

DOJ Cybersecurity Settlement Reinforces the Need for Defensible NIST SP 800-171 Evidence

Government contractors should connect representations, system scope, and control operation before claims reach the government

SCOTTSDALE, AZ, UNITED STATES, September 2, 2026 /EINPresswire.com/ -- The U.S. Department of Justice announced on September 1 that Honeywell Aerospace Inc. agreed to pay \$2,042,518 to resolve allegations under the False Claims Act involving cybersecurity requirements in a U.S. Department of Defense contract. DOJ said the alleged conduct concerned a business unit's compliance with NIST Special Publication 800-171 on one network from April 2020 through December 2023. The claims resolved by the settlement were allegations only, and there was no determination of liability.

For defense contractors and subcontractors, the development underscores a practical distinction between having cybersecurity documentation and being able to substantiate contract-facing representations with current, scoped evidence. Control ownership, system boundaries, remediation decisions, and the records supporting an assessment should tell a consistent story before an invoice, certification, score, or other representation is submitted.

Lazarus Alliance

Proactive Cyber Security



LAZARUS ALLIANCE
We Stop Threats Before They Become Catastrophes.

DOJ CYBERSECURITY SETTLEMENT REINFORCES THE NEED FOR DEFENSIBLE NIST SP 800-171 EVIDENCE

Government contractors should connect representations, system scope, and control operation before claims reach the government.



BUILDING A DEFENSIBLE NIST SP 800-171 READINESS PROGRAM

- 1. DEFINE & CONNECT SCOPE**
Map applicable contract clauses to the exact environment in scope.
- 2. ALIGN POLICIES WITH PRACTICE**
Verify policies and procedures match how systems are actually operated.
- 3. IDENTIFY GAPS**
Use qualified assessment and testing to find control deficiencies.
- 4. REVIEW & RETAIN EVIDENCE**
Keep dated evidence that shows how findings were addressed or accepted.
- 5. REMEDIATE & MAKE DECISIONS**
Correct gaps or formally accept residual risk with leadership approval.
- 6. MAINTAIN & MONITOR**
Continuously monitor controls and update evidence to sustain compliance.

THE RESULT

Stronger risk decisions. More defensible compliance. Greater confidence in the face of audits and scrutiny.

REDUCED RISK EXPOSURE | STRONGER GOVERNANCE | MORE EFFICIENT OPERATIONS | DEFENSIBLE COMPLIANCE

KEY TAKEAWAYS

- SETTLEMENT SPOTLIGHTS REPRESENTATION RISK**
Allegations under the False Claims Act focused on NIST SP 800-171 compliance on one network (Apr 2020–Dec 2023).
- DOCUMENTATION IS NOT ENOUGH**
Organizations must substantiate contract-facing representations with current, scoped evidence.
- CONNECT THE DOTS**
Scope, policies, implementation, remediation decisions, and assessment records must tell a consistent story.
- KNOW WHO REPRESENTS UNDERSTAND THE BASIS**
Ensure the right people are authorized to make representations—and that they rely on credible, current evidence.
- EVIDENCE-LED READINESS REDUCES RISK**
Identify gaps early, test controls, and retain dated evidence of how findings were addressed.

"A cybersecurity representation should be the end of an evidence process, not the beginning of a scramble to reconstruct one. Contractors need a clear system boundary, accountable control owners, current test results, and records that show how leadership reached its conclusion. That discipline supports better risk decisions and more defensible compliance."
—Michael Pletters, CEO & Founder, Lazarus Alliance

LAZARUS ALLIANCE PROACTIVE CYBERSECURITY™
Lazarus Alliance is a veteran-owned global provider of Proactive Cybersecurity™, specializing in cybersecurity audit and compliance, risk assessment and management, privacy audit and compliance, vulnerability and penetration testing, and IT policies and governance. Founded in 2005, we help organizations attain, maintain, and demonstrate information security and compliance excellence.

AUTHORIZED QMCP CIPAD | FedRAMP | AZIA-ACCREDITED FEDRAMP SPAD | PCI DSS QUALIFIED SECURITY ASSESSOR (QSA) | SCOTTSDALE, ARIZONA | lazarusalliance.com

DOJ Cybersecurity Settlement Reinforces the Need for Defensible NIST SP 800-171 Evidence



Contractors need a clear system boundary, accountable control owners, current test results, and records that show how leadership reached its conclusion. That discipline supports defensible compliance.”

Michael Peters, CEO & Founder, Lazarus Alliance

A defensible readiness program should connect the applicable contract clauses to the exact environment in scope; verify that policies match operating practice; identify gaps through qualified assessment and testing; and retain dated evidence showing how findings were evaluated, corrected, or formally accepted. Leadership should also understand who is authorized to make cybersecurity representations and what evidence that person relies on.

Lazarus Alliance helps organizations evaluate cybersecurity and compliance programs, assess risk, test controls, and strengthen governance across complex regulatory and contractual environments. For organizations preparing for

CMMC or managing NIST SP 800-171 obligations, an evidence-led review can help expose disconnects among policy, technical implementation, assessment results, and executive representations. Engagement scope and any assessor-independence requirements should be confirmed before work begins.

“A cybersecurity representation should be the end of an evidence process, not the beginning of a scramble to reconstruct one. Contractors need a clear system boundary, accountable control owners, current test results, and records that show how leadership reached its conclusion. That discipline supports better risk decisions and more defensible compliance.” - Michael Peters, CEO & Founder, Lazarus Alliance

ABOUT LAZARUS ALLIANCE

Lazarus Alliance is a veteran-owned global provider of Proactive Cybersecurity®, specializing in cybersecurity audit and compliance, risk assessment and management, privacy audit and compliance, vulnerability and penetration testing, and IT policies and governance. Founded in 2000, the firm helps organizations attain, maintain, and demonstrate information security and compliance excellence across complex regulatory environments.

Lazarus Alliance is an authorized CMMC Third-Party Assessment Organization (C3PAO), an A2LA-accredited FedRAMP Third-Party Assessment Organization (3PAO), and a PCI DSS Qualified Security Assessor (QSA). Headquartered in Scottsdale, Arizona, Lazarus Alliance serves organizations ranging from startups to multinational enterprises with cybersecurity, privacy, risk, governance, and compliance expertise.

Michael Peters
Lazarus Alliance, Inc.
+1 8888967580

[email us here](#)

Visit us on social media:

[LinkedIn](#)

[YouTube](#)

[X](#)

This press release can be viewed online at: <https://www.einpresswire.com/article/939064705>

EIN Presswire's priority is source transparency. We do not allow opaque clients, and our editors try to be careful about weeding out false and misleading content. As a user, if you see something we have missed, please do bring it to our attention. Your help is welcome. EIN Presswire, Everyone's Internet News Presswire™, tries to define some of the boundaries that are reasonable in today's world. Please see our Editorial Guidelines for more information.

© 1995-2026 Newsmatics Inc. All Right Reserved.