Operationalizing Change Management Under CMMC

FAQ F-Q5 in Practice

David W. Koran

CyberAB Registered Practitioner Advanced

May 2026

Summary

The Department of War added new guidance on April 29, 2026 that materially affects how defense contractors should manage changes to systems within a CMMC environment. The guidance is identified as F-Q5 in the latest revision of the CMMC Frequently Asked Questions. F-Q5 does not introduce new technology, new tools, or new security controls. It introduces a documented procedure that the organization should follow whenever it makes a change that could affect cybersecurity posture or the handling of Controlled Unclassified Information.

The procedure runs in three phases. Before any meaningful change to the environment, a written analysis should explain how the change affects security and how it affects the flow of CUI. Before the change proceeds, the individual who signs the organization's annual cybersecurity attestation should review and approve the analysis. During the change, a working record should document any temporary risks that exist while the work proceeds. After the change is complete, the System Security Plan should be updated, and the same individual who signed the original attestation should review the update before the next attestation cycle.

Two business consequences follow from the guidance. The first is that the individual signing the annual attestation now bears responsibility for a continuous record that an assessor can audit. The False Claims Act can create organizational and, in some circumstances, individual exposure when cybersecurity attestations are knowingly false or unsupported by the facts, and a signed attestation without the underlying records to back it up is the precise scenario that the Department of Justice has pursued under the Civil Cyber Fraud Initiative since 2021. The second is that operational pressure to move quickly on changes now collides with a procedural workflow that takes time. Building the procedure into normal change management is sustainable across the volume of changes any active business generates, while handling each change as a one-off compliance exercise produces gaps that accumulate over time and become visible during assessment.

Three leadership questions follow from F-Q5. The first concerns the individual who will sign the annual attestation and whether that person has the authority to enforce the procedure when operational pressure pushes against it. The second concerns whether the change management process extends through every external IT and security provider the organization uses, or whether it stops at the company perimeter. The third concerns timing, specifically whether the procedural artifacts are being created today while self-assessment is still the standard, or whether the organization is planning to build them under the time pressure of the third-party assessment cycle that begins in

November 2026. The cost of building the procedure now is low compared to the cost of building it under the time pressure of a third-party assessment.

The procedural detail in the remainder of this paper is written for the compliance lead, the IT manager, and the individual who signs the attestation. The executive view above is sufficient for the decisions that leadership owns.

Introduction

The Office of the Chief Information Officer at the Department of War released Revision 2.3 of the CMMC Program Frequently Asked Questions on April 29, 2026. The release added three new entries, restructured scoping content into a dedicated section, clarified the treatment of encrypted CUI under sanitation procedures, and updated several program contact references. Among the new entries, F-Q5 carries the broadest operational implications. It establishes a documented workflow for managing changes within a CMMC environment, converting a cluster of related controls into a single procedural sequence that the program office now expects organizations to follow.

This paper examines F-Q5 in detail. It maps the controls cited in the FAQ, walks through the three implementation phases, identifies the Affirming Official role at each step, and provides sample artifacts that satisfy the documentation expectations. The paper also addresses External Service Provider relationships, the test for significant change, and how the workflow interacts with continuous monitoring obligations under the CMMC Program.

The Problem F-Q5 Addresses

Before Revision 2.3, the controls that govern change within a CMMC environment lived in separate domains and read as separate obligations. CM.L2-3.4.3 sat in Configuration Management. AC.L2-3.1.3 sat in Access Control. CA.L2-3.12.2, CA.L2-3.12.3, and CA.L2-3.12.4 sat in Security Assessment. RA.L2-3.11.1 sat in Risk Assessment. An organization could implement each control in isolation and still leave gaps in how change moved through the environment.

The gaps showed up consistently in self-assessment findings during Phase 1 of CMMC implementation. Changes occurred without security impact analysis. Analyses occurred without entries in the change management system. Change management entries existed without corresponding SSP updates. SSP updates happened without Affirming Official review. Each gap was traceable to a specific control failure, but the underlying problem was that the controls did not describe a sequence.

F-Q5 supplies the sequence. It defines three phases, names the controls that govern each phase, and places the Affirming Official inside the workflow rather than at the perimeter. The result is a procedure that assessors can audit against and that organizations can train against.

The Five Controls in Sequence

F-Q5 names five controls that operate in sequence across the three phases of a change. The table below maps each control to its phase and purpose.

Phase	Control	Purpose
Before	CM.L2-3.4.4	Security impact analysis for the proposed change
Before	AC.L2-3.1.3	Analysis of effects on CUI flow
Before	CM.L2-3.4.3	Documentation of the change in the formal change management process
During	CA.L2-3.12.2	Operational Plan of Action describing the change and any temporary risks
After	CA.L2-3.12.4	System Security Plan update reflecting the completed change

Two additional controls referenced in C-Q12 are not part of the F-Q5 sequence. CA.L2-3.12.3 governs continuous monitoring and operates on its own schedule. RA.L2-3.11.1 governs risk assessments and runs at intervals defined by the organization. Both controls remain relevant to overall compliance posture but are not triggered by individual changes.

The Significant Change Test

Before walking through the three phases of the workflow, it is useful to address the threshold question of which changes warrant the full procedure. The interaction between F-Q5 and C-Q12 produces a workable test. C-Q12 provides three categories. Changes that clearly require reassessment, such as activating a capability that was previously assessed as Not Applicable. Changes that do not require reassessment, such as routine patching or replacing a security solution with one of equal or better capability. Changes that require careful evaluation, such as merging environments or removing support for a security requirement.

F-Q5 supplies the operative practitioner test for the third category. If the security impact analysis identifies a new risk that is not addressed in the existing SSP, the change is probably significant. This shifts the determination from a subjective judgment to a documentary one. The SSP either contemplates the risk or it does not. The contents of the SSP at the time of the change become the reference point.

Two practical consequences follow. The first is that the SSP now functions as the contractor record of risks accepted, deferred, or mitigated. A thin SSP makes the significant change determination harder because the universe of contemplated risks is smaller. The second is that the Affirming Official has a defensible position when declining to invoke significant change. The position rests on the SSP rather than on judgment alone.

The procedure described in the next three sections applies broadly to changes that may affect FCI, CUI, security requirements, or assessment scope. The significant change test determines whether a change crosses the additional threshold that may require reassessment under C-Q12. Most changes will not cross that threshold. The procedure still applies.

Phase One: Before Implementation

Phase one begins when a change is proposed and ends when the Affirming Official approves the analysis. Four actions occur in this phase, in order, each with a specific evidentiary requirement.

Security Impact Analysis under CM.L2-3.4.4

The security impact analysis examines whether the proposed change introduces new risk that is not already addressed in the System Security Plan. The analysis is a written record. It identifies the change, the affected assets, the controls that depend on those assets, and any new risk vectors that result from the change.

The FAQ contains a parenthetical that practitioners should treat as the operative test: if the security impact analysis identifies a new risk that is not addressed in the existing SSP, the change is probably significant. That sentence gives the Affirming Official a defensible internal standard. Risks contemplated by the SSP are operational events that proceed through normal change management. Risks not contemplated by the SSP are architectural events that may require reassessment under C-Q12.

The sample worksheet below illustrates a structure that captures the required analysis. Field labels are constant. Sample content is shown for a hypothetical change involving the addition of a network connected coordinate measuring machine to a small CNC machine shop.

Analysis Identifier	SIA-2026-007

Date of Analysis	May 12, 2026
Analyst	Jane Smith, IT Manager
Change Description	Install one network connected Mitutoyo Crysta-Apex coordinate measuring machine in the inspection area. Connect to the production VLAN to receive measurement programs from the CAD/CAM workstation.
Affected Assets	New CMM endpoint. Production VLAN segment. CAD/CAM workstation. Inspection area network drop.
Controls That Depend on These Assets	AC.L2-3.1.1, AC.L2-3.1.2, CM.L2-3.4.1, SC.L2-3.13.1, SC.L2-3.13.5, SI.L2-3.14.2
Existing SSP Treatment	Production VLAN is documented as a CUI Asset segment. Endpoint configuration baseline exists for Windows workstations. No baseline exists for measurement equipment endpoints.
New Risks Introduced	Measurement equipment may run an embedded operating system that does not accept the standard endpoint baseline. Lack of an existing baseline creates a configuration management gap that the current SSP does not address.
Determination	New risk identified. Baseline gap is not addressed in the existing SSP. Refer to Affirming Official for significant change evaluation under C-Q12.
SSP Sections Implicated	Asset Inventory, Network Diagram, Configuration Baselines, CM.L2-3.4.1 narrative, SC.L2-3.13.1 narrative.

CUI Flow Analysis under AC.L2-3.1.3

The CUI flow analysis answers a different question. It asks whether the change alters where CUI is created, where it moves, where it rests, or who has access to it. A change can introduce new risk without altering CUI flow. A different change can alter CUI flow without introducing new risk. Both analyses are required because each addresses a distinct compliance dimension.

The flow analysis is most useful when expressed as a delta against the current data flow diagram. The diagram shows the existing state. The delta describes the proposed state. The narrative explains what changed and why the change does or does not require updates to controls in the AC, SC, and SI families.

Analysis Identifier	CFA-2026-007
Linked SIA	SIA-2026-007
Current CUI Flow	Engineering receives CUI technical data packages from the prime contractor through the secure file transfer service. Engineering imports drawings into the CAD/CAM workstation. CAM produces G-code that flows to CNC controllers over the production VLAN.
Proposed CUI Flow Delta	CAM workstation will additionally produce CMM measurement programs derived from CUI dimensional data. Programs will flow from the CAM workstation to the new CMM endpoint over the production VLAN.
New Endpoints That Receive CUI	Mitutoyo CMM endpoint. The endpoint stores measurement programs locally for execution and stores measurement results that may include CUI dimensional data.
New Personnel With CUI Access	Quality inspectors operating the CMM. Two inspectors require role assignment under the Access Control policy.
AC Family Implications	Account creation required for inspectors. Role definition required. Access enforcement at the CMM endpoint must be verified.
SC Family Implications	VLAN segmentation already covers the production segment. No new boundary required.
SI Family Implications	Endpoint protection coverage required for the CMM. Verify that the embedded operating system supports the existing endpoint protection agent.

Change Documentation under CM.L2-3.4.3

The two analyses then enter the formal change management system. This step is the documentary anchor for the entire workflow. Without a change ticket that references the analyses by their identifiers and dates, an assessor has no way to verify that the analyses occurred at the right point in the sequence.

The change ticket should reference the SIA identifier, the CUI flow analysis identifier, the proposed implementation date, the assets affected, the personnel responsible, and the rollback procedure. The ticket should not advance to execution until the Affirming Official has reviewed the analyses and recorded the review in the ticket.

Change Ticket	CHG-2026-019
Submitter	Jane Smith, IT Manager
Date Submitted	May 12, 2026
Linked SIA	SIA-2026-007
Linked CUI Flow Analysis	CFA-2026-007
Change Summary	Install network connected CMM in inspection area. Establish endpoint configuration baseline. Configure inspector role and access permissions.
Proposed Implementation Window	May 26, 2026 through June 6, 2026
Personnel Responsible	IT Manager. Quality Manager. External integrator for CMM installation.
Rollback Procedure	Disconnect CMM from production VLAN. Remove inspector role assignments. Restore CAM workstation to pre-change state from configuration backup.
Operational Plan of Action Required	Yes. Temporary configuration baseline gap during implementation.
Affirming Official Review	Pending

Affirming Official Signature	_____ Date: _____

Affirming Official Review

The Affirming Official is the individual who signs the annual affirmation under 32 CFR 170.22 and who carries personal exposure under the False Claims Act. F-Q5 places the Affirming Official inside the change decision rather than at the end reviewing what already happened. The practical effect is that the change management workflow needs a sign-off field for the Affirming Official before any change advances to execution.

The Affirming Official review is not a technical review. It is a compliance review that addresses three questions. Whether the change can proceed under the existing CMMC Status. Whether the change requires an Operational Plan of Action during implementation. Whether the change triggers consideration of significant change under C-Q12.

Phase Two: During Implementation

Phase two opens with the creation of an Operational Plan of Action under CA.L2-3.12.2. The OPA is distinct from a Plan of Action and Milestones. C-Q9 in the same FAQ document states the difference. A POA&M addresses gaps identified during a CMMC assessment and carries a 180 day remediation window. An OPA addresses operational risks that arise after a system is in compliance and has no fixed timeline. The OPA is the working record of how the change is being executed and what temporary conditions exist while the work proceeds.

F-Q5 names three elements that belong in the OPA. The change description and any temporary risks introduced while the work proceeds. The personnel responsible for execution. Progress tracking that allows the Affirming Official and the assessor to see when the change moved from in progress to complete.

The OPA also functions as protective documentation. If the change creates a temporary deficiency that is still present at the next assessment and is assessed as NOT MET, the deficiency converts to a POA&M under C-Q9 and the 180 day window begins. The OPA is therefore the early record that demonstrates the deficiency was being managed before it was identified during assessment, which preserves the organization's options under the CMMC scoring methodology in 32 CFR 170.24.

OPA Identifier	OPA-2026-004
Date Opened	May 26, 2026
Linked Change Ticket	CHG-2026-019
Linked SIA	SIA-2026-007
Description of Change	Install and configure network connected CMM endpoint with access to production VLAN. Establish configuration baseline for measurement equipment. Configure inspector role and access permissions.
Temporary Risks	From May 26 through baseline approval, the CMM endpoint operates without a documented configuration baseline. Endpoint protection coverage will be verified during the second week of implementation.
Mitigation Measures During Implementation	CMM endpoint isolated to a dedicated subinterface within the production VLAN with restricted ACLs until baseline approval. Manual review of CMM configuration by IT Manager at end of each day.
Personnel Responsible	Jane Smith (overall). Mark Diaz (network configuration). Susan Park (endpoint baseline).
Progress Tracking	Week 1: Physical install complete. Network drop active. ACLs in place. Week 2: Endpoint protection agent verified. Baseline drafted. Week 3: Baseline approved. ACLs returned to standard production VLAN configuration.
Date Closed	Pending
Affirming Official Review	May 22, 2026 (initial). Pending (closeout).

Phase Three: After Implementation

Phase three closes the loop with an update to the System Security Plan under CA.L2-3.12.4. The FAQ specifies that the update must reach all sections affected by the change. In practice the update extends further than the asset inventory. New assets

ripple through the data flow diagrams, the boundary description, the inventory of CUI Assets and Security Protection Assets, the role definitions if administrative responsibility shifts, and the control narratives for any control whose implementation now depends on the new asset.

The table below shows the SSP sections most likely to require updates following a typical change involving a new endpoint and new personnel role.

Asset Inventory	Add the new asset. Record asset class, location, owner, and whether it is a CUI Asset, Security Protection Asset, Contractor Risk Managed Asset, or Specialized Asset.
Network Diagram	Update to reflect the new endpoint, its network segment, and any new traffic flows.
Data Flow Diagram	Update to reflect new CUI flow paths if the change altered them.
Boundary Description	Update if the change shifts the assessment boundary or introduces a new connection that requires description.
Configuration Baselines	Add or update the baseline that applies to the new asset class.
Role Definitions	Add new role if introduced. Update existing roles if responsibilities shifted.
Control Narratives	Update narratives for any control whose implementation now depends on the new asset. For a new endpoint, this typically reaches AC, AU, CM, IA, SC, and SI families.
SSP Revision History	Record the revision number, date, change identifier, sections updated, and Affirming Official review date.

The Affirming Official second review occurs at this point, before the next annual affirmation. The timing is deliberate. An affirmation made without Affirming Official review of changes accumulated during the year is defensible only if no significant changes occurred. F-Q5 requires the Affirming Official to be in a position to know.

Revision Number	v3.4
Date	June 9, 2026
Change Identifier	CHG-2026-019
Sections Updated	Section 3 (Asset Inventory). Section 4 (Network Diagram). Section 5 (Data Flow). Section 7 (Configuration Baselines). Section 9 (Roles). Section 12 (Control Narratives: AC.L2-3.1.1, CM.L2-3.4.1, SI.L2-3.14.2).
Summary of Update	Added Mitutoyo CMM endpoint to inspection area. New configuration baseline established for measurement equipment class. New inspector role defined with access to production VLAN.
Linked OPA	OPA-2026-004 (closed June 6, 2026)
Affirming Official Review	June 9, 2026
Affirming Official Signature	_____

External Service Provider Considerations

Two interactions deserve attention in environments where IT operations or security operations run through external service providers. The treatment of MSPs and MSSPs in E-Q3 and E-Q4 places those providers within the assessment scope without granting them their own assessment status. The F-Q5 workflow extends through the provider relationship rather than stopping at it.

When the MSP or MSSP initiates a change, the OSA change management workflow must extend into the provider. A shared responsibility matrix that does not name a responsible party for the SIA, the CUI flow analysis, the change ticket, and the Affirming Official notification leaves a gap that an assessor will identify. The matrix should name a responsible party for each artifact in the workflow and a verification mechanism that confirms the artifact was created.

The Operational Plan of Action remains owned by the OSA, not by the provider. The provider can populate the technical detail, but the document must live in the OSA compliance system because the Affirming Official must review it. This is consistent with

the structure of E-Q3 and E-Q4, which treat the provider as part of the assessment scope. The same principle applies to the SSP update. The SSP belongs to the OSA. The provider may supply technical content, but the OSA owns the document and the Affirming Official approves the revision.

Documentation Architecture

The artifacts produced by F-Q5 form a chain that an assessor can follow from end to end. The chain is auditable when each artifact references the next. The table below summarizes the artifact chain and the cross references that connect each link.

Phase 1, Artifact 1	Security Impact Analysis. References the change description and the SSP sections it implicates.
Phase 1, Artifact 2	CUI Flow Delta Analysis. References the SIA identifier and the data flow diagram revision.
Phase 1, Artifact 3	Change Management Ticket. References the SIA and CFA identifiers. Records the Affirming Official review.
Phase 2, Artifact 4	Operational Plan of Action. References the change ticket and SIA. Records progress, mitigations, and closure.
Phase 3, Artifact 5	SSP Revision. References the change ticket and OPA. Records the Affirming Official review of the completed change.
Annual Affirmation	References the SSP revision history. Confirms that all significant changes have been reviewed and that continuing compliance is intact.

When the chain is complete, the Affirming Official can affirm continued compliance with confidence and the assessor can verify that change management ran as the SSP describes. When the chain is broken, the affirmation rests on assumption rather than evidence, and the assessor must record the gap.

Conclusion

F-Q5 does not introduce new control requirements. It links existing controls into a sequence that the program office now expects organizations to follow. For organizations with mature change management, the FAQ confirms the procedure they already run. For the larger population of small DIB contractors using ad hoc change processes, F-Q5 creates a documentation gap that needs to be closed before the next assessment.

The transition to third party assessments on November 10, 2026 makes the gap consequential. A C3PAO assessor who finds an SSP update without a corresponding security impact analysis, or a change management entry without an Operational Plan of Action when temporary risk existed, is likely to treat that gap as evidence that the change process did not operate as documented. The cost of building the workflow now, while self-assessment is still the standard under Phase 1, is substantially lower than the cost of remediating it under a 180 day POA&M clock during a third party assessment.

The artifacts shown in this paper are templates. The field labels are constant. The content varies with each change. Organizations that adopt the templates as the structure of their internal change records will find that the F-Q5 workflow becomes a normal operating procedure rather than a compliance exercise. That outcome is the goal the program office set out to achieve when it published the FAQ.

About the Author

David W. Koran holds the CyberAB Registered Practitioner Advanced credential. He is the founder and principal of a consulting practice serving Defense Industrial Base contractors and their legal counsel, focused on CMMC readiness, enablement, and implementation. He is an associate member of the ABA Section of Public Contract Law and the author of *The CMMC Decision* (Second Edition).

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

References

Office of the Chief Information Officer, Department of War. Cybersecurity Maturity Model Certification Program (CMMC) Frequently Asked Questions, Revision 2.3. May 2026. https://dowcio.war.gov/CMMC/

32 Code of Federal Regulations Part 170, Cybersecurity Maturity Model Certification Program.
https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-170

32 CFR 170.21, Plan of Action and Milestones requirements. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-170/section-170.21

32 CFR 170.22, Affirmation requirements. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-170/section-170.22

32 CFR 170.24, CMMC Scoring Methodology. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-D/part-170/section-170.24

National Institute of Standards and Technology, Special Publication 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

National Institute of Standards and Technology, Special Publication 800-171A, Assessing Security Requirements for Controlled Unclassified Information. https://csrc.nist.gov/publications/detail/sp/800-171a/final

Defense Federal Acquisition Regulation Supplement clause 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

Defense Federal Acquisition Regulation Supplement clause 252.204-7021, Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement. https://www.acquisition.gov/dfars/252.204-7021