

Is the G-Code CUI?

*A Content and Authority Method for Scoping Controlled Unclassified
Information in the Aerospace Machine Shop*

CAD/CAM, G-Code, CNC, Additive Manufacturing, Inspection, NDT, and Travelers

David W. Koran

CyberAB Registered Practitioner Advanced

June 2026

1. The Recurring Dispute

A familiar argument repeats across aerospace supply chains and across professional discussion online. A prime contractor sends a machine shop a set of drawings and models marked as Controlled Unclassified Information. The shop opens those files, programs the work, runs the machines, inspects the parts, and records the results. Then a question surfaces that no one in the shop seems able to answer the same way twice. Is the G-code that drives the machine itself Controlled Unclassified Information? What about the toolpath file, the inspection program, the scan data, or the traveler that follows the job across the floor?

Two positions tend to harden. One holds that every file touched during a controlled job is automatically Controlled Unclassified Information because it came from a controlled source. The other holds that G-code is only machine motion, a stream of coordinates and feed rates, and therefore can never be controlled. Each position is stated with confidence, and each fails when measured against the governing authorities.

The correct answer does not come from the file extension, the software that produced the file, the machine that reads it, or whether a banner appears at the top of a page. It comes from two questions asked together. What information does the specific file actually contain, and does an applicable authority require that information to be controlled? Controlled Unclassified Information is determined by the content of a given artifact in a given scenario, not by a blanket rule applied to a file type. This paper sets out the method for answering that question in the shop, applies it directly to G-code, and then carries it through the rest of the manufacturing and quality workflow.

2. The Question Is Content and Authority, Not Format

Controlled Unclassified Information is information that the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, when a law, regulation, or Government-wide policy requires or permits safeguarding or dissemination controls. That definition, set out in the National Archives and Records Administration CUI Glossary and codified at 32 CFR 2002.4(h), ties the determination to the nature of the information and to an applicable controlling authority.¹

Several consequences follow directly from that definition. A file extension, a software product, a storage medium, a network location, or the absence of a visible marking does not by itself decide whether information is controlled. A posted program saved as plain

¹[32 CFR 2002.4\(h\)](#); see also the National Archives [CUI Glossary](#).

text is not exempt because of its extension, and a model is not controlled simply because it sits inside an enclave. Status attaches to the information, and the determination rests on the applicable authority.

The same authorities address what happens when a shop creates something new from a controlled source. The National Archives defines re-use as incorporating, restating, or paraphrasing Controlled Unclassified Information from its originally designated form into a newly created document, and it reads the word document broadly enough to include electronic files, computer data, printouts, worksheets, images, metadata, and other data compilations. A new file built from a controlled drawing is therefore squarely within the re-use concept when it carries the controlled content forward.²

Department of Defense Instruction 5200.48 reinforces this from the derivative side. A new derivative document or material must be treated and marked as Controlled Unclassified Information when the information in it qualifies. At the same time, source lineage alone does not automatically make every derivative item controlled. The derivative information must be reviewed on its own terms.³ The same instruction makes clear that information can qualify even when a contractor generates it, and it requires the contract or other legal agreement to articulate the protective measures and dissemination controls that apply.⁴

Two further points bound the analysis. Under the definitions at Defense Federal Acquisition Regulation Supplement clause 252.204-7012(a), covered defense information includes qualifying information that is marked or otherwise identified in the contract and provided by or on behalf of the Department of Defense, and qualifying information that a contractor collects, develops, receives, transmits, uses, or stores in support of contract performance.⁵ And over-designation cuts the other way. Marking information as controlled when no authority requires it is itself a misuse of the program.⁶ The correct method is neither everything related to a controlled job is controlled nor nothing the shop makes is controlled. It is a content and authority determination applied artifact by artifact.

²National Archives [CUI Glossary](#), definition of re-use.

³[DoD Instruction 5200.48](#), Section 3.2 (legacy and derivative information reviewed for CUI when used in a new document).

⁴[DoD Instruction 5200.48](#), Section 5.3 (protective measures and dissemination controls articulated in the contract or other legal agreement).

⁵[DFARS 252.204-7012\(a\)](#), definition of covered defense information.

⁶[32 CFR 2002.4\(ee\)](#) (misuse of CUI includes designating or marking information as CUI when it does not qualify); [DoD Instruction 5200.48](#) (information will not be designated CUI to conceal a violation of law, prevent embarrassment, or restrain competition).

3. Controlled Technical Information, a Category Frequently Implicated

In aerospace and space manufacturing, a Controlled Unclassified Information category frequently implicated is Controlled Technical Information. The exact category must always be verified from the contract and the markings, and Export Controlled Information may apply as a separate category that has to be confirmed rather than assumed. With that caution stated, the Controlled Technical Information category fits much of what a machine shop handles.

The Department of Defense defines Controlled Technical Information as technical information with military or space application that is subject to controls on access, use, reproduction, modification, performance, display, release, disclosure, or dissemination, and that is not lawfully publicly available without restriction. The category expressly includes blueprints, drawings, plans, instructions, computer software, and documentation that can be used or adapted to design, engineer, produce, manufacture, operate, repair, overhaul, or reproduce military or space equipment or related technology.⁷

The Defense Federal Acquisition Regulation Supplement gives concrete examples of technical information, including process sheets, data sets, engineering drawings, specifications, executable code, source code, studies, and analyses. The same body of regulation, in clause 252.227-7013(a), defines a computer program as a set of recorded instructions, rules, or routines capable of causing a computer to perform a specific operation or series of operations, and it defines detailed manufacturing or process data as technical data that describes the steps, sequences, and conditions of manufacturing, processing, or assembly.⁸

These data-rights definitions help establish whether an artifact is technical data or computer software. They do not by themselves make an artifact Controlled Unclassified Information. To be controlled, the artifact must also satisfy the applicable Controlled Technical Information category, a safeguarding authority, and the contractual facts. The data-rights framework and the Controlled Unclassified Information framework answer different questions, and a defensible determination keeps them separate.

Read together, these definitions create a credible basis for treating machine-readable manufacturing instructions and part-specific process records as Controlled Technical Information when they reveal controlled military or space design, manufacturing,

⁷[DFARS 252.204-7012\(a\)](#), definition of controlled technical information; DoD CUI Program, [Controlled Technical Information](#).

⁸[DFARS 252.227-7013\(a\)](#) (computer program; detailed manufacturing or process data); [DFARS 252.204-7012\(a\)](#) (technical information examples).

inspection, or test information. They do not establish that every G-code file, inspection record, or traveler is automatically Controlled Technical Information. They establish the test that decides the question.

4. The Aerospace Shop Fact Pattern

The analysis in this paper rests on a specific and common fact pattern, stated here so that every conclusion can be measured against it.

- A Department of Defense prime contractor, or a higher-tier contractor, provides aerospace drawings, plans, specifications, models, or technical data to a subcontract machine shop.
- That source material is marked as Controlled Unclassified Information and is identified or documented as controlled in the prime contract or subcontract.
- The shop uses the source material to perform defense-contract work and to create downstream manufacturing and quality artifacts.
- The workflow runs through computer-aided design and manufacturing software, computer numerical control machines, additive or three-dimensional printing systems, inspection and metrology equipment, nondestructive testing equipment, and paper or electronic traveler sheets.
- No written decontrol decision and no written contract-specific determination excludes the downstream artifacts from controlled treatment.

Where the source plans are marked and contractually identified as controlled, the shop is not starting from a blank slate. It is starting from a known authority and a known body of controlled content, and the task is to determine which downstream artifacts carry that content forward.

5. The Core Test

The method reduces to a single operating statement. A downstream manufacturing file is not automatically Controlled Unclassified Information because it came from controlled information, and it remains or becomes controlled when it carries forward information that qualifies under the applicable authority.

In the stated fact pattern, the qualifying content is usually concrete and recognizable. It includes controlled geometry, dimensions, tolerances, materials, manufacturing sequences, tooling logic, special-process instructions, acceptance criteria, inspection characteristics, internal structure, defect locations, and other part-specific technical details drawn from the marked source. When an artifact contains or exposes that kind of

content, it falls within the controlled category. When it contains only generic, public, or administrative content, it does not, regardless of the job it supports.

The conservative operating position follows from the test rather than from caution alone. When an artifact reasonably appears to carry forward Controlled Unclassified Information, the shop should segregate and safeguard it at the applicable baseline while it seeks written clarification. Safeguarding in this way is an operational decision, and it is distinct from formal designation and marking, which follow the contract, agency policy, and any authority the contractor holds as an authorized holder.⁹ Marking information that does not qualify is itself a misuse of the program. Ambiguous artifacts should be elevated to the prime, the information originator, or the Government contracting activity rather than resolved by assumption on the shop floor.

6. The G-Code Question, Answered Directly

Apply the test to the file at the center of the dispute. A posted numerical control program, the G-code, is not Controlled Unclassified Information because it carries an NC, TAP, TXT, or similar extension, and it is not controlled because a particular toolpath system or slicer produced it. By the same logic, it is not exempt because a controller reads it as a stream of motion commands. None of those facts speaks to content or authority.

The defensible basis is the controlled content carried into the output and the use of that output in performing the defense contract. A posted program should be treated as Controlled Unclassified Information when it encodes controlled geometry, coordinates, toolpaths, drilling patterns, machining sequences, special operations, or other technical instructions that can be used to manufacture the controlled part. Those are the same characteristics that place process sheets and detailed manufacturing data within the Controlled Technical Information category. A program that reproduces the controlled geometry of a part in machine-readable form is a manufacturing instruction for that part, and its format does not change what it contains.

The opposite case is equally clear. A generic post-processor, a generic machine definition, a generic tool library, a blank template, a standard canned cycle, or a public training example is not controlled merely because the same system also processes controlled work. Such files become a concern only when part-specific controlled information is embedded in them. The proximity of a generic file to a controlled job does not transform the generic file.

⁹[DoD Instruction 5200.48](#), Section 3.6(a) (the authorized holder determines at creation whether information is CUI and applies the markings).

This resolves the dispute by rejecting both overbroad claims. The statement that all G-code is controlled is wrong because it ignores the many programs and components that carry no controlled content. The statement that G-code is never controlled is wrong because it ignores the encoded geometry and manufacturing instructions that often qualify as Controlled Technical Information. The file type does not answer the question. The content does.

7. Walking the Shop, Artifact by Artifact

The same test applies at every station in the shop. What follows is the practical application across the workflow described in the fact pattern. The treatments below reflect the stated fact pattern and remain content, authority, and contract specific in any given case.

7.1 Computer-Aided Design and Manufacturing

Opening or importing a marked controlled drawing, a STEP file, a solid model, a technical data package, or a specification causes the design and manufacturing workstation and its associated storage to process controlled information, independent of the final status of the posted program. Native project files, toolpath files, simulation files, stock and fixture models, setup files, posted intermediate files, and autosave or recovery files should be treated as controlled when they contain controlled geometry, dimensions, tolerances, operations, or process details. Screenshots, thumbnails, simulation videos, printouts, and setup sheets can be controlled when they expose the geometry or the manufacturing process, even when the underlying project file never leaves the enclave. Temporary folders, local caches, spool files, cloud-sync folders, crash dumps, and backups belong in the same review, because each can hold a controlled artifact.

7.2 Computer Numerical Control and Machine Transfer

The method of transfer does not change the status of the information. Moving a program by direct numerical control server, network share, serial link, removable drive, memory card, or manual entry leaves its controlled status intact. A controller processes controlled information when it executes or displays a controlled program, it stores controlled information when the program remains in controller memory or local storage, and it transmits controlled information when it sends the program, a backup, a remote display, or job data to another asset.

The air-gap belief deserves direct correction. An air-gapped machine is not automatically outside the scope of an assessment. Physical separation may reduce the pathways into and out of the asset, but an asset that actually processes or stores controlled information is not an out-of-scope asset under the Level 2 definitions.

Machine history, job lists, operator notes, alarms, and production logs are not automatically controlled, and they should be treated as controlled when they reproduce controlled part numbers, geometry, operations, program content, or parameters.

7.3 Additive Manufacturing

A marked controlled model remains controlled when it is imported into build-preparation or slicing software. Derived STL, 3MF, and AMF files, build-preparation projects, support and orientation files, slice and layer files, printer programs, and machine job packages should be treated as controlled when they preserve or reveal controlled geometry or part-specific build instructions. Part-specific build parameters can themselves be controlled when they reveal controlled materials, layer or scan strategy, energy settings, support design, thermal management, or heat treatment tied to the controlled part. Generic material profiles, standard machine parameters, publicly available slicing profiles, and blank build templates are not controlled unless part-specific controlled information is combined into them.

7.4 Inspection and Metrology

Inspection workstations process controlled information when marked drawings, models, specifications, or technical data packages are loaded to create inspection plans or programs. Part-specific coordinate measuring machine and dimensional measuring interface programs should be treated as controlled when probe paths, nominal values, tolerances, datum structures, feature definitions, or acceptance logic carry forward controlled content. Ballooned drawings, inspection plans, first article inspection reports, full dimensional reports, and nonconformance reports can be controlled when they reproduce controlled dimensions, tolerances, geometry, materials, or acceptance criteria. Laser scans, structured-light scans, point clouds, mesh files, deviation maps, and metrology images should be treated as controlled when they reveal controlled geometry. Inspection results can be controlled even though the shop generated them, because contractor-generated information qualifies when it is created or possessed on behalf of the Government and carries controlled technical content. A minimal record that states only pass, fail, or inspection complete may not be controlled, although it can still be Federal Contract Information or restricted for other reasons.

A scenario observed during recent scoping work shows how an instrument that looks minor can place controlled information in motion. A shop measured a machined part at the CNC using a wireless caliper paired by Bluetooth to a laptop, and the measurement application on the laptop displayed a picture of the part with the inspection points mapped onto it. A single dimension read from a caliper, taken alone, is one value. The display on the laptop is a different matter, because it reproduces the controlled geometry of the part and the layout of the controlled inspection characteristics, which is the same kind of content that places a ballooned drawing or an inspection plan within

the controlled category. The laptop processes and stores that content, which makes it a CUI Asset, and the wireless link between the caliper and the laptop is a transmission pathway that belongs in the data-flow review. The method of transfer, whether wired or wireless, does not change the status of the information, although a wireless pathway carries its own access and protection requirements. The caliper itself transmits a measurement value, and its treatment depends on what it actually processes, stores, or transmits, while the more significant asset in this scenario is the laptop and the application that renders the part and its measurement points.

7.5 Nondestructive Testing

Nondestructive testing workstations and instruments process controlled information when controlled drawings, models, weld maps, material specifications, defect criteria, or part-specific scan plans are loaded or referenced. Part-specific technique sheets, scan plans, inspection zones, transducer paths, exposure layouts, and calibration setups should be treated as controlled when they reveal controlled geometry, materials, internal structure, critical areas, or engineering requirements. Digital and computed radiography images, computed tomography volumes and reconstructed slices, ultrasonic scans, phased-array files, eddy-current maps, and related datasets can be controlled when they reveal controlled design or technical characteristics. A generic procedure based only on a public consensus standard is not controlled merely because the shop uses it, while a job-specific technique developed from a controlled drawing or specification may be controlled. Export controls and customer-specific requirements can apply in addition to the CUI analysis.

7.6 Travelers and Shop-Floor Work Instructions

A traveler is not automatically controlled because it is associated with a controlled job. It should be treated as controlled when it incorporates or restates controlled operation sequences, dimensions, tolerances, material specifications, special processes, heat-treatment or coating requirements, weld requirements, machining instructions, inspection characteristics, nondestructive testing requirements, or acceptance criteria. A traveler can also carry controlled content through embedded excerpts, thumbnails, ballooned drawings, controlled drawing numbers and revisions, links or codes that expose controlled material, or detailed operator notes. A basic routing record that contains only an internal job number, quantity, generic operation names, dates, and status may not be controlled, although part identity, aggregation, and customer direction still matter. A completed traveler can remain controlled after production, because actual process values, inspection results, testing findings, and nonconformance dispositions may add controlled technical information. Printed travelers that contain controlled information are physical media, and printing, staging, posting, annotating, scanning, copying, archiving, and destroying them all belong to the controlled handling workflow.

Treatment Matrix for the Stated Fact Pattern

The matrix below states the default treatment for each artifact under the stated fact pattern. The final determination remains content, authority, and contract specific.

Artifact	Default treatment	Basis or boundary
Source marked drawing, model, or specification	Controlled	Already marked and identified in the contractual chain.
Native project and toolpath file	Controlled when part-specific	Usually carries controlled geometry and manufacturing instructions.
Posted G-code or NC program	Controlled when it encodes controlled content	Machine-readable geometry, paths, and sequences can qualify as Controlled Technical Information.
Generic post-processor, tool library, or template	Not necessarily controlled	Generic or public content is not converted by system proximity.
Setup sheet or work instruction	Controlled when detailed	May restate controlled process, dimensions, tooling, or special operations.
STL, 3MF, slice, or build file	Controlled when derived content is preserved	Can reproduce geometry or part-specific build strategy.
CMM or DMIS program	Controlled when part-specific	Can encode nominal geometry, tolerance, datum, and inspection logic.
Ballooned drawing, FAI, or dimensional report	Controlled when controlled details appear	May reproduce source drawing data and acceptance criteria.
Point cloud, scan, or deviation map	Controlled when geometry is revealed	Can recreate or characterize the controlled part.
Measurement display showing part image and measure points	Controlled when it reveals geometry or characteristics	Reproduces controlled geometry and the inspection characteristic layout.
NDT technique or scan plan	Controlled when controlled details appear	May expose internal structure, materials, or critical zones.
NDT image, data, or report	Controlled when technical content is controlled	May reveal controlled geometry, defects, or engineering limits.
Detailed traveler or router	Controlled when it reuses controlled technical information	Process sheets are an express technical-information example in the regulation.
Minimal status-only traveler or log	Not necessarily controlled	May remain Federal Contract Information or restricted for other reasons.

Artifact	Default treatment	Basis or boundary
Calibration certificate or maintenance log	Not necessarily controlled	Normally generic unless it includes controlled part or process data.
Printout or scan of any controlled artifact	Controlled	Format conversion does not remove the underlying status.
Backup or archive of a controlled artifact	Controlled	A copy retains the status of the information it contains.

8. From CUI Determination to CMMC Scoping

Two distinct questions are often run together, and separating them removes most of the confusion. The first question is a CUI determination question. What information is Controlled Unclassified Information? The second is a scoping question. Which assets process, store, transmit, or protect that information? The determination comes first, because the scoping analysis depends on knowing what content needs protection.

Cybersecurity Maturity Model Certification Level 2 scoping is driven by the assets that process, store, or transmit controlled information and by the assets that provide security protection for the assessed environment. The regulation reads process, store, or transmit broadly. It includes accessing, entering, editing, generating, manipulating, or printing data, retaining data at rest in electronic memory or on paper, and transferring data by physical or digital means. A Level 2 assessment evaluates the in-scope environment against the one hundred ten security requirements of National Institute of Standards and Technology Special Publication 800-171, Revision 2.¹⁰

The asset categories under 32 CFR 170.19(c)(1), Table 3, carry different treatments, and the distinction matters for the shop floor.¹¹ A CUI Asset processes, stores, or transmits controlled information and is assessed against all applicable Level 2 requirements, and it must appear in the asset inventory, the system security plan, and the network diagram. A Specialized Asset can process, store, or transmit controlled information but cannot be fully secured, and its categories include operational technology and test equipment. A Specialized Asset remains in scope at Level 2. It must be inventoried and documented in the system security plan and network diagram and managed under risk-based policies, and the assessor reviews the plan without assessing the Specialized Asset against every other requirement. Computer numerical control machines, additive

¹⁰32 CFR 170.14(c)(3) (incorporating [NIST SP 800-171, Revision 2](#), the 110 security requirements assessed at Level 2).

¹¹32 CFR 170.19(c)(1), [Table 3](#) (CMMC Level 2 asset categories and associated requirements).

systems, coordinate measuring machines, and nondestructive testing systems may qualify for this category. They are inside the Level 2 scope, not outside it.

A Contractor Risk Managed Asset can process, store, or transmit controlled information but is not intended to do so because policies and practices prevent that use. It remains in scope and must be documented, and the assessor may perform a limited check where the evidence raises a question. An Out-of-Scope Asset cannot process, store, or transmit controlled information and provides no protection for CUI Assets, or is separated so that it cannot do so. An asset that actually receives controlled information cannot be moved out of scope by the wording of a policy alone. Finally, a Third Party Assessment Organization evaluates the organization against Cybersecurity Maturity Model Certification requirements. It does not replace the Government information owner, the designating authority, the contracting officer, or the contractual chain that resolves the underlying CUI determination.

Likely Asset Categorization for the Stated Workflow

The categorizations below reflect the stated workflow rather than a universal rule, and each should be validated against the actual implementation.

Asset	Likely CMMC treatment	Fact-specific basis
Design and manufacturing workstation	CUI Asset	Loads marked controlled models and creates derivative technical files.
Engineering file server, PDM, or PLM	CUI Asset	Stores source and derivative design and manufacturing files.
Direct numerical control or transfer server	CUI Asset	Stores or transmits controlled NC programs.
Removable media holding NC or build files	CUI Asset (removable media)	Stores and physically transfers CUI.
Networked CNC controller	CUI Asset or Specialized Asset	Processes and stores controlled information; Specialized Asset only if it cannot be fully secured per the defined criteria.
Air-gapped CNC controller	Specialized Asset or CUI Asset	Still processes and stores controlled information; the air gap does not remove it from scope.
Additive build-preparation workstation	CUI Asset	Processes marked models and creates controlled build artifacts.

Asset	Likely CMMC treatment	Fact-specific basis
Three-dimensional printer or additive controller	CUI Asset or Specialized Asset	Executes and stores controlled build files; Specialized Asset only if it cannot be fully secured per the defined criteria.
CMM programming workstation	CUI Asset	Processes source content and part-specific inspection programs and results.
CMM controller	CUI Asset or Specialized Asset	Processes and stores part-specific controlled inspection data.
Laptop displaying part image and measure points	CUI Asset	Renders controlled part geometry and the inspection characteristic layout.
Wireless (Bluetooth) caliper	Fact-dependent; wireless pathway in scope	Treatment depends on what it transmits; an isolated dimension may not be controlled, while the paired display is.
NDT workstation and viewer	CUI Asset	Processes and stores controlled scan plans, images, and reports.
NDT instrument or radiography system	CUI Asset or Specialized Asset	Processes and stores controlled data and may not meet all standard controls.
ERP, MES, or QMS with detailed travelers	CUI Asset	Stores controlled process, inspection, testing, or acceptance information.
Shop-floor terminal showing detailed travelers	CUI Asset	Displays controlled traveler content; a terminal barred from CUI by policy would be a Contractor Risk Managed Asset.
Printer, scanner, or MFP used for controlled travelers	CUI Asset	Prints, scans, and may spool or store CUI, unless it meets another defined category.
Office endpoint barred from controlled work	Contractor Risk Managed or Out-of-Scope Asset	Depends on technical separation and on whether it can process controlled information.

9. What Is Not Automatically Controlled

The method protects the shop in both directions. Just as it identifies the artifacts that carry controlled content forward, it identifies the artifacts that do not. Generic tools,

blank templates, public consensus standards, generic machine parameters, and publicly available profiles are not controlled simply because they are used near controlled work. Status-only routing records and logs that disclose no controlled technical detail are not controlled on their content alone. Calibration certificates and equipment-maintenance records are normally generic unless they include controlled part or process information. An individual data point such as a drawing number, a revision level, a part number, or a single isolated measurement is not automatically Controlled Unclassified Information. What the information reveals and its context determine the result, because a set of data points assembled together can reveal controlled technical information that no single value would. A distinct concern is compilation that raises the classification level. Contracts require contractors to monitor whether aggregated or compiled information could become classified, a question governed by security classification guidance rather than by the Controlled Unclassified Information analysis.¹²

Two cautions keep this from being read too far. Over-designation is a recognized misuse of the program, so labeling generic material as controlled is not a safe default. It carries its own cost and its own risk. At the same time, a finding that an artifact is not Controlled Unclassified Information does not mean the artifact is unrestricted. Federal Contract Information, export controls, proprietary restrictions, quality-system retention rules, and contract clauses can each apply on their own terms. Removing a banner, renaming a file, or applying encryption does not decontrol information that otherwise qualifies.

10. Evidence the Shop Should Maintain

A determination is only as defensible as the record behind it. The following materials support both the CUI determinations and the scoping decisions, and they give an assessor or a prime a clear basis for review.

- The subcontract, the security requirements, the CUI clauses, the data markings, the distribution statements, and any CUI guidance the prime provided.
- A data-flow map that runs from receipt of the source material through engineering, programming, machine transfer, production, inspection, testing, traveler completion, delivery, retention, backup, and destruction.
- An artifact register that records which file types and records contain controlled information, which do not, the basis for each determination, and the approving authority.

¹²[DoD Instruction 5200.48, Section 5.3\(c\)](#) (contracts require contractors to monitor aggregated or compiled CUI for potential classification under security classification guidance).

- An asset inventory and network diagram that include CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and relevant external providers.
- System security plan descriptions and risk-based policies for the machines, additive systems, measuring machines, and testing equipment treated as Specialized Assets.
- Removable-media procedures, transfer-station controls, physical handling rules for printed travelers and reports, marking practices, retention schedules, and destruction methods.
- Written clarification requests and the responses received from the prime, the information originator, or the Government contracting activity for any disputed or ambiguous artifact.

11. Resolving Disputes the Right Way

When an artifact sits on the line, the resolution does not belong to the loudest voice in a comment thread or to the assessor in the room. Unresolved, contract-specific questions should be directed to the prime, the information originator, or the Government contracting activity, and the answer should be obtained in writing. This escalation aligns with the contract itself. Defense Federal Acquisition Regulation Supplement clause 252.204-7012(m)(1) requires the prime or higher-tier contractor to determine whether the information needed for subcontract performance retains its identity as covered defense information and, if necessary, to consult the Contracting Officer, which places the determination with the party that holds the contractual authority to make it.¹³ The assessment organization evaluates compliance with the certification requirements. It does not designate Controlled Unclassified Information, and it does not resolve the underlying CUI status of a given file.

Authority also belongs at the center of the public debate. Official Government sources are the controlling authorities here, including the National Archives CUI Glossary, the Department of Defense CUI program, Defense Federal Acquisition Regulation Supplement clauses 252.204-7012 and 252.227-7013, Department of Defense Instruction 5200.48, 32 CFR part 2002, and 32 CFR part 170. Industry commentary and assessor experience can illustrate how the rules play out in practice, and that experience has real value, but it does not control the determination. When a position is challenged, the strongest answer cites the authority and applies it to the specific content of the specific file.

¹³[DFARS 252.204-7012\(m\)\(1\)](#) (the prime or higher-tier contractor determines whether subcontract information remains covered defense information and, as needed, consults the Contracting Officer).

12. Position Statement

In an aerospace subcontractor environment where the prime has marked and contractually identified the source plans as Controlled Unclassified Information, the shop must evaluate each downstream manufacturing and quality artifact by its content and by the applicable authority. Design and manufacturing files, G-code, additive build files, coordinate measuring machine programs, inspection reports, nondestructive testing records, and traveler sheets are likely to remain or become controlled when they incorporate, restate, encode, reveal, or operationalize controlled technical information from the plans. Generic files and status-only records are not automatically controlled. Every asset that actually processes, stores, transmits, or protects the resulting controlled information belongs in the Cybersecurity Maturity Model Certification Level 2 scoping analysis. Machines, additive systems, measuring machines, and testing systems may qualify as Specialized Assets, and Specialized Assets are inside the Level 2 scope, not outside it.

The dispute that opens this paper dissolves once the right question is asked. The file extension does not decide it, the software does not decide it, and the lineage alone does not decide it. The content of the artifact and the authority that controls it decide it, one artifact at a time.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced who advises Defense Industrial Base contractors and government contracts attorneys on Cybersecurity Maturity Model Certification Level 2 readiness, enablement, and implementation. He is an Associate Member of the American Bar Association Section of Public Contract Law and the author of The CMMC Decision, Second Edition.

His work draws on more than thirty years in information technology and cybersecurity, including aerospace cybersecurity and the deployment of enterprise resource planning and manufacturing systems on the shop floor.

He can be reached at dkoran@davidkoran.com and (802) 335-2662.

References

[National Archives and Records Administration, Controlled Unclassified Information Glossary](#)

[National Archives and Records Administration, Controlled Unclassified Information Frequently Asked Questions](#)

[32 CFR 2002.4, Controlled Unclassified Information, Definitions](#)

[Department of Defense CUI Program, Controlled Technical Information Category](#)

[Defense Federal Acquisition Regulation Supplement 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting](#)

[Defense Federal Acquisition Regulation Supplement 252.227-7013, Rights in Technical Data, Other Than Commercial Products and Commercial Services](#)

[Department of Defense Instruction 5200.48, Controlled Unclassified Information](#)

[32 CFR 170.4, CMMC Acronyms and Definitions](#)

[32 CFR 170.14, CMMC Model](#)

[32 CFR 170.19, CMMC Scoping](#)

[Department of Defense Chief Information Officer, CMMC Scoping Guide Level 2, Version 2.13, September 2024](#)

[National Institute of Standards and Technology Special Publication 800-171, Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations](#)