2026

EXECUTIVE WHITE PAPER | NOVEMBER 2026

Right-Sizing Your CMMC 2.0 Boundary

How Government Contractors Can Modernize Business Operations While Protecting CUI

5
CMMC Level 2 asset categories to assess and document
Source: 32 CFR § 170.19

3
logical zones in the reference-only CUI-decoupled design
Source: Section 5, this paper

7
buyer due-diligence review areas before selecting a system
Source: Section 8, this paper

PUBLISHER
Scientific Systems & Software International, Corporation (SSSI)

DATE
November 2026

AUDIENCE
Government contractor executives

© 2026 Scientific Systems & Software International, Corporation (SSSI). xpdOffice™ is a product of SSSI. All rights reserved.

Executive summary

CMMC requirements need not force every corporate business application into the same technical environment as Controlled Unclassified Information (CUI). Under 32 CFR § 170.19, Level 2 scope is determined through asset capabilities, security functions, actual data flows, and separation, not merely by whether a company performs defense work. A carefully designed separation between a CUI enclave and a non-CUI business platform may reduce assessment complexity, but the outcome must be validated for each contractor.

A reference-only pattern can support accounting, timekeeping, HR, CRM and project workflows while controlled artifacts remain in the customer's designated CUI environment. This paper explains the conditions, risks and due-diligence checks. It does **not** represent that xpdOffice currently holds a CMMC certification, FedRAMP authorization, or verified out-of-scope determination.

01 The business problem

Government contractors often operate disconnected systems for finance, timekeeping, contracts and HR. CUI requirements can make modernization appear to demand a single highly restricted enterprise-wide software boundary. That assumption can add cost and complexity. Equally, an assumption that ordinary business software is always outside CMMC scope can create security gaps. The right approach is evidence-based scoping.

02 Three questions before selecting a system

- **What information is involved?** Classify the actual fields, attachments, exports, logs and records. Proposals, pricing, SOWs and project details can be CUI when designated; their business label alone does not determine status.
- **What does the system do?** Assess whether it can store, process or transmit CUI, or provides security functions for the CUI environment.
- **How is it connected?** Examine browsers, endpoints, identity, integrations, APIs, link previews, indexing, backups, AI agents and support access.

03 CMMC Level 2 asset categories: practical interpretation

ASSET CATEGORY	WHAT TO ASSESS / DOCUMENT
CUI Assets	Process, store or transmit CUI; in scope for Level 2 assessment. Document in inventory, SSP and network diagram.
Security Protection Assets	Provide security capabilities to the assessment scope; in scope for requirements relevant to those capabilities, even without CUI payloads.
Contractor Risk Managed Assets	Can but are not intended to process/store/transmit CUI; require documented risk-based controls and limited checks per the rule.
Specialized Assets	Special-purpose assets such as certain OT, IoT, test equipment and GFE; document and apply category-specific assessment treatment.
Out-of-Scope Assets	Must satisfy the rule's inability-to-handle-CUI, non-security-protection and separation criteria; justification is required.

These categories are not interchangeable. In particular, "non-CUI" does not automatically mean "out of scope." Systems handling Federal Contract Information (FCI) may also have separate CMMC Level 1 obligations. See 32 CFR § 170.19 and the DoD Level 2 Scoping Guide.

> *"Non-CUI" does not automatically mean "out of scope."*

04 Cloud-provider obligations are a separate question

Under applicable DFARS 252.204-7012 requirements, an external cloud service provider used to store, process or transmit covered defense information must meet the applicable FedRAMP Moderate security baseline or DoD-recognized equivalency requirements. This is a cloud service offering and responsibility question, not a blanket requirement that every non-CUI business application be FedRAMP authorized. A cloud infrastructure provider's authorization does not automatically authorize the SaaS application built on it. The same clause also requires the contractor to ensure that the cloud service provider complies with its cyber incident reporting, malicious software, media preservation and protection, forensic access and damage assessment requirements (DFARS 252.204-7012(b)(2)(ii)(D)).

05 A reference-only CUI-decoupled design

The pattern uses three logical zones: (1) a business platform intended for non-CUI operational data; (2) the user's managed browser and endpoint; and (3) a separately protected customer CUI repository. An authorized user follows a neutral reference link and authenticates directly to the customer-controlled repository. The business platform must not retrieve, cache, preview, index or otherwise process CUI through the link.

> The design is a **candidate architecture**, not proof that any particular product or customer deployment meets the criteria. The endpoint and shared identity or security services require their own scoping analysis.

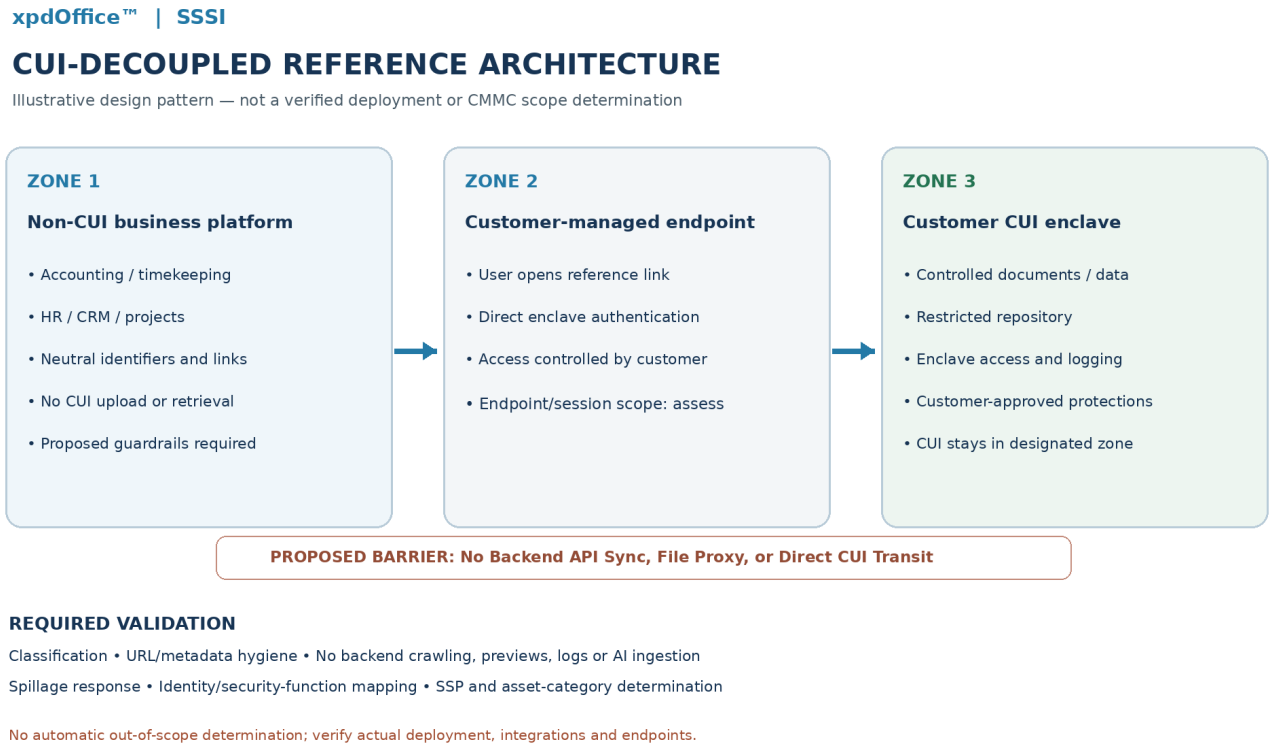


Figure 1. CUI-decoupled reference architecture

Illustrative only. The arrows represent a user-initiated navigation concept, not a validated network or integration flow. Neutral links and operational metadata must themselves be screened for CUI. "CUI stays in designated zone" means CUI remains within the assessed customer boundary, including authorized endpoints as applicable; no CUI enters the business platform. "No … logs" means no CUI content in business-platform logs; required security logging is retained.

06 Example operating workflow

- Store controlled technical volumes, CUI-marked SOWs, drawings and related controlled materials only in the customer's approved enclave.
- Record only reviewed, non-CUI operational identifiers, labor codes, dates and business transactions in the ERP. Never assume that all contract financial or project data is non-CUI.
- If supported and security-reviewed, place a neutral reference URL in the business system. A user opens the link directly; the customer enclave handles authentication and authorization.
- Verify that browser previews, URL titles, tokens, API connectors, audit logs, search, AI agents, notifications and exports do not expose CUI to the business platform.

07 Guardrails needed before operational use

- **Classification and intake:** written prohibited-data policy, field-level guidance, upload warnings and controls, and a tested CUI-spillage process.
- **Technical boundaries:** prohibit backend file fetching, attachment sync, preview generation, indexing, embedding and AI retrieval from CUI repositories.
- **Identity and endpoints:** review SSO, shared security services, privileged access, managed devices and incident response obligations.
- **Evidence:** asset inventory, data-flow diagrams, SSP treatment, customer responsibility matrix, configuration evidence and negative tests.

08 Buyer due-diligence checklist

REVIEW AREA	QUESTIONS TO RESOLVE
Information classification	Which specific fields, files, filenames, URLs and metadata may be CUI or FCI? Who approves classifications?
Application behavior	Can the SaaS receive CUI through uploads, email, API, integrations, logging, support tools, search or AI features?
Reference links	Does a user-initiated link avoid backend retrieval, previews, caching, tokens and content indexing? Has this been tested?
Security functions	Does the SaaS, its identity provider or monitoring service protect CUI assets? If yes, what scope category applies?
Cloud service evidence	If covered defense information enters a cloud offering, what DFARS/FedRAMP authorization or equivalency evidence applies?
Contractor governance	Are SSP, asset inventory, network/data-flow diagrams, user training, policies and spill response aligned?
Vendor assurance	Which controls are implemented, independently tested, planned or not supported? Is the responsibility matrix current?

09 What xpdOffice is pursuing

xpdOffice is an AI-native business operating system designed for GovCon and professional-services operations. Its product direction includes accounting, timekeeping, HR, contracts, projects, CRM and compliance workflows. The near-term commercial approach is to support non-CUI business operations with governed data boundaries; a dedicated CUI-capable offering is a separate longer-term initiative.

The company is targeting **Q1 2027 for an independent CPA review of DCAA accounting-system readiness**. This is a planning target, not a completed review or a DCAA certification. The preliminary **late 2027/2028** horizon for a CUI-capable offering remains conditional on discovery, engineering, investment and applicable security qualification. Current hosting, feature completeness and security controls must be confirmed against deployment evidence before customer-specific representations are made.

10 Conclusion

Modernization and CUI protection need not be opposing goals. A disciplined, evidence-backed boundary may let contractors improve ordinary business operations while protecting controlled information in a separately managed environment.

> *The result depends on implementation, not the diagram alone.*

References

- 32 CFR § 170.19, CMMC scoping (Electronic Code of Federal Regulations)
- DoD CIO, CMMC Resources and Documentation (CMMC program, scoping and assessment guides)
- DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting (Electronic Code of Federal Regulations)
- DoD CIO, CMMC Frequently Asked Questions
- DoD CIO memorandum, FedRAMP Moderate Equivalency for Cloud Service Provider's Cloud Service Offerings (December 21, 2023, PDF)

About SSSI

Founded in 1985, Scientific Systems & Software International, Corporation (SSSI) brings over four decades of experience delivering mission-critical information technology and software engineering solutions to the federal government.

Building on this heritage, SSSI developed xpdOffice™, an AI-Native Business Operating System designed for government contractors and professional services organizations. Moving beyond fragmented traditional business applications, xpdOffice connects enterprise operations, financial management, workforce management, contracts, projects, and customer relationships within a single, unified platform.

With AI-powered intelligence, integrated workflows, and compliance-aware controls, xpdOffice helps organizations make informed decisions, streamline operations, and manage their businesses with greater visibility, efficiency, and control.

Learn more at www.xpdOffice.com and www.sssi.net.

> **Notice:** Informational guidance only. A contractor should confirm the applicability of contractual requirements and its specific assessment scope with qualified security and compliance advisors.