United States ex rel. Tenney v. Honeywell: The Facts

An Executive Examination of the Public Record, Cybersecurity Obligations, and Management Accountability

David W. Koran

CyberAB Registered Practitioner Advanced
ISO/IEC 27001 Auditor and Implementer

September 2026

Summary

The question raised by the Honeywell cybersecurity settlement is whether a contractor can account for the security it promised the government when the evidence inside the business is examined. A company may have a written security plan, a separate network for sensitive work, and products that generate alerts, yet still be unable to explain who had access, what an alert meant, or why an investigation was closed. The distance between those representations and the operating record is where the Honeywell complaint places its allegations.

On September 1, 2026, the Department of Justice announced that Honeywell Aerospace Inc. agreed to pay $2,042,518 to resolve False Claims Act allegations involving NIST SP 800-171 requirements on one network. The announced settlement covers April 2020 through December 2023 and provides $375,823 to former employee Rachel Tenney. DOJ expressly states that there has been no determination of liability. Those are established facts about the resolution; the detailed account of events remains an account alleged in a complaint.

This paper examines that distinction through the redacted complaint, the court's unsealing order, and DOJ's announcement. It follows the alleged relationship between the government work, the network protecting it, the warnings employees raised, and the claims submitted for payment. The complete settlement agreement was not among the materials reviewed, so the analysis does not assume that every allegation was accepted by the government or resolved on its merits. The management value of the case lies in understanding the decisions it places under scrutiny, which are decisions defense contractors make long before anyone files a lawsuit.

What the Public Record Establishes

The action is United States of America ex rel. Rachel Tenney v. Honeywell International Inc., case number 3:22-cv-00129-MEO-DCK, in the Western District of North Carolina, Charlotte Division. Tenney filed the complaint on March 25, 2022. The phrase "ex rel." identifies a proceeding brought by a private relator on behalf of the government. The defendant named in the pleading is Honeywell International, while the company identified by DOJ as agreeing to the settlement is Honeywell Aerospace. A precise account preserves the distinction between those entities.

The order filed August 24, 2026, confirms that the United States intervened in part and authorizes the release of three documents: the government's notice and request, Document 51; the redacted complaint, Document 51-2; and the order itself, Document 53. All other papers and orders then on file, including the original complaint, remain sealed pending further order. The document the public can examine is therefore a deliberately limited record, and partial intervention cannot be read as adoption of every allegation within it.

The order does not identify a settlement agreement or explain the continued seal over particular records. If an agreement was already among the filed papers, the order leaves

it sealed, but the order does not establish that it was filed there. The reason for the settlement amount, the full scope of the negotiated release, and the disposition of claims beyond the announced resolution cannot be reconstructed from these documents. That boundary matters because the complaint describes considerably more conduct than the short settlement announcement explains.

The Work and the Network

According to the complaint, the government work involved quantum computing contracts and a Special Use Network called the Gray Network. The environment allegedly held government data, engineering drawings, technical specifications, simulations, and research associated with sensitive defense and intelligence programs. Honeywell used the network to support the contracted work and represented it as a means of protecting the information involved. The description appears in paragraphs 77 through 100 and 119 through 120 of the complaint.

The familiar management analogy is a separate production area created for a customer with special requirements. The separation is useful only if the controls required for that work operate inside the area. Moving the work behind a boundary does not establish who may enter, what equipment is permitted, which activities are recorded, or who investigates an exception. A network has the same dependency. Its separation from ordinary corporate operations must be accompanied by the people and processes needed to administer it.

Tenney alleges that the Gray Network was separated from corporate systems while lacking protections that existed elsewhere in Honeywell. She describes reliance on a firewall, devices that could leave the facility, and a corporate Security Operations Center that could not monitor the segregated environment. The allegation is consequential because it describes a boundary that limited the reach of corporate security without providing an adequate replacement inside it. For a contractor using an enclave for Controlled Unclassified Information (CUI), the practical question is whether separation has preserved accountability or merely moved the work beyond the people responsible for it. These remain allegations about Honeywell, set out in paragraphs 121 through 133 and 215 through 216.

The Controls Behind the Representation

The complaint organizes the alleged deficiencies around malicious code protection, access control, incident response, and oversight of suspicious activity. These are recognizable operating disciplines. They concern whether the company knows which devices are connected, whether the devices receive protection, whether access can be attributed to an authorized person, and whether an alert reaches someone capable of acting on it. The allegations therefore describe a failure to carry basic administrative responsibilities through the environment supporting the contract.

Paragraphs 142 through 146 reproduce internal exchanges about antivirus coverage and the difficulty of identifying computers outside normal domain management. One

statement says protection had previously been deployed to workstations but not servers. The issue is coverage and administration, not the name of the product: using Microsoft Defender does not itself establish noncompliance. NIST SP 800-171 requires malicious code protection at designated locations and the updating and scanning needed to support it. Management needs evidence that the protection reaches the relevant systems and continues to operate there.

Access presents the same problem from a different direction. Tenney alleges that personnel working exclusively on commercial matters accessed the Gray Network, that remote access was inadequately controlled, and that encryption and automatic session termination were deficient. When suspicious activity appeared, administrators allegedly could not reliably identify the people responsible or the purpose of the activity. The operational consequence is straightforward: the ability to investigate depends on the ability to distinguish authorized use from everything else. That distinction becomes difficult to reconstruct after the event if it was never enforced or recorded before it. The access allegations occupy paragraphs 158 through 194.

The complaint further alleges that the Gray Network's incident response capability was not tested and that monitoring products generated alerts without adequate follow-up by qualified personnel. It cites requirements including automatic session termination under 3.1.11 and incident response testing under 3.6.3. NIST also addresses incident handling and action on security alerts. These requirements explain why the alleged omissions matter, but the record contains no judicial finding that these particular controls were violated. The practical point is that purchasing detection and maintaining response capability are separate management responsibilities, and the first produces little assurance when the second is absent.

The Decision to Close the Incident

SolarWinds gives the complaint its most detailed account of how those weaknesses allegedly came together. Tenney alleges that compromised Orion software was present and that activity after the server was shut down required further investigation. The complaint describes unexplained remote sessions, configuration changes, and more than 1,200 megabytes moving from a central server to the compromised Orion server. Administrators allegedly could not account for the users or explain all the activity, yet management closed the matter without an adequate investigation. The central allegations appear in paragraphs 155 through 156 and 221 through 230.

The data movement should be described precisely. Movement to a compromised server within the described environment does not establish that the same volume of government information was taken outside the company, nor does it establish who obtained it. Paragraph 201 acknowledges that it remained unknown whether SolarWinds attackers acquired the government information. The available record supports examining the adequacy of the investigation, while leaving the ultimate extent of any compromise unresolved.

The more significant management evidence is the correspondence the complaint reproduces. In a January 6, 2021 email quoted in paragraph 272, Tenney challenged the basis for treating the investigation as complete. She described unfinished analysis, missing logs, unexplained remote activity, and software deployment that no team member could account for. In subsequent exchanges she sought the information used to justify closure and questioned how she could evaluate a response she was prohibited from reviewing. Those exchanges potentially support the allegation that specific concerns reached management, although the pleading does not supply the complete underlying email record or independent forensic verification.

The comparison with a quality investigation is useful. A manufacturer that closes a nonconformance needs a reason supported by the record: what was examined, what was found, what was corrected, and why the remaining condition is acceptable. Closing the record does not change the condition of the product. Closing a cyber incident has the same limitation. Management's decision should follow the evidence available and account for what remains uncertain, because a closure statement can later be examined alongside the warnings that preceded it.

When Security Becomes a Payment Question

The connection to the False Claims Act appears in the complaint's allegation that Honeywell continued invoicing while making false representations about network security and incidents. Paragraph 241 expressly alleges continued claims for payment and false certifications. The pleading also alleges that compliance was material to the government's payment decision. The theory concerns what the contractor knowingly represented and received payment for, with the alleged security deficiencies and ignored warnings supplying the factual basis for that account.

A deficiency alone does not establish liability. Under 31 U.S.C. 3729, knowledge includes actual knowledge, deliberate ignorance, and reckless disregard, while materiality concerns the capacity to influence payment or receipt of money or property. The applicable legal elements still have to be established. For management, the useful implication is that a known discrepancy between promised performance and actual practice deserves attention before it becomes part of a payment representation. A company cannot assess that discrepancy if the people responsible for contracts and finance receive assurances disconnected from the operating evidence.

The reporting duty also stands on its own contractual foundation. DFARS 252.204-7012 addresses safeguarding applicable covered contractor systems and reporting incidents affecting covered systems or information. It defines rapid reporting as within 72 hours of discovery; the trigger is not limited to proven theft. The facts and applicability must be assessed against the clause, and the relevant historical contract version must be checked. An organization that waits for certainty about exfiltration may be asking a narrower question than the reporting obligation requires.

The complaint does not identify a failed Cybersecurity Maturity Model Certification assessment or an inaccurate Supplier Performance Risk System score as its basis. Its

account is built around the underlying work, the required security, incident handling, and payment. The implication for contractors is that an assessment calendar and a contractual obligation operate on different terms. A change to the former does not by itself amend the latter, and management's responsibility to understand the security being represented continues between assessments.

What the CUI Allegations Actually Say

The identification of Controlled Unclassified Information, or CUI, deserves a separate examination because it determines what information and systems require protection. Paragraphs 85 through 87 describe contractual restrictions covering hardware photographs and information concerning the design or capabilities of COMSEC and communications protection equipment. The complaint therefore alleges specific notice about protected information, rather than relying only on the fact that Honeywell performed government work.

That specificity is stronger than the complaint's broader treatment of legacy For Official Use Only markings. Paragraph 89 treats FOUO and CUI as interchangeable, which is too broad as a general rule. The National Archives explains that some information carrying an FOUO marking may not qualify as CUI. The applicable authority and information category still have to support the designation; commercial sensitivity or an internal confidentiality label cannot settle the question by itself.

For a defense contractor, this distinction prevents two different mistakes. One is to assume that every item connected with a government customer automatically requires the same treatment. The other is to disregard substantive contractual restrictions because the information carries an older marking. The Honeywell pleading should be evaluated against the particular contract language and information it describes. It does not decide every scope dispute another manufacturer may face, and its shorthand about FOUO should not be adopted as a compliance rule.

The Employee and the Escalation Process

Tenney's account also places the company's response to an employee under scrutiny. She alleges that her responsibilities included identifying threats, investigating anomalous activity, escalating concerns, and assisting with compliance. After raising the SolarWinds concerns, she says she was removed from related duties, instructed not to pursue or debate the issue, threatened, subjected to investigations, and stripped of supervisory responsibilities. She alleges that these circumstances forced her departure. The retaliation allegations appear in paragraphs 267 through 292 and in the federal and Minnesota retaliation counts.

The materials reviewed do not establish the disposition of those claims. Their governance significance nevertheless follows from the function the employee was performing. An escalation process works only when the substance of a concern reaches someone able to evaluate it. If a disagreement about the evidence becomes a dispute over whether the employee is cooperative, management risks losing the very

information the process was intended to surface. Technical disagreement requires examination of the technical record, with an escalation route that remains available when the person receiving the warning is also responsible for the decision being questioned.

Before the Record Is Reconstructed

The materials reviewed do not establish Honeywell's total cost, the government's damages calculation, or the rationale for the negotiated amount. The settlement cannot responsibly be used to calculate the price of ignoring cybersecurity requirements. Its more useful lesson concerns the evidence a company creates while performing the work: the device inventory, the access record, the alert, the email requesting investigation, the explanation for closure, and the representation associated with payment.

Those records already exist in some form in most organizations. The work for management is to make them agree with one another. A security plan should describe the environment that actually operates, an incident closure should be supported by the investigation that preceded it, and a representation to the government should reflect what the responsible people can substantiate. When those records diverge, leadership needs a process that brings the discrepancy forward and resolves it rather than allowing each department to retain its own version of the facts.

The Honeywell complaint illustrates the questions a later investigation may ask, without establishing how every disputed fact would have been decided at trial. A contractor can ask those questions now, while its own personnel and records are available and corrective action remains an ordinary management task. Once an outside party is reconstructing the company's decisions from emails, invoices, and incident logs, management has lost control over the timing of that examination. The opportunity is to establish a defensible record while the decisions are being made.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced (RPA) and the founder of a consulting practice serving Defense Industrial Base contractors and their legal counsel. His work focuses on CMMC readiness, enablement, and implementation. He holds ISO/IEC 27001 certifications as an auditor and implementer, is an Associate Member of the American Bar Association Section of Public Contract Law, and is the author of The CMMC Decision. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

United States ex rel. Rachel Tenney v. Honeywell International Inc., No. 3:22-cv-00129-MEO-DCK (W.D.N.C.). Redacted complaint, Document 51-2, filed August 18, 2026; underlying complaint dated March 25, 2022. References in this paper use the numbered paragraphs of the complaint.
https://storage.courtlistener.com/recap/gov.uscourts.ncwd.107612/gov.uscourts.ncwd.107612.51.2.pdf

United States ex rel. Rachel Tenney v. Honeywell International Inc., same case. Order, Document 53, signed August 21 and filed August 24, 2026. Identifies the records unsealed and confirms partial government intervention.
https://storage.courtlistener.com/recap/gov.uscourts.ncwd.107612/gov.uscourts.ncwd.107612.53.0.pdf

U.S. Department of Justice, Honeywell Aerospace Inc. Agrees to Pay Over $2M to Settle False Claims Act Allegations of Failing to Comply with Cybersecurity Requirements in a U.S. Department of Defense Contract, September 1, 2026.
https://www.justice.gov/opa/pr/honeywell-aerospace-inc-agrees-pay-over-2m-settle-false-claims-act-allegations-failing

31 U.S.C. 3729, False claims. Subsections (a) and (b) address prohibited conduct, knowledge, and materiality.
https://www.law.cornell.edu/uscode/text/31/3729

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting. Current text consulted for the general framework; historical contract applicability requires review of the incorporated clause.
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

National Institute of Standards and Technology, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations, NIST SP 800-171 Revision 2, February 2020, updated January 28, 2021. Sections 3.1.11, 3.6.1, 3.6.3, and 3.14.2 through 3.14.5.
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

National Archives and Records Administration, Information Security Oversight Office, CUI Program Blog, July 2020 questions and answers. Addresses the relationship between legacy FOUO markings and CUI.
https://isoo.blogs.archives.gov/2020/07/

Public materials reviewed through September 7, 2026. This paper does not describe the complete settlement agreement or reconstruct sealed material.