# The Secure Area Strategy

## *Solving the CMMC Scoping Dilemma for Legacy Aerospace Manufacturing*

A Practitioner White Paper

David W. Koran, CMMC Registered Practitioner

David Koran & Associates Inc.

March 2026

# Summary

***Every defense industrial base machine shop owner using an aerospace CNC will be asked the same unpleasant questions about their production system:*** "How can I protect my controlled unclassified information on the CNC controller when it was built prior to the existence of cybersecurity?" The solution is to create the right security around it, not to scrap or dispose of $Millions of dollars' worth of reliable capital equipment.

The Cybersecurity Maturity Model Certification (CMMC) program is currently being implemented in phases. Defense Contractors handling Controlled Unclassified Information (CUI), will be required to demonstrate their compliance with the 110 security requirements as defined by NIST SP 800-171 Revision 2. Most of these controls are able to translate into software configuration and network policy for IT-based organizations. However, due to the nature of Aerospace Manufacturing Operations (i.e. physical work happening in a shop floor environment using Legacy Fanuc, Mazak, Matsuura and Haas controllers), this creates an entirely different compliance environment.

A realistic and viable method to attain CMMC Level 2 compliance within an aerospace environment while retaining older machinery has been proposed in this paper. The author utilized his experiences with implementation of CMMC and ITAR compliance programs at aerospace machining facilities to illustrate the significant time-lapse between regulatory requirements and the capability to meet those requirements on the shop floor. The strategy utilizes a 'Secure Area', which can be defined as a separate area from other areas that are physically or procedurally demarcated. In the Secure Area, a combination of compensating physical, media and personnel controls will provide the necessary security measures to make up for deficiencies provided by legacy technologies alone. This does not constitute a "workaround." Rather it represents the architecture as anticipated by NIST SP 800-171 and the CMMC Assessment Guide for the described operationally constrained conditions.

# The Technical Wall: Why Legacy Equipment Breaks the Standard Model

***The core tension is straightforward.*** A five-axis Matsuura MAM72-35V or a Fanuc Robodrill represents a capital investment that may exceed $500,000 per unit. These machines produce flight-critical components with tolerances measured in ten-thousandths of an inch. They are extraordinary pieces of engineering. They are also, from a cybersecurity standpoint, black boxes.

Most legacy CNC controllers run proprietary real-time operating systems that do not support user authentication, role-based access, audit logging, encrypted storage, or any of the technical controls that NIST SP 800-171 expects from information systems. A Fanuc 31i controller, for example, has no concept of a "user account." There is no password prompt. There is no access control list. The controller boots, loads its parameters, and waits for instructions. That is exactly what it was designed to do, and it does it exceptionally well.

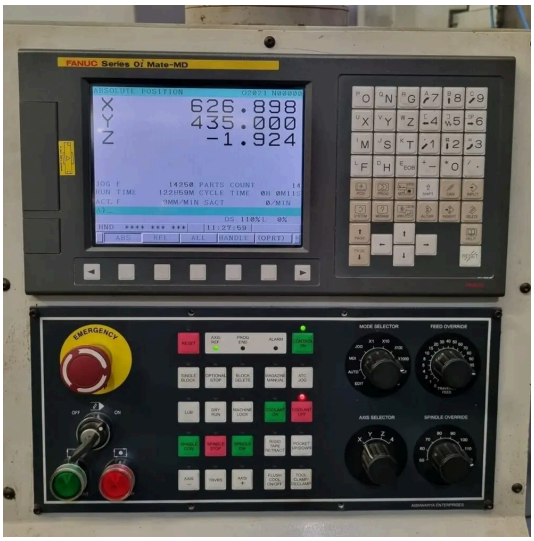



*Figure 1. A Fanuc Series 0i Mate controller. No user accounts. No password prompt. No access control list.*

The problem arises because these controllers process CUI. The G-code and M-code programs that drive a five-axis mill to cut a titanium bracket for a fighter jet nacelle are themselves CUI. They encode geometry, toolpath strategies, feed rates, and surface finish parameters that, taken together, reveal the design intent and manufacturing methodology for controlled defense articles. When that program is loaded into a Fanuc controller's memory and executed, CUI is present on a device that cannot protect it through any conventional IT security mechanism.

This is where many shop owners hit what practitioners call the "technical wall." They look at requirements like IA.L2-3.5.3 (Multi-Factor Authentication) and conclude, correctly, that their CNC equipment cannot implement MFA. They then incorrectly assume one of two things: either that they need to replace the equipment, or that they can simply mark the requirement as "not applicable." Neither conclusion is right.

***Practitioner Note:*** The instinct to declare technical controls "not applicable" on legacy equipment is understandable but dangerous. A C3PAO assessment team will

expect you to demonstrate how CUI is protected on every asset that processes, stores, or transmits it. "The machine can't do it" is not a finding of nonapplicability. It is the beginning of a conversation about compensating controls.

# The Scoping Framework: Specialized Assets and What They Mean for Your Shop

***Before you can solve the problem, you have to scope it correctly.*** The CMMC Assessment Guide defines several categories of assets within an assessment scope, and the one that matters most for legacy manufacturing equipment is the Specialized Asset.

## Defining the Specialized Asset

A Specialized Asset is a device or system that processes, stores, or transmits CUI but is unable to be fully secured due to its operational purpose, technical limitations, or both. CNC controllers, programmable logic controllers (PLCs), coordinate measuring machines (CMMs) with embedded processors, and similar shop floor equipment almost always fall into this category. They handle CUI. They cannot implement the full set of NIST SP 800-171 controls. They are, by definition, specialized.

The critical distinction is that Specialized Assets are not exempt from the assessment. They are in scope. But the CMMC framework acknowledges that these assets will be evaluated differently. Instead of asking whether the controller itself implements MFA or encrypts data at rest, the assessor will ask what compensating controls the organization has implemented around the asset to protect the CUI it handles. The assessment does not require you to do the impossible. It requires you to demonstrate that you have addressed the risk through alternative means.

## The Scoping Boundary Decision

The scoping decision for a manufacturing environment typically involves drawing a boundary around the area where CUI is present in physical or digital form. Inside that boundary, every asset, every person, and every process is subject to the security requirements. Outside it, standard business operations continue without the overhead of CUI handling controls.

For most aerospace machine shops, this boundary will encompass the production floor (or the specific cells and bays where CUI programs are loaded and run), the programming and CAM stations where G-code is generated, the quality inspection area where parts are measured against CUI drawings, and any storage locations where CUI

media or documentation resides. This bounded zone is your Secure Area, and the architecture you build around it is the backbone of your entire compliance posture.

# The Secure Area Architecture

***The Secure Area strategy is built on a simple principle: when the asset cannot protect the data, the environment must.*** This is not a novel concept. Classified environments have operated on this principle for decades. What CMMC requires is a structured, documented, and verifiable implementation of that principle at the CUI level.

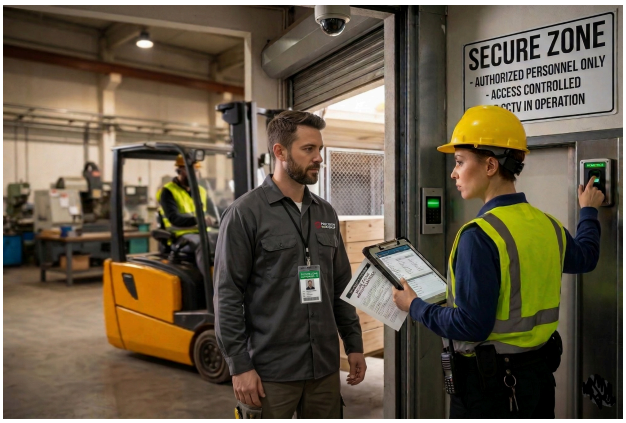
The architecture rests on three interlocking pillars: Physical Protection, Media Protection, and Personnel Controls. Each pillar addresses a specific threat vector, and together they create a compensating control environment that is both operationally practical and defensible under assessment.

## Pillar One: The Physical Protection Perimeter

Physical protection is the foundation. If you cannot control who enters the space where CUI is present, no amount of technical or procedural controls will compensate. The Physical Protection family of controls (PE.L2-3.10.x in NIST SP 800-171) requires organizations to limit physical access to systems, equipment, and operating environments containing CUI, and to protect and monitor the physical facility.

### Access Control Points and the Sentry Protocol

Every Secure Area must have defined and controlled entry points. For a machine shop, this typically means the main personnel door to the production floor and any loading dock or material handling doors. Personnel doors should be secured with electronic access control (badge readers, keypad locks, or both) and should log every entry and exit event with a timestamp and individual identifier.




Loading dock doors present a unique challenge. They must be opened to receive raw material, ship finished parts, and facilitate large equipment moves. They cannot remain locked at all times during operations. The solution is what we call the Sentry Protocol: whenever a loading dock door or bay door is open, a trained CUI-aware employee must be physically stationed at that door. This is not a suggestion. It is the operational implementation of PE.L2-3.10.1, which requires limiting physical access to organizational systems and the facilities in which they are housed to authorized individuals.

The Sentry Protocol requires documentation. The assigned sentry maintains a door log that records the time the door was opened, the reason (material receipt, shipment, ventilation, equipment move), the name of every person who enters or exits through the door while it is open, and the time the door was closed and secured. This log becomes an auditable artifact that demonstrates continuous compliance with the physical access control requirement. It also feeds into your broader monitoring and accountability framework.

***Operational Tip:*** Laminate your door log templates and mount them on clipboards at each dock station. Train your material handlers to treat the log the same way they treat a receiving inspection checklist. It becomes routine within a week.

## Visual Identity Management: The Badge Protocol

In a busy shop environment, the ability to immediately identify who belongs in the Secure Area and who does not is essential. A color-coded badge system provides this at a glance and satisfies the identification requirements embedded across multiple NIST 800-171 control families.

The example system works as follows. Green badges are issued to CUI Handlers: employees who have completed CUI awareness training, signed acknowledgment of handling responsibilities, and are authorized to work with CUI materials, programs, and documentation without escort. Yellow badges identify Non-CUI Staff: employees of the organization who have a legitimate reason to be in the Secure Area (maintenance technicians, janitorial staff during authorized hours, administrative personnel retrieving non-CUI items) but who are not authorized to access CUI and must be accompanied by a Green badge holder while in the zone. Red badges are for Escorted Visitors: any individual who is not an employee of the organization, including customers, vendor representatives, auditors, and equipment service technicians. Red badge holders must be escorted at all times by a Green badge holder, and their visit must be logged.

The visual distinction must be immediately obvious. Do not rely on small colored dots or text on an otherwise identical badge. The badge background color itself should be the indicator, visible from across the shop floor. When a Green badge holder sees a Red badge moving through the shop without an escort, they know immediately that something is wrong and can intervene. This is the "Human Sensor" concept in practice, and it is far more responsive than any camera system.

| **Example Badge Color** | Personnel Category and Access Rules |
|---|---|

| | |
|---|---|
| **Green** | CUI Handler. Full unescorted access to the Secure Area. Trained and authorized to handle CUI materials, G-code, drawings, and traveler sheets. |
| **Yellow** | Non-CUI Staff. Access permitted only when accompanied by a Green badge holder. May not view, handle, or access CUI materials. |
| **Red** | Escorted Visitor. Must be escorted at all times by a Green badge holder. Visit logged with arrival/departure times and purpose. |

## Pillar Two: Media Protection and G-Code Transit

***G-code is the lifeblood of a CNC operation, and in a defense manufacturing context, it is CUI.*** The Media Protection (MP) controls in NIST SP 800-171 address how organizations protect, track, and sanitize media that contains CUI. For machine shops, "media" means the USB drives, compact flash cards, network shares, and any other mechanism used to transfer G-code programs from the CAM workstation to the shop floor controller.

It is worth stating plainly: G-code derived from Department of Defense specifications, technical data packages, or engineering drawings is Controlled Unclassified Information. This isn't an interpretation. The NARA CUI Registry lists Controlled Technical Information (CTI) as a CUI category under the Defense index, governed by DFARS 252.204-7012. CTI is defined as technical information with military or space application that's subject to controls on access, use, reproduction, modification, and dissemination. And under 32 CFR Part 2002, the federal CUI rule, derivative materials inherit the CUI designation of their source. That's the part most shop owners miss. The moment your CAM programmer translates a controlled drawing into a toolpath, that program inherits the CUI marking of its source material. The geometry, the tolerances, the surface finishes, the machining strategies, all of it encodes information that traces directly back to controlled technical data. A G-code file sitting on a USB drive or loaded into a Fanuc controller's memory isn't "just a program." It's CUI, and it has to be protected accordingly throughout its entire lifecycle.

### The Iron Vault Approach: Hardware-Encrypted USB Drives

The most practical and defensible approach to G-code transit in shops without a fully segmented CUI network is the use of FIPS 140-2 (or 140-3) validated, hardware-encrypted USB drives with onboard pin pads. Devices from manufacturers

like Apricorn (Aegis Secure Key) and iStorage (datAshur Pro) meet this standard. These drives require the operator to enter a numeric PIN on the drive's physical keypad before the drive will mount on any system. If the incorrect PIN is entered a preset number of times, the drive performs a crypto-erase, destroying the encryption key and rendering the data unrecoverable.

This approach addresses multiple controls simultaneously. The PIN entry satisfies authentication requirements for access to the media. The FIPS-validated encryption satisfies requirements for protection of CUI on portable media. The crypto-erase capability satisfies sanitization requirements. And the hardware-based nature of the encryption means it works regardless of whether the host device (your Fanuc controller's USB port) has any security capabilities of its own. The encryption lives on the drive, not on the controller.

Standardizing on a single approved drive model simplifies procurement, training, and policy enforcement. Every CUI-containing G-code program moves from the CAM station to the shop floor on an approved Iron Vault drive. No exceptions. No personal thumb drives. No emailed files on unencrypted media. This is a bright line, and enforcing it is straightforward.

## The Media Accountability Log

NIST SP 800-171 control MP.L2-3.8.5 requires organizations to control access to media containing CUI and to maintain accountability for such media during transport outside of controlled areas. For a machine shop, this means every approved USB drive must be individually serialized, assigned to a responsible individual, and tracked.

The Media Accountability Log records the serial number of each approved drive, the individual to whom it is currently assigned, the date and time of each checkout and return, and the content description (typically the job number and program identifier). Drives are stored in a locked cabinet or safe within the Secure Area when not in active use. Inventory is reconciled on a defined schedule, and any drive that cannot be accounted for triggers an incident response procedure.

This level of accountability may feel excessive to shops accustomed to a culture of informal media handling. It is not. A single unencrypted USB drive containing CUI program files, left in a toolbox, lost in a parking lot, or taken home in a pocket, constitutes a potential data spillage event. The Media Accountability Log is the mechanism that prevents "I don't know where it is" from becoming your organization's most expensive sentence.

## Media Sanitization

Control MP.L2-3.8.9 requires organizations to sanitize media containing CUI before disposal or release for reuse. For hardware-encrypted drives, sanitization is accomplished by executing the drive's built-in crypto-erase function, which destroys the encryption key and renders all stored data permanently unrecoverable. For drives that are being decommissioned entirely, physical destruction (shredding or disassembly and destruction of the storage chips) is the definitive method.

The sanitization event must be documented. Record the drive serial number, the sanitization method used, the date, and the name of the individual who performed and verified the sanitization. This documentation becomes part of your compliance evidence and demonstrates that CUI does not persist on media beyond its authorized lifecycle.

# 24/7 Operations: Securing the Unattended Shop Floor

***Aerospace machine shops do not operate on banker's hours.*** High-value CNC equipment, particularly multi-pallet horizontal machining centers like the Matsuura MX-520 or H.Plus-300 and 330 series, are designed for extended unattended operation. A pallet pool loaded on Friday afternoon may run continuously through the weekend, cycling through multiple setups and programs without human intervention. This "lights-out" capability is a significant competitive advantage. It is also a security challenge that must be addressed explicitly in your CMMC implementation.


*Figure 3. Matsuura MX-520 and MX-860 machining centers on a defense production floor.*

## The Surveillance Strategy

Control PE.L2-3.10.2 requires organizations to protect and monitor the physical facility and support infrastructure for organizational systems. During attended hours, your trained workforce (your Human Sensors) provides the primary monitoring function. During unattended operations, video surveillance assumes that role.

Strategic camera placement during lights-out operations requires careful thought. Cameras must be positioned to monitor all access points to the Secure Area: exterior doors, loading docks, and internal doorways from non-CUI areas. They must capture sufficient detail to identify individuals entering or moving through the space. Recording must be continuous or triggered by motion detection, with footage retained for a period defined in your security policy (90 days is a common baseline for the CMMC requirements).

Equally important is where cameras must not be aimed. Camera angles must be deliberately planned to avoid capturing CUI. This means cameras should not face CNC controller screens where G-code parameters or program names may be displayed. They should not be aimed at work surfaces where traveler sheets, inspection reports, or engineering drawings may be present. They should not provide a clear view of CAM workstation monitors. The purpose of the surveillance system is to monitor access and movement, not to create an additional repository of CUI. If your security camera footage captures CUI, then the camera system itself becomes a CUI asset, the recording storage becomes a CUI asset, and anyone with access to the footage requires CUI handling authorization. This is a self-inflicted scoping expansion that serves no one.

***Warning:*** A camera aimed at a CNC controller screen or a work table with traveler sheets creates CUI spillage into the surveillance system. The recording server, the monitoring station, the backup data drives, and every technician with access to the footage all become CUI-scope assets. Angle your cameras toward doors, aisles, and access points. Never toward screens or documents.

## After-Hours Access Control

During unattended operations, access to the Secure Area must be restricted to the absolute minimum number of authorized personnel. This means establishing and enforcing two firm policies.

The first is a No-Guest policy. During hours when the shop floor is operating unattended, no visitors of any kind are permitted in the Secure Area. This includes customer representatives, vendor service technicians, and anyone else who is not a Green-badge CUI Handler. Equipment emergencies that require vendor support during off-hours must follow a documented procedure that includes dispatching an authorized escort to meet the technician, maintaining line-of-sight escort throughout the visit, and logging the event.

The second is a No-Cleaning-Crew policy. Contract cleaning services must not have unsupervised access to the Secure Area at any time, and should ideally be excluded from the Secure Area entirely. Cleaning of the Secure Area should be performed by authorized

personnel (Green badge holders) or by cleaning staff under direct and continuous escort. The scenario of a cleaning crew moving through a manufacturing area after hours, unsupervised, with access to workstations, documents, and potentially unlocked USB drives, is precisely the type of vulnerability that a C3PAO assessment team will probe.

# Personnel and Culture: The Human Element

***Every technical and physical control in this architecture ultimately depends on people.*** The most sophisticated hardware-encrypted USB drive is useless if an operator leaves it plugged into a controller overnight. The best badge system in the world fails if employees do not challenge unescorted Red badges. Physical security is only as strong as the culture that sustains it.

## The Human Sensor

In environments where technology cannot provide automated detection and response, trained human beings become the primary security sensor. This is not a concession. It is a deliberate architectural decision. Your machinists, setup technicians, programmers, and quality inspectors are present on the shop floor every working hour. They know who belongs and who does not. They understand the workflow and can detect anomalies that no camera or access log would flag. A visitor lingering near a CAM workstation. An unfamiliar face in the tool crib. A USB drive sitting on a machine that is not currently running a job. These are the signals that your Human Sensors are trained to detect and act on.

The training investment is modest but critical. Every CUI Handler must understand what CUI is, why it matters, how it flows through your shop, what the approved handling procedures are, and what to do when they observe a deviation. This is not a once-a-year slideshow. It is an ongoing cultural reinforcement that should be embedded in daily operations, shift briefings, and supervisory expectations.

## Personal Device Restrictions

Personal mobile devices with cameras present a direct threat to CUI in a manufacturing environment. A smartphone photograph of a traveler sheet, an engineering drawing, or a CNC controller screen displaying program parameters constitutes unauthorized reproduction of CUI. The simplest and most enforceable policy is to prohibit personal devices with cameras entirely from the Secure Area.

This means establishing a device storage area (lockers or cubbies) outside the Secure Area entrance where employees and visitors deposit their personal phones before entering. Company-issued devices that are required for operational purposes (such as phones used for maintenance coordination or quality documentation) must be explicitly authorized, inventoried, and included in your mobile device management policy. The distinction between personal and company-issued devices must be clear, enforced, and documented.

Will this policy be popular? No. Is it necessary? For any shop that takes CUI protection seriously, the answer is unambiguously yes. The alternative, relying on a policy that says "do not photograph CUI" without removing the capability to do so, is a control that depends entirely on voluntary compliance. In a security architecture, hope is not a control.

## Building the Security Culture

The transition from a typical shop floor culture to a CUI-aware security culture does not happen overnight. It requires visible leadership commitment, consistent enforcement, and a recognition that security procedures exist to protect the business, not to impede it. When a machinist understands that the FIPS-encrypted USB drive protects the contract that pays their salary, the compliance overhead becomes context rather than burden.

Practical culture-building measures include recognizing employees who identify security gaps or suggest procedural improvements, incorporating security performance into supervisory evaluations, conducting periodic tabletop exercises that walk through realistic scenarios ("A vendor arrives to service a machine during second shift. What happens?"), and ensuring that leadership is visibly subject to the same policies as everyone else on the shop floor. If the owner walks through the Secure Area without a badge, the entire program loses credibility.

# Putting It All Together: The Control Mapping

***The Secure Area strategy is not a single control.*** It is an integrated architecture that addresses multiple NIST SP 800-171 requirements through coordinated physical, media, and personnel measures. The following table summarizes how the key components of the architecture map to specific assessment objectives.

| NIST 800-171 Control | Secure Area Component | Implementation Summary |
|---|---|---|
| **PE.L2-3.10.1** | Sentry Protocol, Access Control | Controlled entry points with badge readers; trained sentry at open dock doors with timestamped logs. |
| **PE.L2-3.10.2** | Video Surveillance | Cameras on access points during unattended hours, angled to avoid CUI capture. Footage retained per policy. |
| **PE.L2-3.10.3** | Escort Procedures | Red badge visitors escorted by Green badge holders at all times. Visits logged. |
| **PE.L2-3.10.5** | Device Restriction | Personal devices with cameras prohibited in Secure Area. Storage lockers at entry points. |
| **MP.L2-3.8.1** | Iron Vault USB Drives | FIPS-validated hardware-encrypted USB drives for all G-code transit. No unauthorized media permitted. |
| **MP.L2-3.8.5** | Media Accountability Log | Serialized drives tracked with checkout/return, content descriptions, and periodic inventory reconciliation. |
| **MP.L2-3.8.9** | Sanitization Protocol | Crypto-erase for reuse; physical destruction for decommission. All events documented. |
| **IA.L2-3.5.3** | Compensating Controls | Hardware PIN on USB drives; badge access at zone entry; sentry verification. Documented as compensating for MFA on Specialized Assets. |
| **AT.L2-3.2.1 / AT.L2-3.2.2** | CUI Awareness Training | Role-based training for all CUI Handlers. Annual refresher and onboarding integration. |

This table is illustrative, not exhaustive. A complete System Security Plan will map each of the 110 NIST SP 800-171 controls to specific implementations, policies, and

procedures. The controls listed here represent the areas where the Secure Area architecture provides the most direct and significant compensating coverage for the limitations of legacy manufacturing equipment.

# Conclusion: Compliance Without Capital Destruction

***The CMMC compliance challenge for aerospace machine shops is real, but it is not unsolvable.*** The mistake that too many shop owners make is approaching the problem through the lens of information technology alone. When you look at a Fanuc controller and see a computer that cannot be secured, you see an impasse. When you look at that same controller as a Specialized Asset inside a Secure Area, you see a problem with a proven, documentable, and assessable solution.

The Secure Area strategy does not require you to replace your capital equipment. It does not require exotic technology. It requires disciplined physical controls, rigorous media management, and a workforce that understands its role in protecting the information that keeps your contracts active. It requires documentation that clearly articulates what you are doing, why you are doing it, and how each measure maps to the applicable NIST SP 800-171 requirement.

Legacy CNC equipment built your business. A Secure Area architecture lets you protect that business without dismantling the production capability that earned it. The controls described in this paper are within the reach of any well-run aerospace machine shop. The question is not whether you can do this. It is whether you will do it before the enforcement deadlines make the decision for you.

***About the Author:*** David W. Koran is a CMMC Registered Practitioner and the founder and principal consultant at David Koran & Associates Inc., a CMMC compliance consulting firm serving Defense Industrial Base contractors and their legal counsel. He is an Associate Member of the ABA Section of Public Contract Law.