

The Future of **Defense Sourcing** Secure, Intelligent, and Sovereign

Executive Summary

For Original Equipment Manufacturers (OEMs) and Prime contractors supporting the Department of War, the digital handoff of sensitive intellectual property or controlled information is a primary point of vulnerability. Fragmented email communication and insecure file transfers to the supply base represent a significant risk of data exposure. Paperless Parts provides a secure platform that enables sourcing teams to protect Controlled Unclassified Information (CUI) while leveraging advanced manufacturing intelligence to de-risk the supply chain. This document details our strategic approach to FedRAMP compliance and our Radar intelligence framework.

A Foundation of Trust

FedRAMP Moderate Equivalence

Paperless Parts is hosted on AWS GovCloud (US), a sovereign cloud environment restricted to U.S. Persons. Our security program is built on the FedRAMP Moderate (NIST 800-53 Revision 5) baseline framework. To ensure the highest level of validation, the Paperless Parts Application was independently audited by Schellman, a top-tier FedRAMP-recognized Third-Party Assessment Organization (3PAO).

Through three consecutive annual assessments, Schellman has confirmed that Paperless Parts meets the requirements for FedRAMP Moderate Equivalence, implementing the 323 security controls designed to protect sensitive government data. This equivalency satisfies the standards required by DFARS 252.204-7012 for contractors using external cloud service providers to handle CUI. You can verify these requirements in the [official DoD CIO Memorandum on FedRAMP Equivalency](#).

Platform Data Protection and Resiliency

We protect OEM intellectual property through industry-leading encryption, rigorous backup protocols, and U.S. sovereignty:

- **Encryption in Transit:** All data moving between your browser and our platform is protected using FIPS 140-2 validated TLS 1.2 or higher.
- **Encryption at Rest:** Sensitive files and database records are encrypted using FIPS 140-2 validated AES-256 at the storage layer.
- **Disaster Recovery:** Data is backed up nightly with a resiliency model that ensures high durability and rapid recovery within the GovCloud environment.
- **Integrated Security:** Every file uploaded undergoes automated virus and malware scanning before processing.
- **U.S. Person Restriction:** Our platform and support operations are managed 100% by U.S. Persons on U.S. soil, fulfilling a critical requirement for the Department of War and ITAR-regulated data. Definitions for U.S. Persons can be found in [22 CFR § 120.62](#).

Privacy-Preserving AI

As Artificial Intelligence becomes a force multiplier for manufacturing efficiency, Paperless Parts ensures that innovation does not lead to data compromise. Our AI technologies are built on a Privacy-Preserving Architecture designed with strict security and governance guardrails:

- Based on Peer Reviewed Research: Paperless Parts Co-Founder and Chief Scientist, Scott Sawyer, presented on Privacy-Preserving AI for Document Understanding with Controlled Unclassified Information at the 2024 IEEE High Performance Extreme Computing (HPEC) Conference.
- In-Boundary Processing: All AI models run 100% within our FedRAMP Moderate-equivalent environment. This ensures that sensitive data processed by AI remains protected by the same FIPS 140-2 validated encryption and NIST 800-53 controls as the rest of the platform.
- Data Isolation and Privacy: Your data stays strictly within your tenant boundary and is never used to train a generative model used by another customer.
- No Public Model Training: Paperless Parts does not send your data to third-party providers where it could be used for global model training.
- Human-in-the-Loop Governance: Our AI is designed to assist, not replace. It provides suggestions for manufacturability and costing, but all decisions are reviewed and finalized by your team. Learn more about our AI Security and Privacy.

CONCLUSION

Cybersecurity is a journey rather than a destination. By partnering with Paperless Parts, manufacturers gain a foundation that is not only compliant with today's CMMC and FedRAMP standards but is also resilient against the threats of tomorrow. If you'd like more information, you may contact the Paperless Parts Security Team directly by emailing security@paperlessparts.com.