SecurePoint USA

Whitepaper



CMMC and DFARS visitor evidence

The Physical Protection requirements, who assesses them, and the records that support them

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

A practitioner guide to the visitor records behind the NIST SP 800-171 Physical Protection requirements, which DFARS 252.204-7012 requires and CMMC Level 2 assesses. It quotes each requirement, sets out who assesses them and which can sit on a POA&M, shows where SecurePoint's records give evidence and where they stop, and lists how long each regime requires records to be kept.

Written for
FSOs, compliance officers, CISOs, security directors

Last reviewed
November 7, 2026

First published
March 12, 2026

Read online
securepointusa.com/resources/whitepapers/cmmc-visitor-management

Informational only. Not legal, regulatory, export-control, or compliance advice. Not a substitute for review by qualified counsel or the compliance professionals who know your obligations.

Contents

1.	Executive summary	3
2.	Where the obligations come from and who assesses them	3
3.	The six Physical Protection requirements	5
4.	How SecurePoint’s records map to each requirement	5
5.	What reviewers look for in visitor records	8
6.	Records and retention by regime	10
7.	When a foreign person reaches technical data	10
8.	What SecurePoint records and what stays with you	11
9.	Questions to ask of any visitor system	13
10.	Contract and enforcement exposure	13
	Sources and revision history	15
	About SecurePoint USA	19

Key takeaways

- DFARS 252.204-7012 still requires NIST SP 800-171 Rev. 2. CMMC Phase 2 is suspended, but a solicitation may still require Level 1 (Self) or Level 2 (Self).
- Visitor records are direct evidence only for the visitor part of 3.10.3 and 3.10.4. The other four requirements rest mostly on your own facility controls.
- NIST accepts written or automated logs of physical access. An assessor determines that visitors were escorted, their activity monitored and the logs maintained.
- Keep each record for the longest period that applies: OFAC ten years, EAR and ITAR five, contract records generally three after final payment.
- Clearing every screening list does not authorize a foreign person’s access to ITAR technical data. That takes a license or an exemption.

Last reviewed November 7, 2026 against the sources listed at the end of this paper and against SecurePoint's product as it stood that day.

1. Executive summary

> **Program status, checked November 7, 2026**
>
> On July 13, 2026, the Department of War (DoW) suspended the move to CMMC Phase 2, which from November 10, 2026 would have required a C3PAO assessment as a condition of award in many solicitations, and held later CMMC milestones until further notice.
>
> Class Deviation 2026-O0025 (Revision 3, September 3, 2026) tells contracting officers to work with requiring activities to remove or revise CMMC requirements in solicitations and contracts. A solicitation may still require CMMC Level 1 (Self) or Level 2 (Self), and DFARS 252.204-7012 still requires NIST SP 800-171 Rev. 2, including every requirement in this paper.
>
> No Federal Register rule has changed 32 CFR part 170 since the suspension. Check dodcio.defense.gov and the DPCAP class deviation page before relying on this status.

NIST SP 800-171 Rev. 2 sets 110 security requirements in 14 families for nonfederal systems that hold controlled unclassified information (CUI). DFARS 252.204-7012 requires them on contractor systems that hold covered defense information, and CMMC Level 2 assesses the same 110. Six of them, the Physical Protection (PE) family, govern who may enter a facility, how visitors are escorted, how physical access is logged and how access devices are managed.

In a CMMC Level 2 assessment, a requirement that is not met can go on a plan of action and milestones (POA&M) only to reach a conditional CMMC status, and 32 CFR 170.21 keeps five of the six PE requirements off it: PE.L2-3.10.3, 3.10.4 and 3.10.5 by name, and 3.10.1 and 3.10.2 because each is worth five points. Those five have to be met when the assessment is scored.

Visitor records do not meet any of these requirements on their own. They are direct evidence for the visitor part of escorting and logging (3.10.3 and 3.10.4) and support two more (3.10.1 and 3.10.5); monitoring the facility (3.10.2) and safeguarding CUI at alternate work sites (3.10.6) rest on other controls. This paper sets out who assesses the requirements, what an assessor determines, how SecurePoint's records map to each requirement and where they stop, and how long each regime requires records to be kept.

2. Where the obligations come from and who assesses them

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, applies to contractor information systems that process, store or transmit covered defense information, a category of CUI. It requires the security requirements of NIST SP 800-171 Rev. 2; reporting a cyber incident to DoD at dibnet.dod.mil within 72 hours of discovery; preserving images of the affected systems for at least 90 days after the report; security equivalent to the FedRAMP Moderate baseline from any cloud service provider that

will store, process or transmit covered defense information; and flowing the clause down to subcontractors whose work involves it.

DCMA DIBCAC	The Defense Contract Management Agency's Defense Industrial Base Cybersecurity Assessment Center conducts Medium and High NIST SP 800-171 DoD Assessments: 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). Summary scores are posted in the Supplier Performance Risk System (SPRS). DIBCAC also conducts CMMC Level 3 assessments.
Your organization	Performs a CMMC Level 2 (Self) assessment where a solicitation requires one, scores it under 32 CFR 170.24, posts the result in SPRS, and affirms continuing compliance each year.
C3PAOs	Certified third-party assessment organizations conduct CMMC Level 2 (C3PAO) assessments. During the Phase 2 suspension, solicitations may require only Level 1 (Self) or Level 2 (Self).
DCSA	The Defense Counterintelligence and Security Agency oversees cleared facilities under the NISPOM (32 CFR part 117), which protects classified information and sets its own rules for foreign visitors. DCSA states that it is not currently conducting contractor assessments related to CUI.

An assessment's scope reaches the tools that protect the systems in it. Under 32 CFR 170.19, a security protection asset provides security functions or capabilities to the assessment scope and is assessed against the Level 2 requirements relevant to what it provides. A service provider that processes, stores or transmits security protection data, such as log data, is an external service provider: its services are assessed as security protection assets, and its use is documented in your system security plan and in the provider's customer responsibility matrix (section 8). If your visit records are evidence for the Physical Protection requirements, expect your visitor system to be treated this way.

> **Keep covered defense information out of visit records**
>
> SecurePoint does not represent FedRAMP authorization or FedRAMP Moderate equivalence. Keep covered defense information out of visit records: a visit's purpose, its notes and any documents attached to it should describe the visit, not the technical data it involves.

3. The six Physical Protection requirements

NIST SP 800-171 Rev. 2 states each requirement in one sentence, quoted below. CMMC numbers them PE.L2-3.10.1 through PE.L2-3.10.6, scores them under 32 CFR 170.24, and sets in 32 CFR 170.21 which of them may sit on a POA&M.

Table 1. The Physical Protection requirements, their points and POA&M eligibility in a CMMC assessment

Requirement	NIST SP 800-171 Rev. 2	Points	On a POA&M
PE.L2-3.10.1	Limit physical access to organizational systems, equipment, and the respective operating environments to authorized individuals.	5	No: worth five points
PE.L2-3.10.2	Protect and monitor the physical facility and support infrastructure for organizational systems.	5	No: worth five points
PE.L2-3.10.3	Escort visitors and monitor visitor activity.	1	No: excluded by name
PE.L2-3.10.4	Maintain audit logs of physical access.	1	No: excluded by name
PE.L2-3.10.5	Control and manage physical access devices.	1	No: excluded by name
PE.L2-3.10.6	Enforce safeguarding measures for CUI at alternate work sites.	1	Yes, if the conditions below are met

> **What 32 CFR 170.21 allows**
>
> A POA&M is allowed only to reach a conditional CMMC status in a Level 2 (Self) or Level 2 (C3PAO) assessment. The score divided by the 110 requirements must be at least 0.8; every requirement on the POA&M must be worth one point, except SC.L2-3.13.11 where encryption is used but not FIPS-validated; and none of six named requirements may be on it, three of which are PE.L2-3.10.3, 3.10.4 and 3.10.5.
>
> NIST SP 800-171 DoD Assessments under the DFARS clauses have no conditional status. A requirement that is not implemented lowers the score whether or not a plan addresses it.

4. How SecurePoint’s records map to each requirement

Assessors assess your organization, not a vendor. The table shows, for each requirement, whether SecurePoint’s records are direct evidence, supporting evidence, context only, or not claimed, and what stays with you. Direct means the records answer the requirement for visitors; none of the six is met by visitor records alone.

Table 2. Physical Protection requirements and SecurePoint's records

Requirement	SecurePoint's part	What SecurePoint records	What stays with you
PE.L2-3.10.1	Supporting	Pre-registration approval, host verification and ID capture record who your staff authorized. A badge prints only when the site's required steps are done; front desk, site managers, compliance managers and org admins can override some steps with a recorded reason, never a missing escort.	Deciding who is authorized, and the doors, locks and access-control system that limit access to them.
PE.L2-3.10.2	Context only	Who is on site, since when, and which visits are overdue for check-out. SecurePoint has no CCTV or access-control-system integration and does no location tracking.	Guards, sensors and cameras, and protecting power, transmission and distribution lines, as NIST's discussion describes.
PE.L2-3.10.3	Direct, for visitors	Whether each visit required an escort and why, who was assigned, the start of the escort when the host verifies the visitor, and the close of the escort record at check-out. Where a site requires an escort, check-in stops until an escort is assigned and no badge prints; nobody can override that.	Escorting each visitor, watching what they do on site, and your escort procedure.
PE.L2-3.10.4	Direct, for visitors	Each visit's arrival, departure, host and escort. The database writes check-in and check-out to the audit log in the same transaction as the visit. A visit nobody checked out is closed at the end of the day and recorded as an unverified departure, not a checkout.	Logs of employee and contractor access, and of interior access points, from your access-control system.
PE.L2-3.10.5	Supporting	Each badge print and reprint against the visit, with the badge number, who printed it and when. From a signed-in session, only front desk, site managers, compliance managers and org admins at the visit's site can print or reprint a badge. SecurePoint does not record badge returns, and its badges do not expire.	Collecting badges, badge stock, and the keys, locks, combinations and card readers NIST names as physical access devices.
PE.L2-3.10.6	Not claimed	Nothing. SecurePoint runs at the facilities where you host visitors, not at alternate work sites.	All of it: safeguarding CUI at employees' homes and other alternate work sites.

If your visit records are evidence for these requirements, expect questions under the Audit and Accountability family about the visitor system's own audit log.

Table 3. Audit and Accountability requirements, applied to the visitor system

Requirement	What SecurePoint records	What stays with you
3.3.1 Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.	Check-in and check-out, badge prints and reprints, escort assignments, screening completions and review decisions are written to the audit log with the actor, the time, the status and the record acted on. Audit entries are kept for ten years.	Deciding which events your own systems must log.
3.3.2 Ensure that the actions of individual system users can be uniquely traced to those users, so they can be held accountable for their actions.	An action a signed-in user takes records that user's ID and role. Names and email addresses are stored in the audit log only as one-way hashes. An evidence pack generated in internal mode identifies each user by email; the assessor-safe default uses pseudonyms that stay consistent within the pack. Automated events are labeled as system events.	Giving each person their own account.
3.3.4 Alert in the event of an audit logging process failure.	The database writes check-in and check-out audit entries in the same transaction as the visit. Other audit writes alert SecurePoint's operations team when they fail, on the paths that check for it, and a nightly job re-verifies recent audit entries and alerts that team to a break. Your organization is not alerted directly.	Alerting on logging failures in your own systems.
3.3.8 Protect audit information and audit logging tools from unauthorized access, modification, and deletion.	See the callout below. Any signed-in member of your organization can read its audit entries; exporting them takes export permission.	Protecting your own accounts and logging tools.

How the audit log and tenant data are protected

SecurePoint keeps an append-only, hash-chained audit log that application users cannot edit or delete, with a verifier that checks the chain. Database triggers reject update and delete on audit entries, including from the server's 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.

Each entry's SHA-256 hash covers its sequence number, action, actor ID, the record acted on, the organization and the time, together with the previous entry's hash, starting from a fixed seed for each organization. Other fields, such as status and summary, are protected by the triggers rather than the hash. The database owner can still disable the triggers, so the hash chain and its verifier are what show whether a covered field changed or an entry went missing.

Tenant tables carry row-level security, so a query made with a user's session returns only that user's organization's rows. Server-side jobs that use the service role bypass RLS by design. So do many API routes, which take the organization from the signed-in session on the server and filter every query by it.

5. What reviewers look for in visitor records

NIST SP 800-171A sets the objectives an assessor determines for each requirement. For the four requirements visitor records touch, they read:

PE.L2-3.10.1	[a] authorized individuals allowed physical access are identified; [b] physical access to organizational systems is limited to authorized individuals; [c] physical access to equipment is limited to authorized individuals; [d] physical access to operating environments is limited to authorized individuals.
PE.L2-3.10.3	[a] visitors are escorted; [b] visitor activity is monitored.
PE.L2-3.10.4	audit logs of physical access are maintained.
PE.L2-3.10.5	[a] physical access devices are identified; [b] physical access devices are controlled; [c] physical access devices are managed.

NIST's discussion of 3.10.4 leaves the type of log to the organization: procedural, such as a written log of individuals accessing the facility, automated, or a combination. Its discussion of 3.10.5 names keys, locks, combinations and card readers as physical access devices, and its discussion of 3.10.1 says the credentials of authorized individuals include badges.

For the contents of a visitor record, NIST's federal control catalog is a useful reference:

> *Visitor access records include the names and organizations of individuals visiting, visitor signatures, forms of identification, dates of access, entry and departure times, purpose of visits, and the names and organizations of individuals visited.*
>
> NIST SP 800-53 Rev. 5, control PE-8 (Visitor Access Records), discussion

What to be able to show

- Who was authorized to visit, who approved them, and how they were identified on arrival.
- That each visitor who needed an escort had one, from arrival to departure.
- Arrival and departure times for every visit, and which departures nobody observed.
- Which badges were issued and whether they came back.
- A log that shows whether an entry changed after the fact, kept for the period each applicable regime requires.

What SecurePoint’s evidence packs carry

An evidence pack covers the date range and sites you choose and lists a SHA-256 checksum for every file it contains. The pack’s own checksum is recorded in the audit log, and a later download returns the same file. By default a pack is assessor-safe: names and email addresses become pseudonyms that stay consistent within the pack, and IP addresses and raw metadata are left out.

No single pack carries both the visit register and the audit trail, so for a Physical Protection review generate the PE visitor pack together with one of the others. Source health shows the state of each list when the pack is generated; how current a list was for a particular screening is in the screening file.

The audit report also exports as CSV or PDF, filtered by date range, site and actor, and an export from the admin audit log, up to 10,000 entries a file, has its SHA-256 checksum recorded in the audit entry for that export. For an assessor, the audit trail inside an evidence pack is the stronger export: every row carries its chain sequence and hashes, and the pack reports whether the chain verified.

- CMMC L2 PE Visitor Evidence: a register with one row per visit (arrival, departure, host, escort, badge print, screening and review status), the raw visit, escort and badge logs, an ID document manifest and a policy snapshot. It carries no audit trail and no check of the hash chain.
- CMMC L2 Audit Pack: screening activity, review decisions, the audit trail with a check of its hash chain, and a configuration snapshot.
- DFARS 252.204-7012 Review: screening activity, review decisions, source health, and the audit trail with its chain check.
- ITAR / EAR Export Pack: screening activity, review decisions, source health, the audit trail with its chain check, and a configuration snapshot.

6. Records and retention by regime

Retention periods come from your contracts and from each regime that applies to a record. Keep each record for the longest period that applies to it, and confirm the periods with counsel.

Table 4. Record periods by regime

Records	Rule	Period
Contract records	FAR 4.703	Generally three years after final payment, unless a clause sets a longer period
ITAR records of exports and other regulated activity	22 CFR 122.5	Five years
EAR export records	15 CFR 762.6	Five years
Transactions subject to OFAC regulations	31 CFR 501.601	Ten years, since March 12, 2025
Foreign visitors with access to classified information, at cleared facilities	32 CFR 117.19(e)(4)(iii)	One year

> **What SecurePoint keeps**
>
> SecurePoint keeps the audit log for ten years. Visit records, screening results and review decisions are protected from deletion for ten years after they last change. Visitor photos and ID images are kept for the period your organization sets and then removed by a scheduled job, unless a user with compliance-management permission places an ID document on legal hold, which is itself written to the audit log.

7. When a foreign person reaches technical data

CMMC does not assess export controls, but a facility that holds CUI may also hold ITAR technical data. Releasing or otherwise transferring technical data to a foreign person in the United States is a deemed export (22 CFR 120.50(a)(2)), and the release is deemed an export to every country in which that person has held or holds citizenship or holds permanent residency (120.50(b)).

Clearing every screening list does not authorize a foreign person’s access to ITAR technical data. That takes a license or an exemption, and the decision belongs to your empowered official or export control officer.

1. **Establish what was released**
   Use the visit record, the escort record and the people involved to establish who saw what, and whether a license or an exemption covered it.

2. **Consider a voluntary disclosure**
   DDTC strongly encourages disclosure by anyone who believes they may have violated the ITAR, may treat it as a mitigating factor, and treats a failure to report as an adverse factor (22 CFR 127.12).

3. **Inform DDTC at once where § 126.1 applies**
   Anyone who knows or has reason to know of an export of the kind 22 CFR 126.1(e)(1) describes, to a country that section lists or a person acting on its behalf, must immediately inform DDTC (126.1(e)(2)). A release to a national of a listed country can be such an export.

4. **Report to your CSA at a cleared facility**
   A cleared contractor reports any violation of administrative security procedures or export control regulations that would subject classified information to possible compromise by foreign visitors to its cognizant security agency (32 CFR 117.19(h)).

How SecurePoint screens and holds visitors

Visitors are screened against the OFAC SDN List, the BIS Entity List and the Denied Persons List, among other sources, when the visit is set up, or at check-in where your organization defers screening of host invitations. At check-in, an approval is reused only while its screening is inside the re-screening interval your organization sets, or before a clearance expiry set when it was approved, and only if it ran on the same name. Otherwise kiosk and guided check-ins screen again, QR check-ins move to the kiosk flow, and one-click desk and API check-ins refuse and send the visitor to one that screens.

A possible match holds the visit and alerts your compliance managers and org admins, and no badge prints until a reviewer decides. By default an AI provider named on the Subprocessors page also writes a summary of each screened name for the reviewer; it does not change the risk score or the decision.

At a site set up as ITAR Controlled or DCSA High Security, every visit asks the visitor to attest to U.S.-person status before a badge is issued, and a visitor not confirmed as a U.S. person needs an escort. A national of a § 126.1 country, a visitor whose country cannot be resolved, or one whose attestation conflicts with their citizenship is held for compliance review. SecurePoint records the attestation and the reviewer’s decision; whether a license or an exemption covers the access stays with you.

8. What SecurePoint records and what stays with you

If SecurePoint is an external service provider in your assessment scope, its use goes in your system security plan with a customer responsibility matrix (32 CFR 170.19). The matrix below is a starting point; your scope decides how each line applies.

Table 5. Customer responsibility matrix for the visitor program

Area	SecurePoint records	Stays with you
Who may visit	Pre-registration, host verification, ID capture, and the steps each site requires before check-in	Deciding who is authorized and setting each site's requirements
Screening	Screening against the lists your organization enables, a hold on each possible match, and each reviewer's decision	Reviewing matches, export licensing decisions, and any filing with OFAC, BIS or DDTC
Escorts	Whether an escort was required, who was assigned, the start at host verification and the close at check-out	Escort conduct, escort procedures and training, and watching what visitors do
Badges	Each print and reprint with its badge number, who printed it and when	Collecting badges at departure, badge stock, and reconciling unreturned badges
Physical access	Visitor arrivals and departures, and visits closed without an observed departure	Employee and contractor access logs, doors and locks, and the access-control system
Facility monitoring	Who is on site and which visits are overdue for check-out	Guards, cameras and sensors, and protecting support infrastructure
Audit log	An append-only, hash-chained log that application users cannot edit or delete, kept for ten years	Reviewing it, and protecting the logs of your own systems
Access to SecurePoint	Sign-in under your organization's multi-factor authentication policy, and roles that limit who can print badges, decide matches and export evidence	Assigning roles, removing leavers, and multi-factor authentication at your identity provider when staff sign in through it

Limits to plan around

Plan your own procedures around these limits:

- SecurePoint does not record badge returns, and its badges do not expire.
- Escort events are recorded when staff enter them, when a host verifies a visitor, and at check-out. SecurePoint does not track where an escort or a visitor goes.
- A visit nobody checked out is closed at the end of the day and recorded as an unverified departure, not a checkout. An organization admin can turn that off for a site.
- There is no CCTV or access-control-system integration and no location tracking.
- SecurePoint does not file with OFAC, BIS or DDTC, and it does not represent a GSA Schedule, SOC 2 or ISO certification, CMMC certification, or endorsement by any government.

9. Questions to ask of any visitor system

Whatever system an organization uses, these are the questions an assessor, a prime contractor or DCSA can ask about the records behind a visit.

- Does it record citizenship or U.S.-person status, and hold a visit when it cannot resolve them?
- Can a visitor who must be escorted be checked in or badged without an escort, and who can override that?
- Does it record when an escort started and ended, or only who was assigned?
- Does it record badge returns, and do its badges expire?
- Who can change a visit record after the fact, and does each change leave an entry the editor cannot remove?
- How does it mark a visit closed without an observed departure?
- Can its audit log show that an entry has not changed, and who can disable that protection?
- Which lists does it screen visitors against, and does it keep who reviewed each possible match and why?
- Can it export the visit records and the audit log for one site and one period, with checksums?
- Does the vendor claim FedRAMP authorization or equivalence, and if not, how do you keep covered defense information out of it?

10. Contract and enforcement exposure

A contractor without the CMMC status a solicitation requires is not eligible for that award (DFARS 252.204-7025), and a contracting officer may not exercise an option or extend performance without it (DFARS subpart 204.75, applied as DFARS 240.371 under Class Deviation 2026-O0025). That is ineligibility, not debarment: debarment is a separate, government-wide decision under FAR subpart 9.4, and ITAR debarment (22 CFR 127.7) bars a person from activities the ITAR regulates.

The enforcement that has produced settlements is misrepresentation. The Department of Justice has settled False Claims Act allegations that contractors billed DoD while NIST SP 800-171 requirements were not met or their assessment score was overstated. These are settlements of allegations, not findings of liability. A self-assessment score and an annual affirmation need evidence behind them, and physical-access records are part of that evidence.

Table 6. False Claims Act settlements over NIST SP 800-171 requirements

Contractor	Announced	Amount	What DOJ described
MORSECORP Inc.	March 26, 2025	$4.6 million	Army and Air Force contracts required NIST SP 800-171. MORSE reported a score of 104 in January 2021, a consultant later put its score at -142, and the score was not updated until June 2023.
Raytheon companies and Nightwing Group	May 1, 2025	$8.4 million	An internal development system used for work on DoD contracts allegedly lacked the required cybersecurity controls, for conduct between 2015 and 2021.
Georgia Tech Research Corporation	September 30, 2025	$875,000	Allegedly failed to meet cybersecurity requirements on Air Force and other defense contracts.
LOGZONE Inc.	June 18, 2026	$507,144	On two Navy contracts, allegedly did not implement required NIST SP 800-171 controls; a DCMA assessment scored it -170 out of a possible 110.
Honeywell Aerospace Inc.	September 1, 2026	$2,042,518	Allegedly did not comply with NIST cybersecurity requirements on one network under a DoD contract.

Where visitors can reach ITAR technical data, the civil penalty for each violation of 22 U.S.C. 2778 can reach the greater of $1,271,078 or twice the value of the transaction (22 CFR 127.10, as adjusted in January 2025; OMB Memorandum M-26-11 cancelled the 2026 inflation adjustments). Civil liability does not depend on intent. A willful violation is a crime punishable by a fine of up to $1,000,000, up to 20 years in prison, or both, for each violation (22 U.S.C. 2778(c)).

Sources and revision history

First published March 2026. Last reviewed November 7, 2026 against the sources below and against SecurePoint's product as it stood that day. The sources are listed for traceability, not as endorsements. Confirm current text with the issuing agency before relying on a citation.

[1] **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 quoted for PE 3.10.1 through 3.10.6 and AU 3.3.1, 3.3.2, 3.3.4 and 3.3.8. NIST marked Revision 2 withdrawn on May 14, 2024, in favor of Revision 3; DoD still requires Revision 2 for DFARS 252.204-7012 and CMMC.

[2] **NIST SP 800-171A: Assessing Security Requirements for CUI**
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf
Assessment objectives for each requirement, used for what an assessor looks for.

[3] **NIST SP 800-53, Revision 5: Security and Privacy Controls**
https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final
The PE-8 discussion of visitor access records, quoted for the fields a visitor record holds.

[4] **32 CFR Part 170: Cybersecurity Maturity Model Certification (CMMC) Program**
https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-G/part-170
§ 170.19 sets assessment scope, including security protection assets; § 170.21(a)(2) sets POA&M eligibility for a conditional status and excludes PE.L2-3.10.3, 3.10.4 and 3.10.5 by name; § 170.24 sets point values, with PE.L2-3.10.1 and 3.10.2 at five points.

[5] **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.

[6] **Department of War: "DoW Suspends CMMC Phase II Requirements" (July 13, 2026)**
https://www.war.gov/News/Releases/Release/Article/4542329/forging-the-arsenal-of-freedom-department-of-war-suspends-cmmc-phase-ii-require/
Source for the suspension of CMMC Phase 2.

[7] **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
Revision 3 (September 3, 2026) carries CMMC at DFARS 240.371 and the assessment terms in clause 252.240-7997 for new actions since February 1, 2026, and directs contracting officers to remove or revise CMMC requirements during the Phase 2 suspension; Level 1 (Self) and Level 2 (Self) may still be required.

[8] **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.
Requires NIST SP 800-171 on contractor systems with covered defense information, 72-hour incident reports, 90-day image preservation, FedRAMP Moderate equivalence for cloud providers, and flowdown.

[9] **DFARS 252.204-7019: Notice of NIST SP 800-171 DoD Assessment Requirements**
https://www.ecfr.gov/current/title-48/section-252.204-7019
A current NIST SP 800-171 DoD Assessment score posted in SPRS as a condition of award.

[10] 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.

[11] DFARS 252.204-7025: Notice of CMMC Level Requirements
https://www.ecfr.gov/current/title-48/section-252.204-7025
Award and option eligibility where a solicitation requires a CMMC status.

[12] 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.

[13] 32 CFR § 117.19: International security requirements (NISPOM)
https://www.ecfr.gov/current/title-32/section-117.19
§ 117.19(e)(4)(iii): a one-year record of foreign visitors with access to classified information; § 117.19(h): reporting to the cognizant security agency.

[14] 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.

[15] FAR subpart 9.4: Debarment, suspension, and ineligibility
https://www.acquisition.gov/far/subpart-9.4
Federal procurement debarment, kept separate in the paper from award ineligibility and from ITAR debarment.

[16] 22 CFR § 120.50: Export
https://www.ecfr.gov/current/title-22/section-120.50
A release of technical data to a foreign person in the United States is an export (§ 120.50(a)(2)), to every country of the person's citizenship or permanent residency (§ 120.50(b)).

[17] 22 CFR § 122.5: Maintenance of records by registrants
https://www.ecfr.gov/current/title-22/section-122.5
ITAR records: five years.

[18] 22 CFR § 126.1: Prohibited exports, imports, and sales to or from certain countries
https://www.ecfr.gov/current/title-22/section-126.1
§ 126.1(e)(2): inform DDTC immediately of a proposed or actual export to a listed country.

[19] 22 CFR § 127.7: Debarment
https://www.ecfr.gov/current/title-22/section-127.7
Statutory and administrative debarment under the ITAR.

[20] 22 CFR § 127.10: Civil penalty
https://www.ecfr.gov/current/title-22/section-127.10
ITAR civil maximum: the greater of $1,271,078 or twice the value of the transaction, as adjusted in January 2025.

[21] 22 CFR § 127.12: Voluntary disclosures
https://www.ecfr.gov/current/title-22/section-127.12
A voluntary disclosure to DDTC may be a mitigating factor.

[22] OMB Memorandum M-26-11 (April 17, 2026)
https://www.fec.gov/resources/cms-content/documents/OMB-Memo-Cancellation-of-Penalty-Inflation-Adjustments-for-2026.pdf
Cancelled the 2026 civil penalty inflation adjustments. The copy linked is the one the Federal Election Commission publishes.

[23] 22 U.S.C. 2778(c): Criminal violations
https://www.law.cornell.edu/uscode/text/22/2778
Criminal penalties for willful violations: up to $1,000,000, up to 20 years in prison, or both, per violation.

[24] 15 CFR § 762.6: Period of retention
https://www.ecfr.gov/current/title-15/section-762.6
EAR records: five years.

[25] 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.

[26] DOJ: MORSECORP settlement (March 2025)
https://www.justice.gov/opa/pr/defense-contractor-morsecorp-inc-agrees-pay-46-million-settle-cybersecurity-fraud
False Claims Act settlement over an overstated SPRS score.

[27] DOJ: Raytheon companies and Nightwing Group settlement (May 1, 2025)
https://www.justice.gov/opa/pr/raytheon-companies-and-nightwing-group-pay-84m-resolve-false-claims-act-allegations-relating
$8.4 million False Claims Act settlement over cybersecurity requirements on DoD contracts.

[28] DOJ: Georgia Tech Research Corporation settlement (September 30, 2025)
https://www.justice.gov/opa/pr/georgia-tech-research-corporation-agrees-pay-875000-resolve-civil-cyber-fraud-litigation
$875,000 False Claims Act settlement over cybersecurity requirements on defense contracts.

[29] DOJ: LOGZONE settlement (June 2026)
https://www.justice.gov/opa/pr/alabama-defense-contractor-agrees-pay-507144-resolve-false-claims-act-liability-relating
False Claims Act settlement after DCMA assessments found NIST SP 800-171 requirements unmet.

[30] DOJ: Honeywell Aerospace settlement (September 2026)
https://www.justice.gov/opa/pr/honeywell-aerospace-inc-agrees-pay-over-2m-settle-false-claims-act-allegations-failing
False Claims Act settlement over NIST SP 800-171 requirements on a DoD contract.

[31] DoD CIO: Cybersecurity Maturity Model Certification
https://dodcio.defense.gov/CMMC/
Current CMMC program status.

Revision history

November 7, 2026 Merged in the DFARS audit-readiness paper, which is retired: who assesses the requirements, the DFARS 252.204-7012 duties, record retention by regime, foreign-person access to technical data, and recent False Claims Act settlements. Rewritten so the web page and the PDF carry the same text. Corrected product statements: SecurePoint does not record badge returns, no one can override a missing escort, a visit nobody checked out is recorded as an unverified departure, and the audit log's protection is stated with the maintenance functions that lift it. POA&M eligibility is now stated for a conditional CMMC status.

October 23, 2026	Updated for the July 13, 2026 suspension of CMMC Phase 2 and Class Deviation 2026-O0025. Corrected POA&M eligibility: five of the six Physical Protection requirements cannot be placed on a POA&M, not three. Quoted each requirement as NIST states it, replaced an outdated ITAR civil penalty figure, distinguished award ineligibility from debarment, added False Claims Act settlements, and narrowed product statements to what SecurePoint records.
October 3, 2026	Corrected the escort, export-screening and audit-log statements against the product and DDTC records.
September 27, 2026	Stated what the audit log guarantees: append-only and hash-chained, with the maintenance functions that lift its protection named.
September 1, 2026	Mapped each Physical Protection requirement to the evidence SecurePoint produces: direct, supporting, deployment-dependent, or not claimed.

About SecurePoint USA

SecurePoint USA builds visitor management and restricted-party screening software for defense contractors, manufacturers, research facilities and schools. It screens visitors and other parties against government sanctions and restricted-party lists, holds possible matches for a person to decide, issues badges once a site's required evidence is in place, and keeps an append-only, hash-chained audit log that application users cannot edit or delete, with a verifier that checks the chain. SecurePoint does not file with OFAC, BIS or DDTC, and it does not make an organization compliant: it supplies records for the program your organization runs.

See a visit recorded from arrival to departure.

Request a demo to watch a visitor screened, held until an escort is assigned, badged and checked out, and the visit's records exported in an evidence pack, using demonstration data.

- Request a demo: securepointusa.com/request-demo
- Read this paper online: securepointusa.com/resources/whitepapers/cmmc-visitor-management
- All whitepapers: securepointusa.com/resources/whitepapers

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, or by the compliance, security, export-control or assessment professionals familiar with your organization, its 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.

© 2026 SecurePoint USA LLC. All rights reserved.