



ITSECOPS

ITSECOPS RESEARCH · REPORT 01 · OCTOBER 2026

The CMMC Readiness Gap Report 2026

What a live Microsoft 365 tenant check reveals that the System Security Plan does not

The SSP said one thing. The tenant said another.
14 of 32 findings were contradictions.

Gaurav Sengar, CISA, Founder ITSECOPS

EXTENDED EDITION

Read it as a checklist, not as a story

The free web version of this report tells you what happened when one US defense subcontractor's Microsoft 365 GCC tenant was walked through the way a C3PAO assessment team would walk through it. This Extended Edition is built for the people who have to do the work: the ISSM, the IT lead, the MSP engineer and the compliance owner who need to run the same checks on their own tenant before anyone posts a score.

Four parts carry most of the value. The **findings register** (chapter 03) gives all 32 findings with what was observed, what the fix is and which artefact closes it. The **contradiction register** (chapter 04) shows the 14 places where the written position and the live tenant disagreed. The **POA&M worksheet** (chapter 05) applies 32 CFR 170.21 to a real position and leaves you a blank table to fill in. The **checklists** (chapter 08) compress the whole engagement into tick lists you can run in an afternoon.

Work it in this order: run the 38-line checklist against your own Intune and Entra consoles, mark each line pass, fail or partial, then open the matching finding card for every fail and partial. Capture the evidence the card names while the console is open. Then take your Not Met list to the POA&M worksheet before you touch SPRS.

Contents

01	Executive summary	3
02	The 38 live checks by console area	4
03	The findings register: all 32, anonymised	5
04	The contradiction register	12
05	POA&M admissibility worksheet	14
06	The intake-to-mock journey	16
07	90-day remediation sequence	18
08	Checklists	19
09	Further reading	22

Limits and anonymisation

One engagement. Everything in this report comes from a single CMMC Level 2 readiness engagement: a US defense subcontractor on a Microsoft 365 GCC tenant, about 300 users, roughly 90 of them handling CUI, headquarters plus overseas sites. Working papers run from May to September 2026. The live console walkthrough that produced the 38 checks and 32 findings took place in September 2026.

Patterns, not identifiers. The contractor, its people, its sites, device names, group names and document identifiers have been removed. Where a third-party product appears in a finding it is described by function: a third-party backup platform, a cloud secure web gateway, the ticketing system. Microsoft products are named because they are the controls, not the client.

Scale is rounded. User, device and group counts are given approximately where an exact figure would identify the engagement. Counts quoted from console assignment screens are given as seen, because the point is the mismatch, not the number.

Readiness language only. ITSECOPS is a consultant, not a C3PAO; nothing here is a certification assessment. Point values and POA&M eligibility are cited from 32 CFR 170.21 and 170.24. Before any score is presented to a customer or entered into SPRS, take the values from the current DoD Assessment Methodology rather than from this report.

01 Executive summary

A contractor with a written SSP, a policy corpus and an active remediation programme walked an assessor-style check of its own tenant. One check in 38 passed.

38

LIVE CHECKS

1 pass · 28 fail · 9 partial

32

FINDINGS

13 S1 · 16 S2 · 3 S3

14

CONTRADICTIONS

stated position vs live tenant

53

ENTERPRISE APPS

many unowned, several tenant-wide write

~100

STALE ACCOUNTS

plus 17 guests and 30 devices

What the numbers say

At intake in June 2026 the contractor had **20 of 110** practices fully implemented and a true SPRS-method score of **-159**, formally No Score while the SSP requirement was unmet. Three months later, with the SSP written and a remediation sprint behind it, the position against all 110 requirements at the mock stage was **8 Met, 55 Partial and 47 Not Met**. Partial scores as Not Met except in the narrow cases the rule allows.

The Met count fell while the work went up because the scrutiny went up. Intake took "fully implemented" at face value where nothing contradicted it. The mock applied every NIST SP 800-171A objective and demoted anything the console contradicted. That is what a C3PAO does.

POSITION AGAINST 110 REQUIREMENTS AT MOCK STAGE



32 FINDINGS BY SEVERITY



The three findings that drive the verdict

- Application control is in audit mode with device exclusions, and sits on the POA&M.** MA.L2-3.7.2 and CM.L2-3.4.8 are five-point practices. 32 CFR 170.21(a)(2)(ii) bars anything above one point from a POA&M. The placement does not protect the practices; it adds a finding.
- The declared boundary and the configured tenant do not match.** The SSP declares one site and roughly 90 CUI users. Policies target 130 to 576 objects, CUI groups hold 109, 118 and 130 members, and users and hosts in two out-of-scope countries sit inside CUI-relevant targets. Scope is settled before practices are assessed.
- Fourteen load-bearing claims are contradicted by the console.** PIM described but not in use. MFA "for all users" excluding a service account group. Shared accounts reported removed and still enabled. A backup platform reported removed and still registered. A gateway stated as FedRAMP High that is commercial. Together they are why an assessor widens sampling.

Why now

The clock stopped, the exposure did not.

CMMC Phase 2, which would have put C3PAO certification into new solicitations from 10 November 2026, was suspended by the Department of War on 13 July 2026. A 60-day Reform Task Force review ended around 11 September; its report went to the Department CIO and had not been published at the time of writing. No replacement date exists. Class Deviation 2026-O0025 Revision 3 (3 September 2026) tells contracting officers to accept Level 1 and Level 2 self-assessments and remove third-party requirements at the next option or modification. Many contractors read that as "CMMC moved to 2028". It did not: 10 November 2028 is the original Phase 4 date, and DFARS 252.204-7012 and NIST SP 800-171 Rev 2 remain binding today.

Self-assessment is where enforcement lives.

On 1 September 2026 Honeywell Aerospace paid a **\$2,042,518** False Claims Act settlement over NIST 800-171 compliance on one network. In the LOGZONE matter (DOJ, 18 June 2026) the contractor had self-scored **110** in SPRS; DCMA scored the same environment at **-170**. The engagement in this report had an intake score of **-159**. Nobody had posted it.

Capacity is the other wall. The Cyber AB's 29 September 2026 town hall reported 2,362 final Level 2 certificates and 71 conditional, with 117 authorised C3PAOs. The DFARS final rule projects 118,289 entities needing Level 2 certification by year four. **About 2 percent** of that population holds a certificate. When the pause ends, the queue starts where it stopped.

Sources: hklaw.com, crowell.com, ksg.us, secureframe.com, cmmcmmap.com, justice.gov, cyberab.org. Full list in chapter 09.

02 The 38 live checks by console area

Each check was driven by the contractor's own IT staff with the console on screen, and judged against the state the contractor had documented, not against a generic baseline.

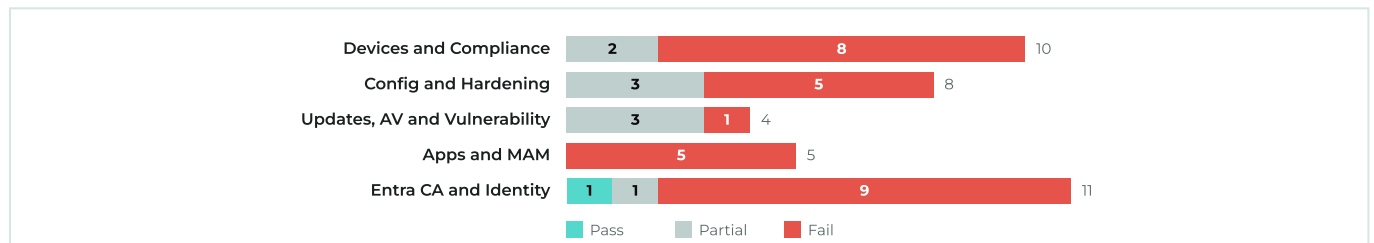
Console area	Checks	Pass	Fail	Partial
Devices and Compliance	10	0	8	2
Config and Hardening	8	0	5	3
Updates, AV and Vulnerability	4	0	1	3
Apps and MAM	5	0	5	0
Entra CA and Identity	11	1	9	1
Total	38	1	28	9

One pass. Terms of Use, recovered from a July downgrade when both policies were scoped to a single pilot user.

Twenty-eight fails against the state the contractor had itself documented.

Nine partials. Partial means the capability is configured but incomplete: the wrong scope, an audit mode rather than an enforcing one, or no proof that the control has ever operated. An assessor scores Partial as Not Met.

The checks were driven by the contractor's own IT staff. The expected state for each row came from the contractor's policies, SSP and previously submitted evidence.



How the method differs from a self-assessment

Examine, Interview, Test

Every observation is tested against the NIST SP 800-171A objectives and judged against the state the organisation has documented. A control that works but is not described accurately is a finding under CA.L2-3.12.4.

Two kinds of finding

Control findings: a required capability is absent, misconfigured or unenforced. Accuracy findings: the organisation asserted a state the live tenant contradicts. Assessors weight the second heavily because it affects every other assertion.

The expected state comes from you

The expected state column was drawn from the contractor's own policies, SSP and submitted evidence. That is the assessor's test: not "is this good practice" but "is this what you said".

Findings by area

Area	Findings	IDs
Identity & privileged access	8	LC-01, LC-02, LC-03, LC-04, LC-05, LC-06, LC-07, LC-30
Device management	4	LC-08, LC-09, LC-10, LC-11
Scope integrity	3	LC-12, LC-13, LC-14
Endpoint hardening	9	LC-15, LC-16, LC-17, LC-18, LC-19, LC-20, LC-21, LC-23, LC-32
Change control	1	LC-22
Boundary & external services	1	LC-24
Patch & vulnerability	1	LC-25
Mobile application management	1	LC-26
Third-party applications	3	LC-27, LC-28, LC-29
Session coverage	1	LC-31

03 The findings register: all 32, anonymised

Grouped by area. Each card gives the practices touched, what the console showed, the required fix and the artefact that closes it. Run it against your own tenant.

S1 Assessment stopper: would prevent a passing determination or undermine confidence in the package as a whole. Fix before scheduling. **S2** Major: a practice-level failure with clear evidence. Fix before assessment. **S3** Moderate: hygiene or consistency. Will not on its own change a determination.

Identity & privileged access 8 findings

LC-01 **S1** Privileged Identity Management is not in use; a permanent Global Administrator remains

PRACTICES AC.L2-3.1.5, AC.L2-3.1.6, AC.L2-3.1.7, IA.L2-3.5.3, CA.L2-3.12.4

OBSERVED LIVE

A named admin account holds Global Administrator with an assignment end time of Permanent and PIM is not in use. No account holds Security Administrator, two named users sit in the Entra joined device local administrator role, and the managed service provider's service principal holds Exchange Administrator. The SSP and the privileged access standard describe approval-gated activation through PIM with 19 standing and 38 eligible assignments, so this is an accuracy finding as well as a control finding.

REQUIRED FIX

Enable PIM for Global Administrator and every privileged role with approval, justification and an activation window of 8 hours or less. Reduce standing Global Administrators to two cloud-only break-glass accounts, authorised in writing by the COO and alert-monitored. Assign Security Administrator and Security Reader to named individuals per the separation of duties matrix. Empty the device local administrator role. Correct the SSP narrative to the state the tenant actually holds.

EVIDENCE TO PRODUCE

PIM role setting screenshots per role, role assignment export showing end dates, signed break-glass authorisation memo, revised SSP section.

LC-02 **S1** "MFA for all users" is not applied to all users

PRACTICES IA.L2-3.5.3, AC.L2-3.1.1, AC.L2-3.1.2, AC.L2-3.1.20, IA.L2-3.5.2

OBSERVED LIVE

The MFA for all users policy excludes a service account group holding seven generic identities, a guest group and an executive exception group, and one named user is excluded from the compliant device requirement. The guest MFA policy excludes an external bid-review group with three guests. The July evidence had recorded the policy as applied to All users and it was accepted on that basis. None of the exclusions has an approval record.

REQUIRED FIX

Reduce the exclusion group to documented break-glass only. Convert generic accounts to workload identities or app-only authentication with certificate credentials so they no longer need an interactive MFA exemption. Obtain COO exception records with expiry dates for anything that remains. Remove the executive exception or produce a signed risk acceptance naming the compensating control. Bring the three guests behind MFA.

EVIDENCE TO PRODUCE

Policy screenshot showing include and exclude, exclusion group membership export, signed exception records, one sample blocked sign-in.

LC-03 **S1** Shared and generic accounts are still enabled

PRACTICES IA.L2-3.5.1, IA.L2-3.5.2, AC.L2-3.1.1, AU.L2-3.3.1, AU.L2-3.3.2

OBSERVED LIVE

Seven shared or generic identities are live and carried in the Conditional Access exclusion group: an administrator mailbox account with no sign-in for two months, an IT support account, an IT operations account in use as a service account, two connector accounts, a SharePoint test user and a testbed account. Policy prohibits shared accounts on CUI systems, and the July package asserted the last shared account had been renamed.

REQUIRED FIX

Inventory each account and assign a named accountable owner. Convert to service principals with certificate credentials where a machine identity is genuinely needed. Disable and then delete the rest. Produce the service account register the Access Control Policy already requires.

EVIDENCE TO PRODUCE

Service account register, disablement records, sign-in log showing no interactive use.

LC-04 **S2** Stale identities at scale: about 100 user accounts, 17 guests, 30 devices

PRACTICES IA.L2-3.5.6, AC.L2-3.1.1, AC.L2-3.1.20

OBSERVED LIVE

The live sweep found roughly 100 stale user accounts, 17 stale guest accounts and 30 stale device objects against a policy that reviews at 90 days and deactivates within five business days. The July review had already found 6 of 8 supposedly disabled accounts still enabled, so the condition has grown rather than closed, which suggests the quarterly review is not running.

REQUIRED FIX

Run the disable campaign now and evidence it with before and after sign-in activity exports. Stand up an Entra ID Governance access review, or a scheduled script with a signed output, so the quarterly cadence is provable rather than asserted.

EVIDENCE TO PRODUCE

Inactive account query output before and after, signed quarterly review record, guest sponsor reconciliation against the guest register.

LC-05 S2 Three Conditional Access policies are sitting in report-only mode**PRACTICES** IA.L2-3.5.3, IA.L2-3.5.4, AC.L2-3.1.1, AC.L2-3.1.20, SC.L2-3.13.15**OBSERVED LIVE**

Block device code flow, the legacy authentication block and the private access restriction policy for the secure web gateway are all in report-only mode. Report-only changes no outcome, so an assessor treats the policy as not implemented. Device code flow is an active phishing path into a tenant that holds CUI.

REQUIRED FIX

Review the report-only impact data, then move each policy to On. Capture one blocked sign-in per policy as operational evidence.

EVIDENCE TO PRODUCE

Policy state screenshots plus a sign-in log entry showing the block, one per policy.

LC-06 S2 Session controls contradict the SSP and are duplicated across two planes**PRACTICES** AC.L2-3.1.10, AC.L2-3.1.11, SC.L2-3.13.9**OBSERVED LIVE**

A reauthentication policy has persistent browser session enabled, which defeats the 7-day sign-in frequency the SSP records. The CUI idle session timeout exists in both Conditional Access and Intune, and testbed groups have been added to it. The unmanaged device download block is scoped to browser clients only, and the primary-PC-only access group holds a single device.

REQUIRED FIX

Choose one enforcement plane for idle timeout and remove the duplicate. Turn off persistent browser session for the CUI cohort. Remove testbed groups from production policies. Extend the unmanaged device download block beyond browser clients.

EVIDENCE TO PRODUCE

Session control screenshots, group membership export, a captured re-authentication event.

LC-07 S2 Exception groups and grace bypasses exist with no approval record**PRACTICES** AC.L2-3.1.2, AC.L2-3.1.5, IA.L2-3.5.3, CA.L2-3.12.4**OBSERVED LIVE**

An admin exception register group, a device grace group referenced in no SOP, an executive exception group, a PowerShell admin tools exception policy with a named admin account added and no approval, a device restriction exception naming an individual with no reason, and a device lock exemption with one member and no reason. The PowerShell exception was first raised in July and is still unexplained.

REQUIRED FIX

For each exception group either produce the approval record or delete the group. Document the device grace group in the relevant SOP. Set expiry dates on all of them and put the review on the ISSM calendar.

EVIDENCE TO PRODUCE

Signed exception register with expiry dates, updated SOP text.

LC-30 S3 A sampled user shows Conditional Access as not applicable**PRACTICES** AC.L2-3.1.1, AC.L2-3.1.2, IA.L2-3.5.3**OBSERVED LIVE**

For the sampled user the MFA requirement was satisfied and the device owner matched the device identifier, but Conditional Access showed as not applicable. This repeats a July finding that 23 percent of sign-ins showed no Conditional Access policy applied.

REQUIRED FIX

Run a what-if analysis across the user population, identify everyone no policy reaches, and close the gap with a catch-all policy.

EVIDENCE TO PRODUCE

What-if output or a sign-in log query showing zero users with no policy applied.

Device management 4 findings**LC-08 S1 No device platform enrolment restrictions exist****PRACTICES** AC.L2-3.1.18, AC.L2-3.1.20, CM.L2-3.4.1, CM.L2-3.4.2**OBSERVED LIVE**

Intune device platform restrictions are empty, so any personally owned Windows device can enrol. This explains the July finding that two personally owned hosts had reached the application control cohort: the door is open by configuration, not by accident.

REQUIRED FIX

Block personally owned Windows and macOS enrolment, allow corporate identifiers or Autopilot only, then re-baseline or remove the two personal hosts already inside the cohort.

EVIDENCE TO PRODUCE

Restriction policy screenshot, enrolment audit showing the two hosts resolved.

LC-09 **S2** Device inventory does not reconcile in any direction

PRACTICES CM.L2-3.4.1, CM.L2-3.4.2, RA.L2-3.11.2

OBSERVED LIVE

Intune shows roughly 370 devices with nearly 50 non-compliant. Entra shows roughly 650 device objects plus 30 stale ones. The justification record for the non-compliant devices was requested in session and none was produced. The record that made 41 non-compliant devices acceptable in July, by justifying each and asserting zero CUI devices among them, no longer covers the population. A C3PAO samples from the inventory, and an inventory that does not reconcile cannot support sampling.

REQUIRED FIX

Rebuild the device hygiene record against the current non-compliant set with a CUI or non-CUI determination and an owner on each row, approved by the ISSM. Explain and close the Entra to Intune delta. Reissue the asset inventory with the five-category CMMC asset classification.

EVIDENCE TO PRODUCE

All devices export with counts visible, Entra device export, rebuilt and approved hygiene record, classified asset inventory.

LC-10 **S1** Policy assignment counts exceed the entire managed device population

PRACTICES CM.L2-3.4.1, CM.L2-3.4.2, CA.L2-3.12.4; scoping determination under 32 CFR 170.19

OBSERVED LIVE

Delivery Optimization is assigned to 566 devices and endpoint analytics reports errors on 571, against roughly 370 devices in All devices. A Defender exclusion set named after headquarters reaches 536 devices, a remote management allow policy 532, the password policy 576 users and the CUI banner policy 130 users, against a declared enclave of roughly 90. Either the inventory or the assignment reporting is wrong, and every count is four to six times the declared enclave.

REQUIRED FIX

Reconcile the inventory before any further remediation. Publish one authoritative device count and one authoritative user count, then rebuild policy targeting from named groups whose membership is derived from that register.

EVIDENCE TO PRODUCE

Reconciliation worksheet: Intune count, Entra count, justified deltas, CUI subset, with the assignment count of each CUI policy alongside.

LC-11 **S3** Stale device cleanup runs at 180 days

PRACTICES CM.L2-3.4.1, IA.L2-3.5.6

OBSERVED LIVE

The device cleanup rule deletes device objects after 180 days of inactivity, while the identity policy applies a 90-day standard to accounts. The 180-day horizon is why 30 stale devices are sitting in the tenant.

REQUIRED FIX

Reduce to 90 days after confirming no in-use device is dormant longer than that, and record the change through the change advisory board.

EVIDENCE TO PRODUCE

Cleanup rule screenshot and change ticket.

Scope integrity 3 findings

LC-12 **S1** Out-of-scope geographies are live inside CUI-relevant policy targets

PRACTICES Scoping determination under 32 CFR 170.19; SC.L2-3.13.1, AC.L2-3.1.12, CA.L2-3.12.4

OBSERVED LIVE

The SSP declares headquarters as the sole in-scope facility. The console shows an RDP host group for an out-of-scope site with 17 hosts, application control exclusions for devices in two out-of-scope countries, a hotspot policy targeting over 90 users at a remote site, and users from a third country inside a Conditional Access policy with a matching country-specific taskbar profile. Scope is settled before practices are assessed, so this is a gate rather than a finding.

REQUIRED FIX

Make one decision and carry it everywhere. Either re-declare the boundary to include every site that touches CUI and accept the practice consequences for those sites, or remove the out-of-scope hosts and users from every CUI group and prove the removal. Do not enter a C3PAO assessment with both versions coexisting.

EVIDENCE TO PRODUCE

Revised scope statement and diagram, group membership exports showing only in-scope hosts, removal tickets.

LC-13 **S2** FCI and CUI cohorts are merged in policy targeting

PRACTICES SC.L2-3.13.1, CM.L2-3.4.2; CMMC asset categorisation

OBSERVED LIVE

Browser hardening, Defender update controls and the default endpoint privilege management policy are assigned to combined FCI and CUI groups. ASR exclusions are split into a CUI set and a non-CUI set that share the same fleet. The enclave has to be demonstrable in the console, not only on the diagram.

REQUIRED FIX

Split targeting so every CUI-relevant policy names a CUI-only group. Keep FCI policies separate even where the settings are identical.

EVIDENCE TO PRODUCE

Assignment screenshots per policy showing CUI-only groups.

LC-14 **S2** CUI group sprawl: four different counts describe the same population

PRACTICES IA.L2-3.5.1, AC.L2-3.1.1, AT.L2-3.2.1, CA.L2-3.12.4

OBSERVED LIVE

One CUI group holds 118 members, a second holds 109, the CUI banner policy reaches 130, and the canonical register the SSP cites says roughly 90. The session note records “too many CUI user groups”. Every downstream count depends on this one: training completion, Terms of Use acceptance, MAM targeting and BitLocker scoping.

REQUIRED FIX

Designate one CUI group with dynamic membership driven by an HR attribute. Delete or rename every other CUI-named group. Reissue the canonical register from the tenant rather than from a spreadsheet, and repoint MAM, BitLocker, Terms of Use and banner policies at the single group.

EVIDENCE TO PRODUCE

Group definition and membership export, reissued canonical register, screenshots of each reported policy.

Endpoint hardening 9 findings

LC-15 **S1** Application control is still not enforcing, and its POA&M placement is not admissible

PRACTICES MA.L2-3.7.2 (5 points), CM.L2-3.4.8 (5 points), CM.L2-3.4.9; 32 CFR 170.21(a)(2)(ii); 32 CFR 170.24(c)(2)(i)(B)(I)

OBSERVED LIVE

WDAC and App Control policies are recorded on the POA&M rather than enforcing. A device exclusion group holds five devices and devices in two out-of-scope countries are excluded as well. The contractor's position was that the POA&M covers it. It does not: both practices are valued at five points, and 170.21(a)(2)(ii) bars anything above one point from a POA&M. Listing them creates a second finding, because it shows the plan was built without applying the rule.

REQUIRED FIX

Choose one of three routes deliberately. Route 1, implement: resolve the signing problem for the engineering toolchain with a managed installer or publisher rules, flip the CUI cohort to enforce, hold for 30 days and collect block events. Route 2, temporary deficiency under 170.24(b)(1)(ii): narrow, read narrowly, and it needs a dated, reviewed, moving remediation record. Route 3, enduring exception under 170.24(b)(1)(i): honest if enforce genuinely cannot be reached, but the exception and its mitigations must be written into the SSP now. In every case remove both practices from the POA&M.

EVIDENCE TO PRODUCE

Route 1: policy XML in enforce mode, assignment screenshot, CodeIntegrity 3076 and 3077 samples from two sampled devices, change record. Route 2: dated operational plan of action with review entries. Route 3: SSP section describing the exception, the technical reason and the compensating controls, approved by the ISSM.

LC-16 **S1** A named account is granted local administrator organisation-wide

PRACTICES AC.L2-3.1.5, AC.L2-3.1.6, AC.L2-3.1.7

OBSERVED LIVE

A configuration profile adds a named administrative account to local administrators on every device, with no ticket, expiry or business justification. Separately, the policy that added Global Administrators as local administrators now reports zero, which closes that part of the July finding.

REQUIRED FIX

Scope the profile to the specific devices that require it, attach a ticket and an expiry, or remove it and use LAPS with time-bound elevation. Empty the Entra joined device local administrator role noted in LC-01.

EVIDENCE TO PRODUCE

Profile assignment screenshot after scoping, net localgroup administrators output from two sampled CUI endpoints, change ticket.

LC-17 **S1** USB blocking carries exclusion groups, including a daily-driver account

PRACTICES MP.L2-3.8.7, MP.L2-3.8.8, MA.L2-3.7.4, SI.L2-3.14.5

OBSERVED LIVE

The USB block policy excludes two administrative accounts and one daily-driver user account. Scan on connect for removable media is not configured. The August review had already found usbBlocked set to False fleet-wide, roughly 200 USB mount events in 30 days and no scan logs. The exclusion mechanism is how media gets through, and there is no scanning behind it, so neither the primary nor the compensating control is in place.

REQUIRED FIX

Remove the daily user account from the exclusion today. Configure scan on connect for removable drives and retain the logs. If administrative exclusions must remain, back them with registered, encrypted, company-issued media listed in the asset register. Correct the Media Protection Policy so it no longer claims a prohibition that is not enforced.

EVIDENCE TO PRODUCE

Device control policy screenshot with exclusions, removable media register, Get-MpPreference output from a sampled device, scan log samples.

LC-18 **S2** Key ASR rules are in audit mode and antivirus exclusions are broad and unjustified

PRACTICES SI.L2-3.14.2, SI.L2-3.14.4, CM.L2-3.4.6, CM.L2-3.4.7, CM.L2-3.4.9

OBSERVED LIVE

The rules that block process creation from PSEXEC and WMI and block executables that fail the prevalence, age or trusted-list test are both in audit mode. Exclusions name a remote management tool, a PDF editor, a CAM application and a setup executable, several by bare filename, split across CUI and non-CUI sets. A bare filename exclusion can be satisfied by any file with that name.

REQUIRED FIX

Move the core ASR set to block on the CUI cohort after a short audit review. Re-express every exclusion as a full path plus publisher, attach a written justification and an owner, and remove the installer exclusion entirely.

EVIDENCE TO PRODUCE

ASR rule state screenshots, exclusion register with justifications, a blocked event sample.

LC-19 **S2** Disk encryption is not universal and FIPS evidence is still absent

PRACTICES SC.L2-3.13.11, SC.L2-3.13.16, MP.L2-3.8.1, MP.L2-3.8.9

OBSERVED LIVE

The BitLocker compliance policy applies only to the CUI user group and a separate encrypt-required group exists, so encryption is not applied to all devices. A sampled device showed LAPS and BitLocker healthy. SC.L2-3.13.11 has been Not Met since July purely for want of CMVP certificate numbers, which cost nothing to produce.

REQUIRED FIX

Require BitLocker XTS-AES-256 on every device in or adjacent to the enclave. Publish the CMVP certificate numbers for the cryptographic modules in use and cite them in the SSP. Keep the sampled device check as evidence: it is the first clean LAPS artefact in the package.

EVIDENCE TO PRODUCE

Encryption report showing 100 percent of in-scope devices, FIPS policy assignment screenshot, CMVP certificate references.

LC-20 **S2** The session lock policy is failing on devices and carries an unexplained exemption

PRACTICES AC.L2-3.1.10, AC.L2-3.1.11

OBSERVED LIVE

The screensaver policy is in a failing state in the console. A device lock exemption exists for an executive exception with a single member and no reason recorded. Policy says a pattern-hiding lock after 15 minutes, the tenant says 30, and the inversion has been open since July. The timed lock demonstration has never been captured.

REQUIRED FIX

Fix the deployment error and confirm success across the fleet. Resolve the 15 versus 30 minute conflict by changing either the tenant or the policy, not by leaving both. Remove the exemption or record a written justification with an expiry. Run and film the timed lock test.

EVIDENCE TO PRODUCE

Profile deployment status screenshot showing success, policy text aligned to the tenant value, timed lock demonstration capture.

LC-21 **S2** The configuration baseline contains erroring, conflicting, empty and spare profiles

PRACTICES CM.L2-3.4.1, CM.L2-3.4.2, IA.L2-3.5.2

OBSERVED LIVE

The Windows Hello profile reports 22 errors and 19 conflicts. A disable Windows Hello policy is empty, another policy is blank, and profiles named SPARE exist. Endpoint analytics reports errors on 571 devices. Sixty-nine configuration profiles are present in total. A console carrying empty and conflicting profiles reads as an unmanaged baseline regardless of what the documentation says.

REQUIRED FIX

Resolve the Windows Hello conflicts, delete the empty and spare profiles or move them into a clearly named staging group outside the CUI scope, and clear the endpoint analytics errors. Then export the profile list as the baseline of record.

EVIDENCE TO PRODUCE

Per-profile deployment status export showing zero conflicts on CUI-targeted profiles, baseline export with a version and an approval.

LC-23 **S2** CUI users can sign in to shared PCs

PRACTICES IA.L2-3.5.1, IA.L2-3.5.2, AU.L2-3.3.1, AU.L2-3.3.2, AC.L2-3.1.1, MP.L2-3.8.1

OBSERVED LIVE

CUI users are able to log in to shared PCs. Shared PC mode puts individual attribution of audit records at risk and leaves cached CUI on a device that multiple users reach. It intersects with the shared account finding in LC-03.

REQUIRED FIX

Exclude CUI users from shared PC devices, or remove shared PC mode from anything in the enclave. If it must remain, prove per-user profile isolation, credential caching disabled, and per-user attribution in the audit log.

EVIDENCE TO PRODUCE

Shared PC profile assignment, an audit sample showing per-user attribution on such a device, or the removal record.

LC-32 **S2** Standard users hold local administrator on their own PCs, granted through per-device groups

PRACTICES AC.L2-3.1.5, AC.L2-3.1.6, AC.L2-3.1.7, CM.L2-3.4.6, CM.L2-3.4.9, AU.L2-3.3.8

OBSERVED LIVE

The local Administrators group on a sampled endpoint shows users holding local administrator on their own machines, assigned through groups scoped to each PC. Per-device scoping is better than a blanket grant but does not answer the practice: such a user can tamper with Defender, alter audit configuration and remove management agents. With application control in audit mode (LC-15) and broad exclusions (LC-18), nothing stops what those users choose to run. No exception record, expiry or compensating control exists.

REQUIRED FIX

Establish who holds these rights and why. Remove them for anyone without a documented technical need. Where a need is real, replace standing local administrator with Intune Endpoint Privilege Management elevation rules on named applications, or a time-bound LAPS retrieval through the service desk. Record any residual grant as an approved exception with a justification and an expiry.

EVIDENCE TO PRODUCE

Full list of per-PC administrator groups and members, net localgroup administrators output from two sampled CUI endpoints, the exception register, the Endpoint Privilege Management policy that replaces the rest.

Change control 1 finding

LC-22 **S2** Live configuration exceptions carry no ticket and no approval

PRACTICES CM.L2-3.4.3, CM.L2-3.4.4, CM.L2-3.4.5, AC.L2-3.1.5

OBSERVED LIVE

An always-on high performance exception applies to a virtual machine with no ticket and no approval. A device restriction exception names an individual with no reason. The antivirus compliance policy is assigned to company-owned devices plus an executive-exempt device group, and one device in that exempt group is in scope. Configuration management is assessed on whether change control operates, not on whether a policy describes it.

REQUIRED FIX

Retro-ticket every live exception through the change advisory board with a business justification and an expiry date, or remove it. Remove the in-scope device from the executive-exempt group.

EVIDENCE TO PRODUCE

Change advisory board minutes and tickets referencing each exception, revised group membership.

Boundary & external services 1 finding

LC-24 **S1** A secure web gateway's trusted root CA is deployed to endpoints, on a commercial tenant

PRACTICES SC.L2-3.13.8, SC.L2-3.13.11, SC.L2-3.13.15, SC.L2-3.13.16, SC.L2-3.13.7, CA.L2-3.12.4, DFARS 252.204-7012

OBSERVED LIVE

A root trusted CA profile for a cloud secure web gateway, with one-year validity, is deployed to endpoints. It was seen in the Intune configuration profile list; the gateway console was not opened. The gateway tenant was confirmed commercial in July, while the SSP and the customer responsibility matrix still claim FedRAMP High and IL5. A pushed root CA means TLS interception, so CUI is being decrypted and inspected inside a commercial cloud service. That is a control failure, a misstatement in the SSP, and it engages the DFARS 252.204-7012(b)(2)(ii)(D) cloud service condition. CA.L2-3.12.4 can never sit on a POA&M.

REQUIRED FIX

This is an architecture decision, not a console setting. Three viable paths: migrate to the gateway's government cloud with the FedRAMP authorisation and a signed customer responsibility matrix; exclude the CUI enclave from TLS inspection and route it through an authorised path; or replace the service for CUI traffic. Whichever is chosen, correct the SSP and the responsibility matrix immediately, because the false FedRAMP claim stands as a finding on its own until it is withdrawn.

EVIDENCE TO PRODUCE

Decision memo signed by the ISSM, revised responsibility matrix, service provider authorisation package or the exclusion configuration, client About screenshot recording the true cloud name.

Patch & vulnerability 1 finding

LC-25 **S3** Update rings and patch compliance reporting exist; the service level conflict and a KEV item remain

PRACTICES SI.L2-3.14.1, RA.L2-3.11.3, CM.L2-3.4.1

OBSERVED LIVE

Windows update rings are configured and patch compliance reporting runs automatically, materially better than the August position of no timeframes and no report. What remains is documentary: the SOP states 7 and 14 days while the patch policy states Critical 15, High 30 and Medium 90. An assessor tests against whichever is stricter and finds the contradiction either way. A 7-Zip KEV item is open on roughly 31 devices past its due date.

REQUIRED FIX

Reconcile the SOP and the policy to a single service level and reissue whichever document changes. Close the KEV item. Keep the compliance report as a recurring artefact with a named owner.

EVIDENCE TO PRODUCE

Ring settings and assignment screenshots, the automatic patch compliance report export, the reconciled service level in one document, KEV closure record.

Mobile application management 1 finding

LC-26 **S1** App protection permits 250 characters of cut and copy out of managed apps, and the PIN never expires

PRACTICES AC.L2-3.1.19, AC.L2-3.1.20, MP.L2-3.8.7, SC.L2-3.13.16

OBSERVED LIVE

The app protection policy sets the cut and copy character limit to 250 and PIN reset after a number of days to No. The mobile device policy says copy and paste of CUI to unmanaged apps shall be blocked, and 250 characters is enough to move a marking, an identifier or a coordinate set into a personal application. The policy also targets the 118-member group rather than the roughly 90-user roster the SSP cites.

REQUIRED FIX

Set the cut, copy and paste character limit to 0 and restrict data transfer to policy-managed apps only. Enable PIN expiry. Re-verify that save-as remains restricted to OneDrive for Business and SharePoint Online. Repoint the policy at the single authoritative CUI group once LC-14 is resolved.

EVIDENCE TO PRODUCE

App protection policy settings screenshots, assignment screenshot, a device-level demonstration that copy out is blocked.

Third-party applications 3 findings

LC-27 S1 An uncontrolled enterprise application estate holds tenant-wide Graph permissions, much of it without owners

PRACTICES AC.L2-3.1.20, AC.L2-3.1.1, AC.L2-3.1.2, AU.L2-3.3.8, AU.L2-3.3.9, RA.L2-3.11.1, SC.L2-3.13.1, CA.L2-3.12.4, DFARS 252.204-7012 flow-down

OBSERVED LIVE

Fifty-three applications were reviewed live. Among them: an AI assistant integration holding all permissions with sign-in activity present; a portal automation registration with Sites.FullControl.All, Files.ReadWrite.All, Directory.Read.All and TermStore.ReadWrite.All, flagged red in the console; a second automation registration holding all Graph and SharePoint permissions; a backup service registration with Files.ReadWrite.All, Sites.Manage.All and Mail.Send and no owner; Graph command line tools with Mail.ReadWrite.All; a PDF editor with mail read and write plus user impersonation; a deployment tool signing in non-interactively under a named admin account; and an IDE extension carrying user-consented Sites.Read.All and full control of all site collections, which directly contradicts the accepted claim that users cannot consent. Seventeen registrations have no owner recorded. None of this appears in the SSP, the responsibility matrix or the POA&M.

REQUIRED FIX

Run a consent and permission audit across all 53 applications. For each, record owner, business purpose, data reached, whether it can reach CUI, authorisation status (FedRAMP or SOC 2 Type II) and a keep or remove decision. Replace tenant-wide write scopes with Sites.Selected wherever the application only needs specific sites. Disable every application with no owner. Verify in the portal, not in a JSON export, that user consent is off and allowedToCreateApps is false. Add every surviving application that can reach CUI to the responsibility matrix as an external service provider with flow-down language.

EVIDENCE TO PRODUCE

Application disposition register, permission grant export before and after, consent settings portal screenshot, updated responsibility matrix.

LC-28 S1 A third-party backup platform is still present in the tenant

PRACTICES AC.L2-3.1.20, CM.L2-3.4.9, MP.L2-3.8.9, CA.L2-3.12.4

OBSERVED LIVE

The backup platform's Intune integration registration holds permissions with a named admin account attached and no owner, and its main registration shows a headquarters user group and an IT administrator assigned. The SSP changelog records the platform as removed and the evidence package asserted it was absent. The removal has now failed verification three times. The August review found no backup artefacts of any kind and one empty archive, so what protects CUI data now is unanswered.

REQUIRED FIX

Delete both service principals, remove the user and group assignments, sweep endpoints for the agent through discovered apps, and produce a 30-day sign-in export showing zero activity. Separately, document and demonstrate the backup mechanism that replaced it, with a restore test record.

EVIDENCE TO PRODUCE

Service principal deletion record, filtered sign-in log with no results, discovered apps search showing no agent, backup job configuration and a restore test.

LC-29 S2 The managed service provider's service principal holds a standing privileged role

PRACTICES AU.L2-3.3.8, AU.L2-3.3.9, AC.L2-3.1.5, CA.L2-3.12.4

OBSERVED LIVE

The provider's service principal holds Exchange Administrator with a named admin account as owner. The July review found the same principal holding Compliance Administrator and Privileged Authentication Administrator, with an actor from the provider's domain visible in the audit trail. A third party with standing administrative roles and no documented relationship is a direct finding against audit record protection, and the Log Analytics workspace access export requested in July was never supplied correctly.

REQUIRED FIX

Remove the standing role and move to PIM-eligible activation with approval. Name the provider in the SSP and the responsibility matrix with a DFARS flow-down agreement in place. Supply the Log Analytics workspace access control export rather than an Entra roles export.

EVIDENCE TO PRODUCE

Role assignment screenshot after removal, provider agreement, workspace IAM export.

Session coverage 1 finding

LC-31 S2 The session produced notes, not evidence artefacts

PRACTICES CA.L2-3.12.1, CA.L2-3.12.3; evidence sufficiency across every practice touched

OBSERVED LIVE

Every observation was recorded as a written note. None of the screenshots or exports named in the workbook's evidence column was captured, and nothing carries a visible system clock or a date-stamped filename. A C3PAO accepts a live capture as Test evidence because the capture proves the state at a point in time. A written note proves only that the consultant says so. That applies to the favourable results too: the Terms of Use pass, the healthy LAPS and BitLocker state and the patch rings all need an artefact before they count.

REQUIRED FIX

Adopt a two-person format: one drives the console, one captures. No row is closed until its artefact is saved under a date-stamped name in the control's evidence folder. Re-capture the rows already observed, starting with the ones that produced a good result, because those are the ones the contractor needs to be able to prove.

EVIDENCE TO PRODUCE

A dated evidence folder per control containing the named capture, cross-referenced in the evidence register.

04 The contradiction register

Fourteen places where the live tenant contradicted a position stated in a policy, the SSP, the customer responsibility matrix or previously submitted evidence.

#	Stated position	Live tenant state	Finding
1	The privileged access standard and the SSP: Global Administrator activation is approval-gated through PIM, with 19 standing and 38 eligible assignments	PIM is not in use. A named admin account holds Global Administrator with a permanent end time. No Security Administrator is assigned.	LC-01
2	July evidence: "MFA for All" set to All users	The policy excludes a service account group containing seven generic identities, a guest group and an executive exception group.	LC-02
3	July evidence: the shared admin account was renamed and no shared identities remain	An administrator mailbox account, an IT support account, an IT operations account, two connector accounts, a SharePoint test user and a testbed account are live.	LC-03
4	Identification and Authentication Policy: inactive accounts reviewed at 90 days and deactivated within five business days	Approximately 100 stale user accounts, 17 stale guests and 30 stale devices.	LC-04
5	SSP: headquarters is the sole in-scope facility, one named enclave, roughly 90 CUI users	An RDP host group at an out-of-scope site with 17 hosts, application control exclusions for two out-of-scope countries, a remote site policy for over 90 users, users from a third country inside Conditional Access.	LC-12
6	SSP section 5: roughly 90 CUI users, canonical register of 18 July	CUI groups holding 109, 118 and 130 members, plus a session note that there are too many CUI groups.	LC-14
7	Media Protection Policy: removable media restricted to company-issued, identifiable, registered media	The USB block policy carries exclusion groups, one containing a daily-driver user account. The August review had already found usbBlocked set to False fleet-wide.	LC-17
8	Mobile Device Management Policy: copy and paste of CUI from managed to unmanaged apps shall be blocked	The app protection policy permits 250 characters of cut and copy, and the PIN never expires.	LC-26
9	July evidence: users cannot consent to applications, allowedToCreateApps is false, admin consent workflow is on	An IDE extension carries user-consented Sites.Read.All and full control of all site collections.	LC-27
10	SSP changelog: the third-party backup platform has been removed	Two registrations remain, one with a named admin account attached and no owner, one with a headquarters user group and an IT administrator assigned.	LC-28
11	SSP and customer responsibility matrix: the secure web gateway operates at FedRAMP High and IL5	The gateway tenant was confirmed commercial in July, and its root CA is now deployed to endpoints, so CUI is decrypted inside a commercial service.	LC-24
12	Access Control Policy: pattern-hiding lock after no more than 15 minutes on all devices	The screensaver policy is failing, the tenant value is 30 minutes, and a device lock exemption exists with one member and no reason.	LC-20
13	POA&M and SSP: application control is moving to enforce	Application control policies are recorded on the POA&M and carry a five-device exclusion group plus two-country exclusions.	LC-15
14	Access Control Policy: least privilege, no standing local administrator rights	A profile grants a named administrative account local administrator organisation-wide with no exception record.	LC-16

Why assessors weight accuracy findings

A C3PAO does not test all 110 requirements to the same depth. The team samples. How wide the sample runs is decided early, and it is decided by how far the written package can be trusted. Every contradiction between the SSP and the console is evidence that the package was written from intent rather than from the system, and each one widens the sample.

That is the mechanism behind the fourteen rows opposite. None of them is exotic. PIM was planned, described and never switched on. The MFA policy was set to All users and then an exclusion group grew underneath it. The backup platform was scheduled for removal, the changelog recorded the removal, and the registrations stayed. These are ordinary operational drift. What makes them findings is that the document kept saying the old thing.

Three reasons the weighting is heavy

1. **CA.L2-3.12.4 cannot be deferred.** The SSP requirement is one of six named in 32 CFR 170.21(a)(2)(iii) that may never appear on a POA&M at any point value. An inaccurate SSP is therefore an immediate Not Met with no plan-of-action route out of it. A false FedRAMP claim, a privilege model the tenant does not run or a boundary the groups do not honour each land here.
2. **Accepted evidence becomes a liability.** Four of the fourteen rows are July evidence that was accepted in good faith: MFA for All, no shared identities, users cannot consent, backup platform removed. When a later check contradicts accepted evidence, the assessor has to ask what else in the evidence folder was true on the day and is not true now.
3. **The False Claims Act reads the same documents.** An SPRS score is a representation to the government. In the LOGZONE matter the gap between a self-score of 110 and a DCMA score of -170 was the case. A contradiction register is the cheapest way to find that gap before someone else does.

Run your own contradiction test

For every sentence in your SSP that describes a configured state, find the console screen that proves it and capture it with the clock visible. Record the pairs in a four-column table: stated position, source document, live state, capture filename.

Then sort by the gap. Anything where the live state is weaker than the statement is a contradiction and must be fixed in one direction before assessment: change the tenant, or change the document. Leaving both is the finding.

Start with the claims that are easiest to test and most often wrong:

- Who holds Global Administrator and for how long
- Who is excluded from the MFA policy
- How many members the CUI group has, in every group with CUI in its name
- Which third-party services are registered as enterprise applications
- What the authorisation status of each external service really is
- What the session lock, idle timeout and sign-in frequency values are, in both planes

The contractor in this report had 14 contradictions in 32 findings. The number was not the problem. Nobody had looked.

05 POA&M admissibility worksheet

32 CFR 170.21 decides which Not Met requirements may sit on a plan of action. Most contractors apply the rule after the assessment. It has to be applied before.

The rules, in the order an assessor applies them

170.21(a)(2)(ii) Only requirements with a point value of **1** may be placed on a POA&M. One exception: **SC.L2-3.13.11** (3 points) may be carried where encryption is employed but is not FIPS-validated.

170.21(a)(2)(iii) Six requirements are barred from a POA&M at any point value: **AC.L2-3.1.20** (external connections), **AC.L2-3.1.22** (publicly accessible content), **CA.L2-3.12.4** (system security plan), **PE.L1-3.10.3**, **PE.L1-3.10.4** and **PE.L1-3.10.5** (physical access).

170.21(a)(2)(i) Conditional status requires the assessment score divided by the total number of requirements to be at least **0.8**. For 110 requirements that is a score of **88 or better**.

170.21(b) POA&M closeout. Every item must close within **180 days** of the assessment, confirmed by a closeout assessment. Miss the window and conditional status lapses.

170.24(c)(2) Point values. The score starts at **110** and each Not Met requirement subtracts its value: **5** for basic requirements and a set of high-impact derived ones, **3** for a middle set, **1** for the rest. Two partial credits exist: **IA.L2-3.5.3** at 3 points off when MFA covers only remote and privileged users, and **SC.L2-3.13.11** at 3 points off when encryption is in place but not FIPS-validated.

170.24(b)(1) Two routes score as Met without being fully implemented: an **enduring exception** described in the SSP with its mitigations, and a **temporary deficiency** with an operational plan of action and documented reviews. Both must exist in writing before the assessment.

Worked example: the engagement's position

The contractor's POA&M carried three five-point practices as open items: **MA.L2-3.7.2** (application control, basic), **CM.L2-3.4.8** (software allow and deny, derived) and **IR.L2-3.6.2** (incident reporting, basic). Two more were at risk of landing on it: **CA.L2-3.12.4** and **AC.L2-3.1.20**, both barred at any value.

Practice	Value	Admissible
MA.L2-3.7.2	5	No
CM.L2-3.4.8	5	No
IR.L2-3.6.2	5	No
CA.L2-3.12.4	barred	No, at any value
AC.L2-3.1.20	barred	No, at any value
SC.L2-3.13.11	3	Only under the FIPS exception

The arithmetic, illustratively. Three five-point practices Not Met take the ceiling from 110 to 95 on their own. The conditional gate is 88, so at most 22 points of deductions may remain across everything else, and every one of those must be a one-point item (or **SC.L2-3.13.11** under its exception). That means a lawful POA&M can hold at most 22 one-point items, or 19 plus **SC.L2-3.13.11**. The contractor's position was 8 Met, 55 Partial and 47 Not Met. Even before any five-point item is counted, 102 requirements short of Met cannot fit inside 22 points.

Closing the three five-pointers is necessary and not sufficient. The volume of Not Met is the larger problem, and it only shows up when Partial is scored honestly.

Blank worksheet

List every requirement that is not fully Met today. Fill the value from the current DoD Assessment Methodology. A requirement is admissible only if its value is 1 (or SC.L2-3.13.11 under the exception) and it is not one of the six barred requirements. Anything not admissible must reach Met, or be written up as an enduring exception or temporary deficiency, before the assessment.

Requirement	Value 1 / 3 / 5	Barred by 170.21(a)(2)(iii)?	Status today Met / Not Met	Admissible on POA&M?	Owner	Close by (≤ 180 days)	Evidence that closes it

Starting score	110
Minus the sum of values of every Not Met requirement (Partial counts as Not Met, less the two partial credits)	- _____
Equals your assessment-method score	= _____
Divide by 110. Conditional status needs 0.8 or more, which is 88 or better.	_____ / 110
Count of items on the POA&M that are not admissible (must be zero before you schedule)	_____

Point values in this worksheet are to be taken directly from the current DoD CMMC Assessment Methodology and 32 CFR 170.24, not from this report. The illustration on the previous page shows the mechanism and is not a computed SPRS score.

06 The intake-to-mock journey

Three months separated the intake gap assessment from the live console walkthrough. Some things moved a long way. The things that did not move share one pattern.

Intake, June 2026

- **20 of 110** practices fully implemented
- True SPRS-method score **-159**; formally No Score with no SSP
- A 90-item internal "POA&M" that included barred practices (3.1.20, 3.1.22, 3.12.4, 3.10.3/4/5) and five-point practices
- No operational SIEM: connectors unconfigured
- On-prem CUI VMs at two offices missing from the SSP boundary
- NOFORN marking unverified against contracts
- No change logs, rollback plans or approval authority
- CUI printing at homes and remote sites uncontrolled
- Incident reporting pointed at the wrong agency; no DIBNet medium-assurance certificate
- Policies contradicted the SSP and the tenant
- CUI inside a third-party backup platform's scope
- Unified Audit Log at the 90-day default against a 12-month policy



Mock stage, September 2026

- **8 Met, 55 Partial, 47 Not Met** against all 110
- SSP written, but contradicted by the tenant in 14 places
- POA&M still carries three five-point practices
- Patching fixed: update rings and automatic compliance reporting
- LAPS and BitLocker healthy on a sampled device
- Terms of Use recovered to correct scope and near-full acceptance
- Global Admins as local admins at zero
- Backup platform still registered after three removal attempts
- Boundary now wrong in the other direction: out-of-scope sites inside CUI targets
- New exposure: 53 enterprise applications with tenant-wide permissions, many unowned
- Stale accounts grew to about 100 users, 17 guests, 30 devices

What moved, and why

Four items moved from Not Met to something an assessor could accept, and all four share a shape: a single owner, a single console, a configuration with a visible status. **Patching** went from no timeframes and no report to rings with deadlines and an automatic compliance report. **LAPS** went from a 403 error blob in July to a clean artefact on a sampled device. **Terms of Use** went from a single pilot user, 4 of roughly 90 acceptances, to correct scope and near-full coverage. The **Global Administrators as local administrators** policy went to zero.

The items that did not move share the opposite shape. They are cross-cutting, they depend on a decision someone has to own, and the console does not show a red status when they are wrong. PIM is a decision about who may be a permanent Global Administrator. The boundary is a decision about which sites are in. The backup platform removal needed verification three times and nobody owned the third. The POA&M structure needed someone to read 170.21.

The number went down while the work went up

Twenty fully implemented at intake, eight Met at mock. Nothing regressed; the lens changed. Intake counted a practice as implemented where the SSP said so and nothing visible contradicted it. The mock applied the 800-171A objectives one by one and demoted every practice where the console contradicted the document. Expect the same drop when you move from self-assessment to assessment, and plan for it rather than being surprised by it.

The lesson: targeting and enforcement state, not absence

Almost nothing in the 32 findings was missing. Enrolment, compliance and configuration policies were present and actively maintained. Conditional Access existed. Application control existed. USB blocking existed. App protection existed. The failures were in three states that look fine at a glance:

- **Wrong target.** The right policy pointed at the wrong group, or at four groups that each claimed to be the CUI population.
- **Wrong mode.** Report-only, audit mode, or a failing deployment that nobody had opened.
- **Exclusion underneath.** A correct policy with an exclusion group that had quietly grown to include a daily-driver account, a testbed, a service account or an executive.

The evidence lesson

The session produced written notes and no captures. A C3PAO accepts a dated capture as Test evidence because the capture proves the state at a point in time. A consultant's note proves only that the consultant says so. Nothing from the session could go into the evidence repository, and that applied to the good results as much as the bad ones. The fix costs nothing: two people in the session, one driving, one capturing, no row closed until its file is saved under a dated name.

What was working, so it is not lost

Terms of Use scoped correctly with acceptance at or near full coverage, the only outright pass, recovered from a July downgrade. Update rings configured and patch compliance reporting running automatically. LAPS and BitLocker healthy on a sampled device, the first clean LAPS artefact in the package. The "Global Administrators as local administrators" policy at zero. Defender tamper protection and controlled folder access scoped to CUI users. A device cleanup rule in place and every enrolment, compliance and configuration policy present and actively maintained. **The problem across the findings is targeting and enforcement state, not absence.**

07 90-day remediation sequence

Derived from the required fixes, sequenced by what unblocks the most. Identity and privilege first, because every other control inherits from who can change it.

Action	Findings	1	2	3	4	5	6	7	8	9	10	11	12	13
Workstream 1 • Identity and privilege first														
Remove daily-driver account from USB exclusion; move report-only CA policies to On	LC-17, LC-05													
Remove organisation-wide local admin profile; remove standing role from MSP service principal	LC-16, LC-29													
Enable PIM with approval and activation window; two break-glass Global Admins; assign Security Administrator	LC-01													
Empty MFA exclusion group; convert generic accounts to workload identities; signed exceptions	LC-02, LC-03, LC-07													
Stale identity campaign and a repeatable quarterly access review	LC-04, LC-30													
Workstream 2 • Scope and boundary second														
One boundary decision: widen the declared scope or remove out-of-scope hosts and users from every CUI group	LC-12, LC-13													
One authoritative CUI group (dynamic); repoint MAM, BitLocker, ToU and banner policies	LC-14, LC-26													
Reconcile Intune, Entra and the hygiene record; publish one device count and one user count	LC-09, LC-10, LC-11													
Gateway decision: government cloud, exclude the enclave from inspection, or replace; correct SSP and CRM	LC-24													
Workstream 3 • Endpoint enforcement third														
Enrolment restrictions; app protection limit to 0 and PIN expiry	LC-08, LC-26													
Application control route decision, then enforce on the CUI cohort and hold 30 days collecting block events	LC-15													
ASR rules to block; exclusions rewritten as path plus publisher with owners	LC-18													
Session lock fixed and aligned; profile baseline cleaned and exported; exceptions retro-ticketed through CAB	LC-20, LC-21, LC-22													
Per-device local admin removed, replaced with EPM rules or time-bound LAPS; shared PC access resolved	LC-32, LC-23													
BitLocker on every in-scope device; CMVP certificate numbers published and cited in the SSP	LC-19													
Workstream 4 • Third-party application estate														
Disable unowned applications; revoke user-consented grants; delete backup platform registrations	LC-27, LC-28													
Disposition register for all 53 applications; Sites.Selected replaces tenant-wide write scopes	LC-27													
Survivors that reach CUI added to the CRM as external service providers with flow-down; replacement backup proven with a restore test	LC-27, LC-28, LC-29													
Workstream 5 • Evidence capture discipline														
Two-person capture format; re-capture every row already observed, good results first	LC-31													
Patch service level reconciled to one number; KEV item closed	LC-25													
SSP, CRM and policies corrected to the tenant's real state; POA&M rebuilt under 170.21	CA.L2-3.12.4													
Internal re-run of the 38 checks with captures; SPRS decision only after the worksheet closes	All													

Weeks are indicative for an organisation of this size with one IT team and an MSP. Nothing is closed until the artefact named on the finding card exists under a dated filename.

Why identity goes first

A permanent Global Administrator, an MSP service principal with a standing role and an MFA exclusion group full of generic accounts can undo every endpoint control. Fix who can change the tenant before changing the tenant.

Why scope goes before endpoints

Every endpoint policy is targeted at a group. Until there is one CUI group and one device inventory, re-targeting a policy moves the problem rather than closing it.

Why evidence runs the whole way

Each fix produces an artefact or it did not happen. Re-capturing the good results early means that if the plan slips, the package still shows dated proof of progress.

08 Checklists

Three lists that compress the engagement: what to confirm before a score goes into SPRS, what a C3PAO looks at in Intune and Entra, and how to capture evidence that counts.

A. Before you post an SPRS score: 12 points

- | | |
|--|--|
| <p>1 ☐ The SSP exists, describes the system as it is configured today, and CA.L2-3.12.4 is Met. No SSP means No Score.</p> <hr/> <p>2 ☐ The boundary in the SSP matches the groups and policy targets in the tenant: one site list, one CUI user count, one device count.</p> <hr/> <p>3 ☐ Every requirement marked Met has at least one dated artefact an assessor could examine or test.</p> <hr/> <p>4 ☐ Partial is scored as Not Met, except the two partial credits (IA.L2-3.5.3 at 3 points off for remote and privileged MFA only; SC.L2-3.13.11 at 3 points off for non-FIPS encryption).</p> <hr/> <p>5 ☐ Point values are taken from the current DoD Assessment Methodology and 32 CFR 170.24, not from working papers or a tool's defaults.</p> <hr/> <p>6 ☐ The POA&M holds only one-point items (plus SC.L2-3.13.11 under its exception) and none of the six barred requirements.</p> <hr/> | <p>7 ☐ Every POA&M item has a named owner and a closure date within 180 days.</p> <hr/> <p>8 ☐ The score divided by 110 is at least 0.8 before anyone relies on conditional status.</p> <hr/> <p>9 ☐ The contradiction test has been run: each configured-state claim in the SSP paired with a dated capture, and every mismatch fixed in one direction.</p> <hr/> <p>10 ☐ The enterprise application estate is inventoried, every registration has an owner, and anything that reaches CUI is in the customer responsibility matrix.</p> <hr/> <p>11 ☐ External service providers (backup, gateway, MSP, any SaaS that holds CUI) are named in the SSP and CRM with their real authorisation status and a flow-down agreement.</p> <hr/> <p>12 ☐ A senior officer signs the score with the SSP version, the date and the CAGE scope recorded, and the SPRS screenshot is kept. A score is a representation to the government.</p> <hr/> |
|--|--|

B. What a C3PAO looks at in Intune and Entra: 38 lines

One line per live check. Mark each pass, fail or partial. Every fail or partial has a matching finding card in chapter 03.

Devices and Compliance 10

- 1 ☐ Device platform enrolment restrictions: personally owned Windows and macOS blocked, corporate identifiers or Autopilot only
- 2 ☐ All devices count in Intune against the Entra device object count, with every delta explained
- 3 ☐ Non-compliant device count, and a justification record naming each device, its owner and whether it handles CUI
- 4 ☐ Compliance policy assignments bounded by one named CUI group, not combined FCI and CUI groups
- 5 ☐ Compliance exemption groups: every member has a ticket, a reason and an expiry
- 6 ☐ BitLocker compliance scope covering every device that can reach CUI, with CMVP module numbers cited
- 7 ☐ Device cleanup rule horizon aligned to the identity policy (90 days), and stale device objects at zero
- 8 ☐ Sampled device: LAPS password rotation and BitLocker status both healthy, captured with the clock visible
- 9 ☐ Sampled device: registered owner matches the signed-in user and the device identifier in the inventory
- 10 ☐ Policy assignment counts never exceed the managed device population or the declared CUI user count

Config and Hardening 8

- 11 ☐ Application control (WDAC or AppLocker) in enforce mode on the CUI cohort, with exclusion groups empty or justified
- 12 ☐ Local administrator membership: no organisation-wide profile, no per-device standing grants, LAPS plus EPM instead
- 13 ☐ USB and removable media control: block enforced, exclusions limited to registered media, scan on connect configured
- 14 ☐ Session lock: deployment status succeeded fleet-wide, timeout matches the written policy, no unexplained exemption
- 15 ☐ Idle timeout enforced on one plane only (Conditional Access or Intune), with no testbed groups in production policies
- 16 ☐ Configuration profile health: zero errors, zero conflicts, no empty, blank or spare profiles in the CUI scope
- 17 ☐ Shared PC mode absent from the enclave, or per-user isolation and attribution proven
- 18 ☐ Trusted root certificate profiles: every third-party CA on endpoints tied to an authorised service in the responsibility matrix

Updates, AV and Vulnerability 4

- 19 ☐ Update rings on the General Availability channel with deferral, deadline and grace set and assigned to all CUI devices
- 20 ☐ Patch compliance report produced automatically, with one remediation service level stated identically in SOP and policy
- 21 ☐ ASR rules in block mode on the CUI cohort; antivirus exclusions expressed as path plus publisher with a written owner
- 22 ☐ Open KEV items at zero past due date, with closure records

Apps and MAM 5

- 23 ☐ App protection cut, copy and paste limit set to 0, transfer restricted to policy-managed apps
- 24 ☐ App protection PIN expiry enabled, and save-as restricted to OneDrive for Business and SharePoint Online
- 25 ☐ App protection policy targeted at the single authoritative CUI group
- 26 ☐ Discovered apps: no agent from a decommissioned third-party platform on any endpoint
- 27 ☐ Endpoint privilege management rules in place for named applications instead of standing admin rights

Entra CA and Identity 11

- 28 ☐ Global Administrator: two break-glass accounts only, everything else PIM-eligible with approval and an activation window
- 29 ☐ Security Administrator and Security Reader assigned to named individuals per the separation of duties matrix
- 30 ☐ "MFA for all users": the exclusion list holds break-glass accounts only, each with a signed exception and an expiry
- 31 ☐ Guest and external MFA policy with no excluded guest groups
- 32 ☐ No Conditional Access policy in report-only mode where the SSP relies on it; one blocked sign-in captured per policy
- 33 ☐ Persistent browser session off for the CUI cohort; sign-in frequency matches the SSP
- 34 ☐ Exception and grace groups: each documented in an SOP with requester, justification, compensating control, expiry and approver
- 35 ☐ Shared and generic accounts at zero; service account register with a named owner for every machine identity
- 36 ☐ Stale users, guests and devices at zero against the 90-day standard, with a signed quarterly review record
- 37 ☐ Terms of Use scoped to the right groups with acceptance at or near full coverage
- 38 ☐ Enterprise applications: owner on every registration, user consent off, no tenant-wide write scopes without a decision, no standing privileged role on any service principal

C. Evidence capture standard

The difference between a finding and evidence is a file. These rules make a screen-share observation assessment grade.

- ☐ **System clock visible.** Every screenshot shows the device clock or the portal timestamp in frame. Crop nothing that proves the date.

- ☐ **Dated filename.** YYYY-MM-DD_control-id_what-it-shows, for example 2026-09-08_IA.L2-3.5.3_MFA-policy-exclusions.png. The filename is read before the file is opened.

- ☐ **Export plus screenshot, as a pair.** A screenshot proves what the screen showed; an export proves the full population. Pair them for anything with a count: group membership, role assignments, device lists, application permissions.

- ☐ **Include and exclude together.** A Conditional Access or compliance policy capture that shows only the include tab proves nothing. Capture the exclusions in the same frame or the next file.

- ☐ **Portal, not JSON, for settings claims.** A JSON export of tenant settings can be edited. The portal screen with the setting and the clock cannot.

- ☐ **One operational event per enforcing control.** A policy state screenshot shows configuration. A blocked sign-in, a CodeIntegrity 3077 event, a timed lock on camera shows operation. Assessors test; give them the test.

- ☐ **Two people in the session.** One drives the console, one captures and names files. A row is not closed until its file is in the folder.

- ☐ **Folder per control, index per folder.** 05_Evidence/IA.L2-3.5.3/ with a one-line register that lists each file, its date and the assessment objective it supports.

- ☐ **Good results first.** The controls you will rely on at assessment are the ones you most need to be able to prove. Capture the passes before the failures.

- ☐ **Re-capture after every fix.** The before capture is the finding. The after capture is the closure. Keep both.

What an assessor will not accept

- A consultant's written note of what was on screen
- A screenshot with no date in frame and a filename like "Screenshot (14).png"
- A policy that is described in a document but was never opened in the console during the session
- A changelog entry that says "removed" with no capture of the empty list
- An exception group with members and no register that names who approved each one and when it expires

What happened in this engagement

Thirty-eight checks were driven and recorded as notes. None of the captures named in the workbook's evidence column was taken. The findings stood, because findings only need to be true. The passes did not, because passes need to be provable. The Terms of Use recovery, the healthy LAPS device and the patch rings all had to be captured again on another day.

Evidence is the only part of readiness that cannot be done later.

09 Further reading

Tools and explainers on itsecops.cloud that extend this report, and the public sources behind the context in chapter 01.

On itsecops.cloud

Run your own 110-practice self-check

<https://itsecops.cloud/cmmc-level-2-gap-analysis-tool/>

SPRS score calculator

<https://itsecops.cloud/sprs-score-calculator/>

CMMC Level 2 continuous compliance checklist

<https://itsecops.cloud/cmmc-level-2-continuous-compliance-checklist/>

CMMC questions, answered

<https://itsecops.cloud/cmmc-questions/>

Conditional status: what happens when the 180 days expire

<https://itsecops.cloud/cmmc-questions/conditional-status-180-days-expiring/>

CMMC compliance services

<https://itsecops.cloud/compliance/cmmc/>

CMMC consultants, USA

<https://itsecops.cloud/cmmc-consultants-usa/>

NIST 800-171 controls list

<https://itsecops.cloud/nist-800-171-controls-list/>

CMMC Phase 2 suspended: what it means

<https://itsecops.cloud/cmmc-phase-2-suspended/>

The self-assessment risk while CMMC is paused

<https://itsecops.cloud/cmmc-paused-self-assessment-risk/>

Class Deviation Revision 3 and DFARS 240

<https://itsecops.cloud/cmmc-class-deviation-revision-3-dfars-240/>

CMMC and the False Claims Act

<https://itsecops.cloud/cmmc-false-claims-act/>

Do I need GCC High for CMMC?

<https://itsecops.cloud/answers/do-i-need-gcc-high-for-cmmc/>

Commercial Microsoft 365 for CUI

<https://itsecops.cloud/answers/commercial-microsoft-365-for-cui/>

What is a CMMC enclave?

<https://itsecops.cloud/answers/what-is-a-cmmc-enclave/>

VEDVERA: the ITSECOPS CMMC GRC tool

<https://itsecops.cloud/vedvera/cmmc-grc-tool/>

This report's hub page (ungated)

<https://itsecops.cloud/research/cmmc-readiness-gap-report-2026/>

Public sources

32 CFR Part 170, the CMMC Program rule (170.19 scoping, 170.21 POA&M, 170.24 scoring)

<https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-170>

NIST SP 800-171A, assessment procedures

<https://csrc.nist.gov/pubs/sp/800/171/a/final>

DoD CIO CMMC documentation: Assessment Guide Level 2, Scoping Guide Level 2

<https://dodcio.defense.gov/CMMC/Documentation/>

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>

DIBNet, cyber incident reporting portal

<https://dibnet.dod.mil/>

Holland & Knight: CMMC Phase 2 suspension and the Reform Task Force

<https://www.hklaw.com/>

Crowell & Moring: Class Deviation 2026-O0025 Revision 3 analysis

<https://www.crowell.com/>

Koprince McCall Pottroff: CMMC pause coverage for contractors

<https://www.ksg.us/>

Secureframe: CMMC news and updates 2026 tracker

<https://secureframe.com/hub/cmmc/news-updates-2026>

CMMC Map: implementation timeline tracker

<https://cmmcmmap.com/>

US Department of Justice: Honeywell Aerospace \$2,042,518 settlement (1 September 2026); LOGZONE matter (18 June 2026)

<https://www.justice.gov/>

Cyber AB: town hall of 29 September 2026, certification and ecosystem counts

<https://cyberab.org/>

Redspin: CMMC pause survey, 1 October 2026

<https://www.redspin.com/>

Merrill Research and CyberSheath: 2025 state of DIB compliance

<https://cybersheath.com/>

Public context verified 26 October 2026. Where a source is given at domain level, search the site for the dated item named.



Book a 30 minute readiness review

Bring your SSP and your tenant. We will run the first ten lines of the 38-line checklist with you on a screen share, capture the evidence the right way, and tell you which of your POA&M items would survive 32 CFR 170.21.

https://itsecops.cloud/contact/?itso=research_cmmc
saleslead@itsecops.cloud

KANSAS CITY
United States

STAVANGER
Norway

24/7 DELIVERY CENTER
India

Gaurav Sengar, CISA
Founder, ITSECOPS

12+ years across cybersecurity, IT operations and compliance. Has helped several companies reach CMMC readiness, and runs ITSECOPS across the United States, Norway and India, delivering managed security, Microsoft 365 GCC implementations and compliance programmes for MSPs and regulated SMBs.

ITSECOPS Research · Report 01 · October 2026 · The CMMC Readiness Gap Report 2026 · Extended Edition

Readiness language only. ITSECOPS is a consultant, not a C3PAO; nothing here is a certification assessment.

© 2026 ITSECOPS. Please link to <https://itsecops.cloud/research/cmmc-readiness-gap-report-2026/> rather than redistributing the file.