

FIELD GUIDE

Understanding CMMC's Specialized Assets



SENTINELBLUE

SUMMARY

Who This Guide Is For

- Organizations Seeking Certification (OSCs)
- Federal contractors in the Defense Industrial Base
- Anyone with an interest in CMMC

What This Guide Contains

- FAQs about specialized assets, compensating controls, and documentation in CMMC.

About Sentinel Blue Field Guides

Security is a team sport. We believe the Defense Industrial Base is stronger when knowledge and expertise are shared openly. That's why we've created free educational resources for federal contractors navigating cybersecurity and compliance challenges.

If you find this guide helpful, please share it with your community. Shields up!

Understanding Specialized Assets in CMMC

Machine shops and manufacturers in the DIB routinely deal with equipment that touches Controlled Unclassified Information (CUI) but wasn't built with modern IT security in mind. From legacy CNC lathes to cutting-edge 3D printers, this kind of equipment shows up on shop floors across the defense industry.

This is where specialized assets come in: a scoping category built specifically for equipment that handles CUI but can't be locked down using conventional IT security practices. Specialized assets are one of the more misunderstood corners of CMMC, so we've created this introductory guide to help.

Q: What are specialized assets?

A: Devices or systems that can process, store, or transmit CUI but can't fully meet the 110 NIST SP 800-171 controls, usually because they're purpose-built equipment rather than general-purpose IT. Under the CMMC Level 2 Scoping Guidance (32 CFR § 170.19), specialized assets fall into five categories: Government Furnished Equipment (GFE), IoT/IIoT devices, Operational Technology (OT), Restricted Information Systems (RIS), and Test Equipment. Common shop floor examples include CNC machines, 3D printers, and similar equipment that can't run endpoint agents or be easily patched.



Q: How are specialized assets different from CUI assets?

A: CUI assets are assessed directly against the full set of applicable NIST SP 800-171 requirements. Specialized assets are still in scope and still have to be documented, but they aren't assessed against those same practices... often because it's technically impossible to secure them in the same way. (You can't use endpoint monitoring on a laser cutter, for example.)

Q: How do you secure specialized assets under CMMC?

A: Through compensating controls, documented in your SSP and reflected in your asset inventory. You can't put MFA on CNC controller, so instead you isolate it, restrict who and what can reach it, and document the reasoning behind your protocols. An assessor won't test the asset against the standard control set, but they will review your documentation and verify the compensating controls are real and functioning.

Q: What documentation do assessors expect to see?

A: Assessors will expect an inventory that lists each specialized asset and its category. They'll also want to see a justification explaining why each one is considered a specialized asset and detailing the compensating controls that have been implemented instead. Lastly, they'll ask for evidence that the compensating controls are actually in place: signed agreements, configuration screenshots, network diagrams, etc.

Q: What are some examples of compensating controls?

A: Choosing the right compensating controls depends heavily on the specific asset and environment. In general, however, compensating controls might include:

- Physical access restrictions
- Network segmentation to isolate the asset from the rest of the CUI environment
- Warning banners or pop-ups on machines that aren't authorized to process CUI
- Signed employee agreements prohibiting CUI on certain equipment
- Boundary-level logging and monitoring where endpoint monitoring isn't possible
- Regular manual checks to confirm the asset hasn't drifted from its documented configuration



Q: What's the biggest mistake that companies make with specialized assets?

A: Confusing them for CRMAs or out-of-scope assets. Specialized assets still touch CUI, so they still belong in the inventory and the SSP. Leaving them out of your documentation is an easy way to fail a CMMC assessment, even if the underlying risk is actually well managed.

Contractor risk managed assets (CRMA) can technically access or reside near CUI, but they have technical safeguards and company policies keeping them from storing, processing, or transmitting CUI, so they don't have to be physically or logically separated. Out-of-scope assets do not touch CUI and don't need to be physically or logically separated.

Q: How should a company manage CMMC compliance for specialized assets?

- **Inventory your assets.** Catalog all GFE, IoT/IloT devices, OT, RIS, and test equipment, flagging anything that processes, stores, or transmits CUI.
- **Assess applicability.** For each asset, determine whether standard CMMC controls can realistically be applied. Wherever they can't, record the specific operational or technical reason why not.
- **Define your compensating controls.** Identify the alternative safeguards you'll use instead, such as network segmentation, physical access restrictions, or enhanced monitoring, and document how each one addresses the relevant risk.
- **Build your evidence base.** Gather artifacts that prove your compensating controls are actually implemented and functioning.
- **Maintain your documentation.** Revisit it whenever your assets change so it always reflects your current environment.



CMMC gaps are cheaper to fix now than during an assessment. Let's talk.

[Contact Us Now](#)