD contractors handling covered defense information, these

requirements have been incorporated into federal contracting requirements through the Defense Federal Acquisition Regulation Supplement (DFARS), including DFARS 252.204-7012.

The Honeywell matter is particularly notable because it originated with a whistleblower complaint filed by Rachel Tenney, a former Honeywell employee, under the FCA's qui tam provisions. Tenney will receive approximately $375,823 from the settlement. The lawsuit is captioned *United States ex rel. Rachel Tenney v. Honeywell International Inc.*, Civil Action No. 3:22-cv-129 (W.D.N.C.). DOJ emphasized that the settlement resolves allegations only and that there has been no determination of liability.

That fact should be significant to business leaders. Cybersecurity deficiencies may be identified not only through a breach or regulatory investigation, but also by employees, former employees, contractors, auditors, consultants, or government assessors who discover a disconnect between an organization's stated compliance posture and its actual practices.

Honeywell is Part of a Broader Enforcement Pattern

The Honeywell settlement should not be viewed in isolation.

In June 2026, DOJ announced a $507,144 settlement with LOGZONE Inc., a Huntsville, Alabama defense contractor, involving alleged failures to implement NIST SP 800-171 controls under two Navy contracts. Notably, LOGZONE had submitted a perfect self-assessment score of 110 in October 2021, but a February 2024 assessment by the Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) produced a score of -170—near the bottom of the applicable scoring range of -203 to 110. Unlike many recent FCA cybersecurity matters, the LOGZONE case was not initiated by a whistleblower but instead was triggered by the government's own assessment process, signaling that proactive government audits can themselves lead to FCA enforcement.

In March 2025, DOJ resolved a $4.6 million settlement with MORSECORP Inc., a Cambridge, Massachusetts defense contractor, for alleged failures to comply with cybersecurity requirements in contracts with the Departments of the Army and Air Force. DOJ alleged that MORSE had submitted a self-assessment score of 104, near the top of the possible range, but that a third-party cybersecurity consultant subsequently determined the actual score to be -142. MORSE also admitted that it used a third-party email hosting service that did not meet security requirements equivalent to the FedRAMP Moderate baseline.

In September 2025, the government reached an $875,000 resolution with Georgia Tech Research Corporation (GTRC) following allegations that the institution failed to install antivirus tools on systems conducting sensitive DoD cyber-defense research, failed to implement a required system security plan, and submitted a false cybersecurity assessment score of 98 based on a "fictitious" or "virtual" environment that did not correspond to any actual contracting system.

In May 2025, DOJ announced an $8.4 million settlement with Raytheon Company, RTX Corporation, and related Nightwing entities to resolve allegations that Raytheon failed to develop a required system security plan and failed to implement required cybersecurity controls on an internal development system used for unclassified DoD contract work.

Taken together, these matters demonstrate that DOJ is examining more than whether an organization has suffered a cyberattack. Enforcement has focused on whether required controls were actually implemented, whether system security plans accurately described the environment, whether deficiencies were properly documented, and whether cybersecurity scores and other compliance representations submitted to the government were supportable.

Why This Matters Beyond the IT Department

For executives and boards, the key lesson is that cybersecurity certifications should be treated with the same seriousness as other representations made to obtain or retain government business.

A company may have a sophisticated cybersecurity program and still face substantial risk if there is a disconnect between what the contract requires, what management believes has been implemented, what technical personnel have actually deployed, and what the company ultimately represents to the government.

That gap can be particularly dangerous under the FCA because cybersecurity deficiencies can potentially become allegations concerning the accuracy of claims for government payment. As DOJ Deputy Assistant Attorney General Brenna E. Jenny has stated, the government's cyber enforcement is not about punishing victims of data breaches but rather addressing misrepresentations to the government where representations of compliance do not align with actual practices.

The Honeywell settlement also illustrates the importance of escalation procedures. Security personnel may identify control deficiencies that initially appear to be ordinary remediation items. If those deficiencies concern controls required by a government contract, however, the issue may have implications extending well beyond information security.

The Role of Self-Disclosure and Remediation

DOJ's enforcement history also provides an important counterpoint: identifying a cybersecurity deficiency does not necessarily mean a company should conceal it until remediation is complete.

In a July 2025 settlement involving defense contractor Aero Turbine Inc. and its private equity owner Gallant Capital Partners LLC, the companies agreed to pay $1.75 million to resolve allegations of cybersecurity noncompliance in an Air Force contract. DOJ specifically acknowledged the companies' voluntary self-disclosures, cooperation with the government's investigation, and prompt remedial action. Those actions resulted in cooperation credit under Justice Manual § 4-4.112, reportedly yielding an approximately 1.5x damages multiplier—well below the typical 2x FCA multiplier.

The lesson is not that every technical deficiency requires immediate disclosure. Rather, companies should have a process for determining when a technical finding implicates a contractual certification, government representation, reporting requirement, or other legal obligation.

That determination should involve legal, compliance, procurement, and cybersecurity personnel rather than remaining exclusively within the IT organization.

What Business Leaders Should Do Now

Companies that contract with the federal government, particularly DoD contractors and subcontractors, should consider several immediate steps:

1. **Validate cybersecurity representations against the actual environment.** Do not assume previously submitted certifications, assessment scores, or self-assessments in the Supplier Performance Risk System (SPRS) remain accurate. The LOGZONE and MORSECORP matters demonstrate that self-assessed scores will be scrutinized and potentially tested against independent assessments.
2. **Review NIST SP 800-171 implementation evidence.** Organizations should be able to demonstrate how applicable controls are implemented, not simply state that they are compliant. With the Cybersecurity Maturity Model Certification (CMMC) program now finalized and third-party assessments beginning in

2026, the evidentiary expectations for contractor cybersecurity compliance are increasing.

3. **Reconcile technical findings with contractual obligations.** Vulnerability assessments, penetration tests, internal audits, and third-party assessments should be evaluated for potential implications under government contracts.
4. **Review system security plans and remediation documentation.** Documentation should accurately describe current systems, boundaries, controls, deficiencies, and corrective measures. The Georgia Tech and Raytheon matters illustrate that the absence or inaccuracy of a system security plan can itself form the basis of FCA allegations.
5. **Create a legal escalation process.** Cybersecurity personnel should know when an identified deficiency must be escalated to legal or compliance personnel before additional representations or certifications are made.
6. **Consider whistleblower risk when responding to internal concerns.** Employees who raise cybersecurity compliance concerns should have meaningful channels for escalation and investigation. The Honeywell, MORSECORP, and Georgia Tech matters all originated from whistleblower complaints filed by current or former employees.
7. **Evaluate self-disclosure when significant compliance gaps are identified.** The Aero Turbine settlement demonstrates that timely self-disclosure, cooperation, and remediation can meaningfully reduce FCA penalties, and DOJ has increasingly been formalizing cooperation credit in cybersecurity matters.
8. **Preserve evidence of remediation.** Organizations should document when deficiencies were identified, how they were investigated, who evaluated their contractual significance, and when corrective measures were completed.

Practical Takeaways

The Honeywell settlement reinforces an important shift in federal cybersecurity enforcement: cybersecurity compliance is increasingly becoming enterprise legal risk.

For organizations receiving federal funds or performing government contracts, technical controls, contractual promises, security assessments, and payment claims are becoming increasingly interconnected. A cybersecurity deficiency therefore cannot always be treated as an isolated IT problem, particularly as CMMC implementation introduces independent third-party verification requirements that will make compliance gaps harder to overlook.

Business leaders should be asking a broader question: Can we substantiate what we are telling the government about our cybersecurity program?

As DOJ's recent cases demonstrate, the answer should be supported by evidence rather than assumption.

DOJ Press Release: Honeywell Aerospace Inc. Agrees to Pay Over $2M to Settle False Claims Act Allegations (Sept. 1, 2026)

Shumaker