paperlessPARTS

10 CMMC-Related Questions to Ask Every Software Vendor You're Considering Partnering With

1. Determine the Security Baseline to be Validated

- **Requirement:** DFARS 252.204-7012 Paragraph (b)(2)(ii)(D) establishes that a cloud provider must meet requirements "equivalent" to the FedRAMP Moderate baseline. (https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012:~:text=(D)%C2%A0%20If,cyber%20incident%20damage%20assessment)
- **SaaS:** Is the SaaS platform FedRAMP Moderate Authorized or Equivalent?
- **On-premise:** Do you follow a recognized framework (like NIST 800-171) and provide a Software Bill of Materials (SBOM)?

2. Review the Body of Evidence

- **Requirement:** DoD CIO Memorandum: "Federal Risk and Authorization Management Program Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings," explicitly validates the **"**Equivalency**"** pathway for commercial vendors (like Paperless Parts) and defines the exact Body of Evidence (SSP, SAR, Attestation) required to prove it. (https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf)
- **SaaS:**
    - If the vendor holds a FedRAMP ATO - verify listing in FedRAMP Marketplace (https://marketplace.fedramp.gov/products).
    - If the organization is FedRAMP Moderate Equivalent, ask to see the System Security Plan (SSP), Customer Responsibility Matrix (CRM), and Security Assessment Report (SAR). Vendors should also be able to demonstrate zero open assessment items on the POAM, a requirement unique to equivalency.

    - The 3PAO should be listed on the CyberAB website for both cases. (https://cyberab.org/)
- **On-premise:** Can you provide a Security Hardening Guide and evidence of regular vulnerability scanning?

3. Validate the Encryption Standard

- **Requirement:** NIST SP 800-171 control 3.13.11 "Employ FIPS-validated cryptography when used to protect the confidentiality of CUI." (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf)
- **SaaS:** Do you use FIPS validated modules for data at rest and in transit?
- **On-premise:** Does the software utilize NIST-validated cryptographic modules for local data storage?

4. Verify US Personnel Only

- **Requirement:** The International Traffic in Arms Regulations. Code of Federal Regulations (CFR) Title 22, § 120.62**:** Defines "U.S. Person".
- **SaaS:** Are all system admins and support staff "US Persons"?
- **Requirement:** International Traffic in Arms Regulations
- **On-premise:** Are support technicians who might remote-in for troubleshooting "US Persons"?

5. Verify US Data Sovereignty

- **Requirement:** The International Traffic in Arms Regulations. Code of Federal Regulations (CFR) Title 22, § 120.50: Defines "Export," clarifying that data remaining in the U.S. (CONUS) is not an export. (https://www.ecfr.gov/current/title-22/chapter-I/subchapter-M/part-120/subpart-C/section-120.50)
- **SaaS:** Is all data (including backups and metadata) stored strictly within the US?
- **On-premise:** Does the software "phone home" to servers or update nodes outside the US? Is that connection FIPS compliant?

6. The Shared Responsibility Matrix (SRM) or Customer Responsibility Matrix (CRM)

- **Requirement:** CMMC Assessment Process (CAP) v1.0, Section 1.5.4 of this document explicitly instructs auditors to validate security through the review of the provider's Body of Evidence (BoE) and Shared Responsibility Matrix. (https://cyberab.org/Portals/0/Documents/Process-Documents/CMMC-Assessment-Process-CAP-v1.0.pdf)
- **SaaS:** Do you provide an SRM that defines the split of responsibilities between software provider and customer?
- **On-premise:** Do you provide a Configuration Matrix showing which settings we must enable to be CMMC-compliant?

7. Access Control & MFA

- **Requirement:** NIST SP 800-171, Control Number: 3.5.3, Identification and Authentication. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf)
- **SaaS or On-Prem:** Does the platform integrate with our Identity Provider (SSO) or require MFA for local logins?

8. Support Privileged Access

- **Requirement:** NIST SP 800-171, Control Number: 3.7.4, Maintenance. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf)
- **SaaS:** Are support sessions logged, monitored, and restricted by the Principle of Least Privilege?
- **On-premise:** Do you require a persistent "backdoor" (like a VPN), or do you support session-based screen sharing?

9. Incident Reporting (DFARS 7012)

- **Requirement:** DFARS 252.204-7012 (b)(2)(ii)(D)(c)

- **SaaS:** Are you prepared to rapidly report the discovery of any cyber incident to the DoD within 72 hours? (https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012:~:text=(c)%C2%A0%20Cyber%20incident%20reporting%20requirement.)
- **On-premise:** Will you notify us within 72 hours if a vulnerability in your code is exploited at other sites?

10. Auditability & Logging

- **Requirement:** NIST SP 800-171, Control Number: 3.3.2, Audit and Accountability. (https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf)
- **SaaS or On-Prem:** Does the platform track specifically who accesses or modifies controlled data? Can Administrators export these logs for a CMMC audit?

To learn more about how Paperless Parts fulfills these security requirements, visit www.paperlessparts.com/security.