

WHITEPAPER

DFARS Audit Readiness for Visitor Management Programs

Building defensible visitor evidence for DoD assessments.
Append-only audit trails, evidence packs, and 10-year retention strategies.

DFARS 252.204-7012

NIST 800-171

CMMC Level 2

DIBCAC / DCSA

110

NIST 800-171
Requirements

PE+AU

Visitor-Touching
Families

SHA-256 10yr

Checksums
on Exports

SecurePoint Audit
Log Retention

securepointusa.com

Published: 2026-03-21 | Last reviewed: 2026-10-23 | Reading time: ~14 minutes

SecurePoint USA

Procurement evidence during scoping | Built for the defense industrial base

01 Executive Summary

DFARS 252.204-7012 requires defense contractors to implement NIST SP 800-171 across all systems that process, store, or transmit covered defense information, a category of Controlled Unclassified Information (CUI). While most organizations focus on network security and endpoint protection, the Physical Protection (PE) requirements are equally mandatory, and two of them address visitors directly: escort visitors and monitor visitor activity (3.10.3), and maintain audit logs of physical access (3.10.4).

Unlike technical controls, which lend themselves to automation, visitor-management evidence has to be produced at each step of a visit: who arrived, who escorted them, and when they left.

This whitepaper provides a practical framework for building visitor management records that support DFARS 252.204-7012 and stand up to the NIST SP 800-171 assessments behind it, and to DCSA security reviews where a facility is cleared.

We cover the specific NIST 800-171 requirements that map to visitor management, the evidence assessors ask to see, common documentation gaps, and a 90-day plan that takes the highest-risk gaps first.

02 The DFARS Mandate & What Assessors Actually Check

DFARS 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting," flows down from the DoD to every prime contractor and subcontractor handling covered defense information. The clause requires the 110 security requirements of NIST SP 800-171 Rev. 2. Medium and High NIST SP 800-171 DoD Assessments are conducted by DCMA's Defense Industrial Base Cybersecurity Assessment Center (DIBCAC): under DFARS 252.204-7019 and 252.204-7020 in existing contracts, and under clause 252.240-7997 in new actions since February 1, 2026 (Class Deviation 2026-O0025). CMMC Level 2 (32 CFR Part 170) assesses the same requirements by self-assessment today; third-party (C3PAO) certification as a condition of award was suspended on July 13, 2026.

DCSA is a different reviewer, and says it is not currently conducting contractor assessments related to CUI. For contractors with a facility clearance, DCSA Industrial Security Representatives conduct security reviews under the NISPOM (32 CFR Part 117), which protects classified information and has its own rules for visits. Many defense facilities answer to both.

What Reviewers Ask to See

Every reviewer looks for evidence of consistent operation, not just for a policy that says a control exists. For visitor management, they examine:

Visitor Logs:

Not just that a log exists, but that entries are complete (name, organization, date/time in and out, escort, purpose of visit) and that no gaps or alterations exist.

Escort Documentation:

Evidence that visitors requiring escorts actually received them: assignment records, status tracking, and completion confirmations.

Badge Management:

Issuance and return records for visitor badges, with serial number tracking and reconciliation procedures.

Screening Records:

Documentation that visitors were screened against appropriate lists before access was granted, with adjudication records for any hits.

Access Restrictions:

Evidence of who was authorized to enter, who approved them, and the escort assigned for controlled spaces.

Retention Compliance:

That records are maintained for the required retention period and protected from modification or deletion.

03 NIST 800-171 Controls That Map to Visitor Management

The Physical Protection (PE) family in NIST SP 800-171 contains the requirements most directly applicable to visitor management. Several Audit & Accountability (AU) requirements also apply to the records a visitor program keeps.

PE Family: Physical Protection

3.10.1: Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.

Supporting. Visitor pre-registration with host authorization, and badge issuance gated on the evidence the site requires. SecurePoint authorizes the person; your facility enforces the physical boundary.

3.10.2: Protect and monitor the physical facility and support infrastructure for organizational systems.

Deployment-dependent. Visitor dashboard showing who is on site and for how long, with automated checkout for overdue visits. Facility monitoring itself remains yours: no CCTV or access-control-system integration and no location tracking.

3.10.3: Escort visitors and monitor visitor activity.

Direct. Escort assignment recorded against the visit, escort start and end captured as events, and badge issuance gated on the escort where the site requires one.

3.10.4: Maintain audit logs of physical access.

Direct. Append-only audit logs; update and delete are refused by the database rather than discouraged in the application, each row hash-chained to the previous one, with SHA-256 checksums on exports.

3.10.5: Control and manage physical access devices.

Supporting. Badge issuance and return recorded against the visit with a print job audit trail, so an unreturned badge is visible. Physical badge stock and any electronic credential system remain yours.

3.10.6: Enforce safeguarding measures for CUI at alternate work sites.

Not claimed. Per-site security profiles apply to the facilities SecurePoint runs in; that is not alternate-work-site CUI safeguarding.

AU Family: Audit & Accountability

3.3.1: Create and retain system audit logs to enable monitoring, analysis, investigation, and reporting.

Visit actions are logged: check-in, checkout, badge issue and return, escort assignment, screening result, and decisions. Entries carry the actor, time, status, and the entity acted on. A scheduled job replaces the IP address on entries older than 180 days with a salted hash, working through them in batches.

3.3.2: Ensure actions of individual system users can be uniquely traced.

An action taken by a signed-in user records that user's ID, name, email, and role. Automated events are labeled as system events rather than given a person's identity, and SecurePoint support access is recorded with its own context.

3.3.4: Alert in the event of an audit logging process failure.

A failed audit write alerts SecurePoint's operations team, and a nightly job re-verifies the last 24 hours of each organization's entries and alerts that team to a break. A pack that includes the audit trail re-verifies the chain for its period. Your organization is not alerted directly.

3.3.8: Protect audit information and audit logging tools from unauthorized access, modification, and deletion.

Direct for modification and deletion: database triggers refuse update and delete on the audit log, including from service-role connections, apart from the maintenance functions named in section 10, and each row is hash-chained to the previous one per organization. Partial for access: a signed-in user can read only their own organization's audit rows, and exporting them takes export permission. Protecting your own accounts and logging tools stays with you.

04 7 Visitor-Management Evidence Gaps

Each of these gaps leaves an assessor without the record a PE control asks for:

1. Incomplete Visitor Logs

Paper logs with missing checkout times, illegible entries, or unsigned escort fields. Incomplete records leave an assessor unable to tell authorized access from unauthorized.

2. No Escort Verification

Organizations assign escorts but keep no record that the escort actually accompanied the visitor, which leaves 3.10.3 to be shown by interviews alone.

3. Badge Reconciliation Gaps

Visitor badges issued but no systematic tracking of returns. Where a visitor badge opens a door or a reader, an unreturned one is an uncontrolled physical access device under 3.10.5.

4. No Screening Documentation

Visitors granted access without documented screening against restricted party lists. If a foreign person reached ITAR-controlled technical data without authorization, you will need to assess a possible violation and whether to disclose it to DDTC under 22 CFR 127.12, and the visit record is what that assessment starts from.

5. Mutable Records

Spreadsheets and paper logs can be altered after the fact. NIST SP 800-171 3.3.8 asks, among other things, that audit information be protected from unauthorized modification and deletion.

6. Missing Retention Compliance

Records destroyed before the retention period expires, or no documented retention policy. Periods come from your contracts and from each regime that applies: generally five years for ITAR and EAR records, and ten for OFAC.

7. No Multi-Site Consistency

Different visitor processes at each facility, making it hard to demonstrate one security program across every cleared facility.

05 Building Defensible Evidence Packs

When DIBCAC schedules an assessment, a prime contractor asks for the evidence behind your SPRS score, or DCSA conducts a security review of a cleared facility, your visitor management system has to produce evidence of consistent operation over time, not only a description of the process.

What an Evidence Pack Should Contain

A defensible evidence pack for visitor management should include the following components, generated on demand for any date range or site:

Screening Activity Report:

Complete record of every visitor screened, including match scores, risk levels, source attribution (which sanctions list triggered the match), and final disposition.

Adjudication Summary:

Every screening that required human review, who reviewed it, what decision was made, time-to-decision SLA metrics, and override justifications.

Visitor Activity Log:

Check-in/checkout records with timestamps, host information, escort assignments, badge numbers, and zone access approvals.

Escort Enforcement Log:

Assignment records, status transitions, and completion confirmations. Failed escort checks that blocked visitor check-in.

Badge Management Record:

Issuance events with serial numbers, print job IDs, return confirmations, and reconciliation data.

Configuration Snapshot:

Point-in-time capture of screening thresholds, site security profiles, escort policies, and access zone definitions.

Source Health Report:

Sanctions list sync timestamps, record counts per source, and data freshness verification showing lists were current at time of screening.

Manifest with Checksums:

SHA-256 hashes for every file in the evidence pack, export job ID, operator identity, and generation timestamp.

Evidence Pack Templates

Evidence packs come in templates named for the review in front of you. CMMC_AUDIT, DFARS_REVIEW, and ITAR_EAR_EXPORT carry screening, review, and audit-trail evidence, and the DFARS and export packs add list health. CMMC_PE_VISITOR carries the physical-access evidence: a per-visit register of arrival, departure, host, and escort, with escort, badge, and zone-approval logs. For the physical-access requirements in a CMMC or DFARS review, generate it alongside that review's pack. Custom templates allow organizations to select specific sections.

06 Append-Only Audit Trail Architecture

NIST SP 800-171 3.3.1 asks for audit logs that support monitoring, analysis, investigation, and reporting, and 3.3.8 asks, among other things, that audit information be protected from unauthorized modification and deletion. The second requirement is where spreadsheets, paper logs, and visitor systems that let administrators edit records fall short.

Database-Enforced Append-Only Log

SecurePoint USA implements append-only audit logging at the database level using PostgreSQL triggers that raise exceptions on any UPDATE or DELETE operation against the audit_logs table. It is enforced by the database engine rather than by application code; the only exceptions are the maintenance functions named in section 10.

Append-Only Storage:

Triggers (trg_audit_logs_no_update, trg_audit_logs_no_delete) reject UPDATE and DELETE on existing records, including from service-role connections.

Row-Level Security:

RLS policies ensure each organization can only read its own audit records. Tenant isolation is enforced at query time via the current_org() function.

SHA-256 Checksums:

Every audit export includes a content checksum in the X-Content-Checksum response header, enabling independent verification of export integrity.

Archival System:

A maintenance function moves rows older than ten years to the audit_logs_archive table, so the working log stays fast without deleting history.

Change Tracking:

Changes to users, roles, and screening configuration record the prior and new values alongside who made the change.

What Each Audit Record Carries

The organization, site, action, and entity acted on; the actor's ID, name, email, and role for an action a person took, or a system label for an automated one; status, summary, request ID, and user agent; and the row's sequence number and hash in the organization's chain. The strict CSV export adds a data classification and compliance tags derived from the action.

07 10-Year Retention & Legal Hold Strategy

Retention periods for defense contractors come from their contracts and from each regime that applies: contract records generally three years after final payment (FAR 4.703), ITAR records (22 CFR 122.5) and EAR records (15 CFR 762.6) five years, OFAC records (31 CFR 501.601) ten, and, at cleared facilities, the NISPOM's own periods for records of classified visits by foreign nationals (32 CFR 117.19). SecurePoint keeps the audit log for ten years for every organization, including screening and decision history. ID images are kept only as long as the organization's ID-retention setting allows.

Retention Architecture**Ten-Year Audit Log:**

Audit history is kept ten years on every plan. Rows past ten years can move to an archive table rather than being deleted.

Photo & ID Retention:

Visitor photos and ID images are kept for the period the organization sets, then removed by a scheduled retention job.

Legal Hold Capability:

A user with compliance-management permission can place an ID document on legal hold with a stated reason. The retention job skips held documents, and the hold is audit-logged.

Packs That Prove Themselves:

An evidence pack lists the SHA-256 checksum of every file it contains, and the pack's own checksum is recorded in the audit log when it is generated.

Export & Portability

Audit records export in strict CSV format with column headers including: organization_legal_name, export_request_id, export_generated_at, record timestamps, actor identity fields, action details, entity attribution, data_classification, and compliance_tags. Exports support filtering by date range, action type, actor, role, status, site, and free-text search across up to 10,000 records per request.

08 Multi-Tenant Isolation for Joint Ventures & Sub-Contractors

Defense contractors operating across multiple cleared facilities, or managing visitor programs for joint ventures and sub-contractors, need demonstrable tenant isolation. A reviewer, or a joint-venture partner, will want to know that one organization cannot see or change another organization's visitor records on a shared platform.

Row-Level Security:

Every tenant table enforces `organization_id = current_org()` at the database level, so a query made with a user's session returns only that organization's rows. Server-side jobs that use the service role bypass RLS by design.

Account-Isolation Check:

SecurePoint staff can run an account-isolation check that flags test accounts holding roles, users in more than one organization, banned accounts that still hold roles, and sign-in metadata that disagrees with membership.

Per-Site Security Profiles:

Each site within an organization can have independent security profiles: `itar_controlled`, `dcsa_high_security`, or `normal`. Policies cascade from organization defaults but can be overridden per facility.

Per-Organization Settings:

Screening sources, adjudication rules, and feature flags are set per organization, so one organization's configuration never changes another's.

09 90-Day Audit Readiness Roadmap

This roadmap sequences the work over 90 days and takes the highest-risk gaps first. Your own timeline depends on the number of sites and how much of the process already exists.

Phase 1: Foundation (Days 1-21)

- Deploy visitor management system with append-only audit logging enabled
- Configure site security profiles matching facility clearance levels
- Enable sanctions screening with appropriate list coverage (OFAC SDN minimum)
- Establish escort enforcement policies per site classification
- Import your visitor directory, and keep legacy logs for the periods they cover

Phase 2: Evidence Generation (Days 22-45)

- Generate first evidence pack and review for completeness against NIST 800-171 PE controls
- Read the audit-chain verification the evidence pack reports
- Conduct badge reconciliation audit and establish return tracking procedures
- Train front desk staff on escort assignment and verification workflows
- Confirm which compliance managers receive hold alerts

Phase 3: Validation (Days 46-70)

- Self-assess the PE and AU requirements against the NIST SP 800-171A assessment objectives, using the evidence

packs

-
- Verify SHA-256 checksums on exported audit records
-
- Confirm who can override an escort, decide a match, and export evidence
-
- Review screening adjudication records for completeness and timeliness
-
- Confirm retention policies meet contract-specific requirements

Phase 4: Continuous Compliance (Days 71-90)

-
- Establish monthly evidence pack generation schedule
-
- Review list freshness in the source-health section of each DFARS_REVIEW pack
-
- Document standard operating procedures for visitor management
-
- Brief FSO on evidence pack generation for assessment preparation
-
- Schedule quarterly self-assessments using DFARS_REVIEW evidence template

10 How SecurePoint USA Delivers Audit Readiness

SecurePoint USA was built for organizations where visitor management is a compliance requirement, not a convenience feature. It produces the visitor evidence mapped above for the NIST SP 800-171 requirements it supports, and says plainly where your own controls take over.

Purpose-Built for Compliance:

Sanctions and denied-party lists, fuzzy name matching, OFAC 50% ownership analysis for entities (recorded without changing the decision by default), and human adjudication with an optional AI-written summary, all recorded in an append-only audit log.

Evidence Pack Templates:

Pre-configured for CMMC_AUDIT, DFARS_REVIEW, ITAR_EAR_EXPORT, and CMMC_PE_VISITOR assessments. One-click generation for any date range or site.

Database-Enforced Append-Only Audit Log:

PostgreSQL triggers reject UPDATE and DELETE on the audit_logs table, including from service-role connections. Only designated maintenance functions lift that block: archiving rows past the ten-year retention period, deleting an organization, and scrubbing IP addresses from older rows. SecurePoint refuses to delete an organization that has audit history; it is retired instead, which freezes access and keeps its records.

Multi-Site, Multi-Tenant:

Row-level security and per-site security profiles for organizations managing multiple cleared facilities, plus an account-isolation check SecurePoint staff can run.

10-Year Retention Pattern:

Ten-year audit history on every plan, legal hold for ID documents, and per-organization retention for ID images. Contract-specific retention obligations vary; verify with your contracting officer.

Procurement Evidence:

Procurement identifiers and SAM.gov evidence are provided during sales/procurement review after the evidence capture checklist is complete. SecurePoint USA does not represent GSA Schedule, FedRAMP authorization, SOC 2, ISO, CMMC certification, or government endorsement.

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] 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>.
Primary contract clause that triggers the NIST SP 800-171 obligation discussed in this paper.
- [2] DFARS 252.204-7020: NIST SP 800-171 DoD Assessment Requirements**
<https://www.ecfr.gov/current/title-48/section-252.204-7020>
Medium and High assessments by DCMA DIBCAC in existing contracts.
- [3] DPCAP: Class Deviation 2026-O0025 (FAR overhaul Part 40 / DFARS Part 240)**
https://www.acq.osd.mil/dpap/dars/dfars_far_overhaul_class_deviations.html
Clause 252.240-7997 carries the assessment terms in new actions since February 1, 2026. Revision 3 also addresses CMMC requirements during the Phase 2 suspension.
- [4] 32 CFR § 170.7: DCMA Defense Industrial Base Cybersecurity Assessment Center (DIBCAC)**
<https://www.ecfr.gov/current/title-32/section-170.7>
DIBCAC's role in CMMC and in NIST SP 800-171 DoD Assessments.
- [5] NIST SP 800-171, Revision 2: Protecting CUI in Nonfederal Systems and Organizations**
<https://csrc.nist.gov/pubs/sp/800/171/r2/upd1/final>
Requirement text for the PE and AU requirements mapped in the paper, including 3.3.8. DoD still requires Revision 2.
- [6] NIST SP 800-171A: Assessing Security Requirements for CUI**
<https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf>
Assessment objectives used in the self-assessment step of the roadmap.
- [7] DCSA: Controlled Unclassified Information**
<https://www.dcsa.mil/Industrial-Security/Controlled-Unclassified-Information-CUI/>
DCSA states it is not currently conducting contractor assessments related to CUI.
- [8] 32 CFR § 117.19: International security requirements (NISPOM)**
<https://www.ecfr.gov/current/title-32/section-117.19>
Includes the record periods for classified visits by foreign nationals at cleared facilities.
- [9] FAR 4.703: Policy (contractor records retention)**
<https://www.ecfr.gov/current/title-48/section-4.703>
Contract records, generally three years after final payment unless a clause sets longer.
- [10] 22 CFR § 122.5: Maintenance of records by registrants**
<https://www.ecfr.gov/current/title-22/section-122.5>
ITAR records: five years.
- [11] 15 CFR § 762.6: Period of retention**
<https://www.ecfr.gov/current/title-15/section-762.6>
EAR records: five years.
- [12] 31 CFR § 501.601: Records and recordkeeping requirements**
<https://www.ecfr.gov/current/title-31/section-501.601>
OFAC records: ten years, effective March 12, 2025.

Revision history

- 2026-10-23** Corrected who assesses what: DCMA's DIBCAC conducts NIST SP 800-171 assessments (under DFARS 252.204-7019 and 252.204-7020, or clause 252.240-7997 in new actions since February 2026), and DCSA reviews cleared facilities under the NISPOM and does not assess CUI. Added NIST SP 800-171 3.3.8 for audit-log protection, replaced a single ten-year retention figure with each regime's own period, corrected what an unauthorized ITAR release requires, and updated for the CMMC Phase 2 suspension. Narrowed product statements: audit alerts reach SecurePoint's operations team rather than your organization, physical-access records come in the CMMC_PE_VISITOR pack, and SecurePoint staff run the account-isolation check.
- 2026-10-03** Corrected the tenant-isolation and audit-log statements against the code, including the maintenance functions that lift audit-log protection.
- 2026-09-26** Stated OFAC's ten-year recordkeeping period (31 CFR 501.601).

Originally published: 2026-03-21 Last reviewed: 2026-10-23

Ready for Your Next Assessment?

SecurePoint USA gives defense contractors visitor records they can put in front of an assessor: append-only logs and multi-list screening.

securepointusa.com/request-demo

Procurement evidence during scoping | Built for the defense industrial base

SecurePoint USA | securepointusa.com

Copyright 2026 SecurePoint USA LLC. All rights reserved. Last reviewed: 2026-10-23

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 product behavior as of the "Last reviewed" date, not a contractual commitment. Capability fit for any specific environment must be confirmed during scoping.