CYBERCRUNCH

FOR C3PAO ASSESSORS · DEFENSE & GOVERNMENT ITAD

What a Clean Media-Sanitization Finding Looks Like

The IT asset disposition evidence that resolves MP.L2-3.8.3 to MET on the first pass — why it so often doesn't, and what a properly credentialed ITAD changes for the file in front of you. A reference for the assessment room.

R2v3 | NAID AAA | RIOS | PA DEP

November 10, 2026

CMMC Phase 2 — C3PAO Level 2 certification becomes the default for applicable CUI contracts.

01 / THE FRICTION POINT

The control that's small on paper and slow in the room

A Level 2 assessment runs against 110 NIST SP 800-171 requirements and their 320 assessment objectives. Most resolve through a policy, a configuration, a screen share, a log. Then there's **3.8.3** — one line in the Media Protection family, easy to read past in the SSP, and reliably where a strong program meets a paper trail that was never built.

The pattern is familiar: the organization spent two years hardening the network, but nobody owned what happened to last year's decommissioned drives, the laptops from departed staff, or the multifunction printers returned on a lease. The control is satisfied operationally; it just can't be *shown*. And because Phase 1 only verifies that evidence *exists and is accessible* — without evaluating it or offering advice — disposition is where teams scramble to reconstruct records after the readiness check. Reconstruction is exactly what doesn't survive sampling.

02 / THE CONTROL, PRECISELY

3.8.3 and what its objectives demand

MP.L2-3.8.3 (NIST SP 800-171 §3.8.3): *sanitize or destroy system media containing CUI before disposal or release for reuse.* The 800-171A guide scores two determination statements: **[a]** media is sanitized or destroyed before disposal, and **[b]** before release for reuse — two paths, each needing its own evidence.

It rarely travels alone. Expect to sample it alongside the rest of the Media Protection family: **3.8.1 / 3.8.2** (protect and limit access to media), **3.8.4** (mark media with CUI markings), and **3.8.5 / 3.8.6** (control transport and cryptographically protect CUI on portable media). All three assessment methods apply: **examine** the policy and certificates, **interview** the disposition owner, and **test** by tracing one sampled serial from its inventory retirement entry to its destruction record.

> BOTTOM LINE
>
> 3.8.3 is binary at sampling in a way most controls aren't: the serialized record either exists and reconciles to inventory, or it doesn't — and there's nothing to coach into place during the assessment.

03 / WHAT GOOD EVIDENCE LOOKS LIKE

The artifact set that resolves on the first pass

The disposition evidence that holds up is not voluminous — it's *reconcilable*. Each retired CUI asset should trace from inventory to a sanitization or destruction event that names what was done and how. An assessor can work straight down this map:

What you're confirming	Artifact that shows it	Method
A defined sanitization standard	Written media-sanitization policy mapped to 3.8.3 and NIST 800-88	Examine
Each retired device handled	Serialized, device-level records reconciled to asset inventory	Examine / Test
The right method applied	Certificate citing the 800-88 tier by media type	Examine
Custody was unbroken	Chain-of-custody documentation, facility to processor	Examine / Interview
The downstream is qualified	Processor certifications — R2v3 and NAID AAA	Examine
The process runs as described	Owner walks the workflow; a sampled serial traces end-to-end	Interview / Test

Behind the map sits NIST SP 800-88, which defines three sanitization tiers — the defensible choice depends on media type, condition, and whether media is leaving organizational control:

CLEAR · TIER 1

Clear

Logical overwrite; protects against simple non-invasive recovery. Some internal reuse; rarely sufficient alone for media leaving control.

PURGE · TIER 2

Purge

Cryptographic erase or firmware techniques resistant to lab recovery. A **verified** Purge can satisfy 3.8.3 for media released for reuse.

DESTROY · TIER 3

Destroy

Shred, disintegrate, or incinerate. Most defensible for failed drives, end-of-life flash, and ITAR-adjacent media.

THE DECISIVE TRAIT

Serialization that reconciles to inventory. A certificate naming a device by serial, tied to its retirement entry, is sampleable in seconds. A certificate for "one pallet" names nothing you can trace.

04 / WHERE IT GOES WRONG

The deficiency patterns you've already seen

Most 3.8.3 findings that slide toward NOT MET or a POA&M share a small set of root causes — each visible early in examination:

- [ ] **"We use a recycler."** Answers logistics, not evidence. Vendor selection is not a sanitization record.
- [ ] **Inventory that won't reconcile.** Assets last-seen with no corresponding disposition event — the gap is the finding.
- [ ] **Deleted treated as destroyed.** A format isn't a Purge; SSD and flash wear-leveling leaves recoverable data behind.
- [ ] **Chain-of-custody gaps.** No documented hand-off facility-to-processor for the window that matters most.
- [ ] **Unknown or uncredentialed downstream.** No R2v3 or NAID AAA — the organization can't show what happened after pickup.
- [ ] **ITAR data meeting a foreign person.** Offshore downstream processing of ITAR-adjacent media can constitute an unauthorized export.

Sampling checklist — what to ask for

- [ ] Media-sanitization policy that cites 3.8.3 and names NIST 800-88 as the method standard.
- [ ] A serialized disposition register that reconciles 1:1 with asset-inventory retirements.
- [ ] Certificates that state the 800-88 tier (Clear / Purge / Destroy) per media type, per serial.
- [ ] Chain-of-custody records from facility to processor, with dates and signatures.
- [ ] Current R2v3 and NAID AAA certificates for the downstream processor.
- [ ] For ITAR-adjacent media: documented domestic processing and serial-level destruction.

05 / WHY A CREDENTIALED ITAD REDUCES FRICTION

What you recognize when you see it

R2v3 and NAID AAA are the recognized way an organization demonstrates its downstream is qualified. For an assessor they do real work: they let you treat the processor's controls as *evidenced* rather than reconstructed. Pair recognized certifications with serialized certificates that cite the 800-88 method by media type and a documented chain of custody, and 3.8.3 resolves in the room instead of in a follow-up request.

> You verify the evidence; you don't design the program, and you can't coach it into existence during the assessment. **By the time disposition reaches your sampling, the artifacts are either there or they aren't.** A contractor whose ITAD produces this evidence by routine is simply a faster, cleaner file — because the records were built right the first time.

CyberCrunch builds that evidence set by default — serialized certificates of sanitization and destruction, NIST 800-88 method mapping by media type, documented chain of custody, domestic processing for ITAR-adjacent media, and witnessed destruction on request. We name it here not because an assessor would ever recommend a vendor — that's not the role — but because when this evidence shows up in a file, you recognize what good looks like, and the control moves.

HAVE AN OSC ASKING WHAT "GOOD" LOOKS LIKE?

Point them to this brief.

Or talk to our compliance team about the serialized 800-88 evidence set we produce by default.
ccrcyber.com/contact

This brief accompanies the full reference at promo.ccrcyber.com/articles/cmmc-assessor-disposition-evidence and the assessor field guide at /guides/cmmc-assessor-itad-guide.