COMPLIANCE

NEWSLETTER

October 21, 2026



Cybersecurity and Supply Chain Risk

Cybersecurity requirements increasingly shape IT acquisition, subcontract management, and software supply chain oversight.

For government contractors, managing these connected risks means protecting sensitive information and ensuring subcontractors and software providers meet applicable contract requirements.

Integrating these checks into purchasing and supplier oversight strengthens security, supports compliance, and reduces operational risk.

The Importance of Compliance

Integrating cybersecurity into purchasing and supplier oversight helps protect sensitive data, reduce risk, and meet contract requirements.

Connect with our experts to discuss your contracting challenges or explore solutions tailored to your team.

Operational Vulnerabilities

In cybersecurity and supply chain management, noncompliance can put sensitive information and contract performance at risk. Potential consequences include:

- **Security Breaches** that expose data or disrupt operations.
- **Financial Losses** from recovery costs, corrective actions, or contractual remedies.
- **Contract Consequences,** withheld payments or termination.
- **Reduced Eligibility** for future awards when required security standards are unmet.
- **Legal Exposure** when inaccurate compliance claims or certifications are submitted.
- **Damage to Customer** trust and business relationships.
- **Counterfeit Components,** malicious software, or unauthorized changes.

info@jawhite.com 803-750-9150 www.jawhite.com