WHITEPAPER

Closing the CMMC Gap: Visitor Management for Defense Contractors

How purpose-built visitor management maps directly to CMMC Level 2 physical security controls — and why generic solutions put your contracts at risk.

CMMC Level 2 | NIST SP 800-171 | DFARS 252.204-7012

6
PE Controls

3
Non-Deferrable

110
Total Practices

SecurePoint USA

SAM.gov Registered · Active CAGE Code · Built for Defense Contractors

securepointusa.com

2026

Originally published: 2026-03-01 Last reviewed: 2026-05-09

01 Executive Summary

The Cybersecurity Maturity Model Certification (CMMC) program codifies the security practices required for many Department of Defense contracts. Within Level 2, six Physical Protection (PE) controls govern facility access, visitor escorts, and physical-access logging.

Under current CMMC guidance, three of the six PE controls discussed in this paper are commonly identified as POA&M-ineligible at Level 2 (POA&M rules can change — confirm against 32 CFR Part 170 and DoD's current assessment guidance before relying on this).

Those three controls are PE.L2-3.10.3 (Escort Visitors), PE.L2-3.10.4 (Maintain Audit Logs), and PE.L2-3.10.5 (Control Physical Access Devices). Where they apply, the underlying capabilities should be operational when the assessor arrives, not deferred.

SecurePoint USA is a visitor management platform purpose-built for CMMC Level 2 alignment, ITAR/EAR-aware screening, and defense-contractor operational requirements. Capability fit for any specific environment is confirmed during scoping.

02 The CMMC Challenge for Physical Security

CMMC Level 2 aligns with NIST SP 800-171, Revision 2. Requirements apply to contractors handling Controlled Unclassified Information (CUI) across 14 domains. The Physical Protection domain defines six controls that directly govern visitor management.

PE.L2-3.10.1 POA&M Eligible

Limit Physical Access

Limit physical access to organizational information systems, equipment, and operating environments to authorized individuals. A sign-in sheet at the front desk is unlikely to satisfy "limit" on its own.

PE.L2-3.10.2 POA&M Eligible

Protect and Monitor the Physical Facility

Protect and monitor the physical facility and support infrastructure. Scope extends beyond visitors to surveillance, intrusion detection, and environmental controls.

PE.L2-3.10.3 **POA&M ineligible***

Escort Visitors

Escort visitors and monitor visitor activity. Where this control applies, every visitor in a CUI-adjacent space should have a designated escort, and escort enforcement should be operational at the time of assessment.

PE.L2-3.10.4 **POA&M ineligible***

Maintain Audit Logs

Maintain audit logs of physical access. Each check-in, check-out, escort assignment, badge issuance, and access event should be recorded in tamper-evident logs. Retroactively generated logs are unlikely to satisfy this control.

PE.L2-3.10.5

POA&M ineligible*

Control Physical Access Devices

Control and manage physical access devices. Visitor badges should be tracked from issuance through return or deactivation, with a documented chain of custody.

PE.L2-3.10.6

POA&M Eligible

Enforce Safeguarding at Alternate Sites

Enforce safeguarding measures for CUI at alternate work sites. Visitor management policies should extend uniformly to every site where CUI is handled.

** POA&M eligibility under CMMC has changed in past rule cycles and may change again. Confirm against 32 CFR Part 170 and the DoD's current CMMC Assessment Process before relying on deferrability.*

03 Why Generic VMS Solutions Often Fall Short

Most of the visitor management market is built for corporate offices, co-working spaces, and commercial real estate — environments with very different security requirements than CUI-handling facilities. Platforms designed to streamline lobby check-ins typically do not include controls that map cleanly to the PE family in NIST 800-171.

This is a design-goal mismatch, not a vendor critique: hospitality-first VMS products optimize for visitor experience; CMMC-aligned visitor management has to optimize for compliance evidence. The capability gaps below are the ones that show up most often in our assessments of competing tools.

Common Gaps in Generic VMS

- **ITAR/EAR Screening**
  Generic VMS products often do not capture citizenship or foreign-person status. Without that data, the system cannot route foreign nationals away from ITAR-controlled areas — and unescorted foreign-national access to controlled technical data may create deemed-export exposure under 22 CFR Part 120.
- **OFAC Sanctions**
  Many commercial VMS platforms do not screen visitors against the OFAC SDN list at pre-registration or check-in. Multi-list screening (SDN, Entity List, Denied Persons, OFSI) is generally outside the standard hospitality feature set.
- **Escort Enforcement**
  Many systems treat the escort as an optional data field. Optional capture is unlikely to satisfy PE.L2-3.10.3 if an assessor can demonstrate that a visitor can be checked in without an assigned escort.
- **Audit Log Integrity**
  SaaS platforms commonly allow administrators to edit or delete records. PE.L2-3.10.4 contemplates tamper-evident logs; mutable records are unlikely to satisfy that expectation.
- **Badge Lifecycle**
  Printing a visitor badge is not the same as managing one. PE.L2-3.10.5 contemplates tracking issuance, active use, return, and deactivation as a connected lifecycle.
- **Multi-Site Enforcement**
  PE.L2-3.10.6 contemplates consistent controls across facilities. Per-location configuration without centrally enforced policy guardrails leaves room for site-by-site drift.

Commercial VMS platforms optimize for visitor experience. CMMC-aligned visitor management has to optimize

for compliance evidence. These are different design goals, and bolting compliance onto a hospitality platform tends to leave gaps that assessors are trained to find.

04 How SecurePoint USA Maps to CMMC Level 2

Control-by-control mapping showing exactly how SecurePoint USA satisfies each Physical Protection requirement.

PE.L2-3.10.1 POA&M: Eligible

Pre-registration approval workflows with multi-level authorization. Government ID verification. Real-time ITAR/EAR nationality screening blocks unauthorized foreign persons before badge issuance.

PE.L2-3.10.2 POA&M: Eligible

Integration with access control systems and CCTV platforms. Real-time visitor location tracking. Automated alerts for overstay, unescorted movement, or restricted area access attempts.

PE.L2-3.10.3 **POA&M: No Deferral**

Mandatory escort assignment — system blocks badge issuance without a designated, confirmed escort. Escort notification and acknowledgment workflow. Automatic escalation if escort does not confirm.

PE.L2-3.10.4 **POA&M: No Deferral**

Immutable, append-only audit trail with cryptographic hashing. Every event is permanently recorded. Exportable in CSV, PDF, and JSON formats.

PE.L2-3.10.5 **POA&M: No Deferral**

Full badge lifecycle management: issuance, activation, tracking, deactivation, and return confirmation. Automatic badge expiration. Overdue badge alerts with escalation chains.

PE.L2-3.10.6 POA&M: Eligible

Centralized policy engine enforces identical rules across all facilities. Multi-site dashboard provides unified compliance visibility.

05 Key Differentiators

ITAR/EAR Visitor Screening

ITAR (22 CFR Parts 120-130) and the EAR (15 CFR Parts 730-774) impose controls on who can access defense-related technical data. Allowing a foreign person to view, hear, or be present where controlled technical data is disclosed can constitute a "deemed export" under 22 CFR § 120.54 — and may carry significant civil and criminal exposure (penalty maximums change; consult current DDTC and BIS guidance).

SecurePoint USA screens every visitor against ITAR/EAR criteria during pre-registration. Foreign-person status is captured, citizenship is recorded, and license-exception eligibility can be evaluated before the visitor arrives on site. If a visitor does not clear screening, the configured workflow can block badge issuance pending review by an empowered/export-control official.

OFAC Sanctions Checks

Every visitor is automatically screened against the OFAC SDN list, the Entity List, and the Denied Persons List. Screening occurs at pre-registration and again at check-in to catch list updates. Matches trigger an automatic hold and compliance officer notification.

Escort Enforcement

SecurePoint USA does not treat escort assignment as a data field — it treats it as a workflow gate. The system requires: (1) a designated escort from the authorized personnel roster, (2) escort notification via the platform, and (3) escort acknowledgment confirming availability. If the escort does not confirm, the system escalates to backup escorts. At no point can a visitor receive a badge without a confirmed escort.

Immutable Audit Trails

Every action generates an append-only, cryptographically hashed log entry. Records cannot be edited, deleted, or backdated — by anyone, including system administrators. Audit data is exportable in CSV, PDF, and structured JSON formats with date-range filtering and control-specific report templates designed to match common C3PAO assessment request formats.

06 The Cost of Non-Compliance

Defense contractors often underestimate the financial exposure created by inadequate visitor management. The penalties are not theoretical — they are actively enforced.

ITAR Exposure

ITAR civil penalties have historically reached the $1M-per-violation range and criminal penalties include substantial fines and imprisonment, but maximums are periodically adjusted and applied by DDTC on a case-by-case basis. Unauthorized foreign-person access to controlled technical data may give rise to one or more violations; multiple visitors, days, or articles can compound exposure. Liability is generally treated as strict, so even accidental exposure can create enforcement risk. Confirm current penalty figures and program risk with qualified export-control counsel.

Debarment from DoD Contracts

ITAR violations and CMMC assessment failures can result in debarment — the loss of eligibility to receive Department of Defense contracts. For contractors whose revenue depends on defense work, debarment is existential. It does not merely pause revenue; it eliminates the entire business model.

CMMC Assessment Failure

A failed CMMC Level 2 assessment means your organization cannot bid on or perform contracts requiring CUI handling. Because three PE controls cannot be deferred, a visitor management gap discovered during assessment results in an immediate failure that requires reassessment. The cost includes months of scheduling delay, contracts you cannot bid on, and reputational damage with prime contractors.

The Math Is Simple

A purpose-built CMMC visitor management solution costs a fraction of a single ITAR violation. It costs a fraction of a failed assessment. And it costs an infinitesimal fraction of the contract revenue at risk from debarment.

SRC Sources & Notes

The references below are the primary sources used in this paper. They are listed for traceability and verification — they are not endorsements, and SecurePoint USA does not represent any source as exhaustive. Confirm current text and guidance with the source itself before relying on any citation.

[1] NIST SP 800-171, Revision 2 — Protecting CUI in Nonfederal Systems and Organizations
https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final
Primary source for the PE (Physical Protection) and AU (Audit & Accountability) control requirements discussed.

[2] 32 CFR Part 170 — Cybersecurity Maturity Model Certification (CMMC) Program
https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-170
Final CMMC rule governing assessment scope and POA&M eligibility. Verify current text before relying on POA&M deferrability statements.

[3] DFARS 252.204-7012 — Safeguarding Covered Defense Information and Cyber Incident Reporting
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.
Contract clause flowing the NIST 800-171 obligation down to defense contractors handling CUI.

[4] DoD CIO — CMMC Assessment Process (CAP)
https://dodcio.defense.gov/CMMC/
DoD-published assessor guidance referenced for what C3PAO assessors examine in physical evidence.

Originally published: 2026-03-01 Last reviewed: 2026-05-09

Close the Gap Before Your Assessment

Where they apply, the non-deferrable PE controls are easier to implement before assessment than after. SecurePoint USA is designed to provide the visitor-management evidence — escort enforcement, immutable audit logs, badge lifecycle tracking — that CMMC Level 2 assessors typically request.

Mapping is environment-specific; a scoping conversation will confirm which capabilities apply to your contracts and facilities.

Schedule a Compliance Review

securepointusa.com/request-demo

SAM.gov Registered · Active CAGE Code · Built for Defense Contractors

 Last reviewed: 2026-05-09

This whitepaper is provided for general informational purposes only and does not constitute legal, regulatory, export-control, or compliance advice.

It is not a substitute for review by qualified counsel, a C3PAO, your Facility Security Officer (FSO), an export-control or empowered official, sanctions counsel, or other advisor familiar with your specific contracts, facilities, and obligations.

Regulatory citations, enforcement examples, and statistics reflect publicly available information believed to be accurate as of the "Last reviewed" date on the cover page. Regulations and enforcement priorities change; consult primary sources before acting on anything in this document.

Statements about SecurePoint USA capabilities describe current product behavior, not a contractual commitment. Capability fit for any specific environment must be confirmed during scoping.