Identifying Unauthorized Use

The Policy Half of SI.L2-3.14.7

David W. Koran

CyberAB Registered Practitioner Advanced

April 2026

Introduction

SI.L2-3.14.7 is the seventh control in the System and Information Integrity family of NIST SP 800-171, which CMMC adopts for Level 2 certification. The SI family addresses how contractors identify, respond to, and recover from system and information integrity issues. Control 3.14.7 specifically requires the contractor to identify unauthorized use of organizational systems.

The CMMC practitioner community treats SI.L2-3.14.7 primarily as a monitoring control. Most implementation guidance points contractors toward Security Information and Event Management platforms, intrusion detection, and network traffic analysis. That guidance addresses part of what the control requires and not all of it.

The NIST SP 800-171A assessment objectives for 3.14.7 separate into two determinations. The first is that authorized use of the system is defined. The second is that unauthorized use is identified. These are distinct requirements with distinct evidence. An implementation that addresses only the second has satisfied only half of what the assessor is directed to evaluate.

This paper proposes the authorization-first reading of the control as the more defensible interpretation. The argument is straightforward. A detection mechanism that identifies unauthorized use must have a definition of authorized use to compare against. Without that definition, the identification step has no reference point. The authorization baseline is the artifact that provides the reference point, and it is a policy artifact the contractor produces.

The paper walks through what 800-171A actually requires, what the authorization baseline contains, how the detection layer connects to it, and what evidence the assessor will examine. A worked example carries through the middle sections using a fictional ten-person CNC machine shop to make the framework concrete. The final sections address the trajectory from Revision 2 to Revision 3 and respond to the predictable objection that assessors will not evaluate the control this carefully in early wave certification work.

What the Control Requires

NIST SP 800-171 Revision 2 states the control in a single sentence. The text reads as a single detection requirement on its face. The assessment objectives in NIST SP 800-171A tell a different story.

The objectives for 3.14.7 separate into 3.14.7[a], authorized use of the system is defined, and 3.14.7[b], unauthorized use of the system is identified. Two determinations, not one. The CMMC Assessment Process directs assessors to evaluate each objective using the examine, interview, and test methods. For objective [a], the examine method points to policy and procedure artifacts. The contractor must produce something that defines authorized use. Objective [b] then tests whether the contractor identifies activity that falls outside that definition.

Objective	Determination	Primary Evidence Category
3.14.7[a]	Authorized use of the system is defined	Policy and procedure artifacts
3.14.7[b]	Unauthorized use of the system is identified	Detection configuration and event records

The assessment methodology does not permit evaluating only objective [b]. An assessor who marks the control satisfied without confirming that authorized use is defined has not followed the CAP. That is the foundation on which the rest of the paper rests.

Why Monitoring Alone Does Not Satisfy the Control

A SIEM platform detects deviation from technical baselines. It observes what is happening on the network and flags activity that matches configured rules. The

rules are typically written against indicators of compromise, known attack patterns, and statistical anomalies. None of that answers the question of whether the observed activity was authorized.

Consider a user who transfers a large file to a cloud storage service at 2:00 a.m. The SIEM may flag the transfer based on volume, time of day, and destination. Whether the transfer was authorized depends on the contractor's policy. If the user is an engineer working an approved overnight shift, transferring project files to an approved collaboration platform, the transfer is authorized and the SIEM alert is a false positive. If the user is transferring CUI to a personal storage account, the transfer is unauthorized and the SIEM alert is correct. The SIEM cannot distinguish between the two without a policy definition of what counts as authorized.

This is the conceptual gap the control exposes. Detection technology observes activity without determining whether the activity is authorized. That determination requires a policy reference, which the control requires the contractor to produce separately. The identification step has meaning only once the authorization definition is in place.

Contractors who approach 3.14.7 as a pure monitoring problem miss this. They invest in detection capability without producing the policy artifact that gives detection its reference point. The result is a technically sophisticated implementation that cannot satisfy objective [a] because nothing in the implementation defines authorized use.

The Authorization Baseline

The authorization baseline is the set of policy artifacts that together define authorized use of organizational systems. It is not a single document. It is a structured collection of artifacts that each define one dimension of authorized use, and together provide the reference point the detection layer requires.

A reasonable counter-argument deserves direct treatment. Many contractors already maintain documentation that bears on authorized use. Access control policies specify who can reach what resources. Configuration management

baselines specify approved system states. Acceptable use policies specify prohibited behavior. A contractor reading this paper may ask whether the existing documentation already satisfies objective [a] without producing a new artifact.

The answer depends on coherence rather than content. Scattered documentation that collectively defines authorized use satisfies objective [a] only if the contractor can assemble it into a coherent reference on demand. The same ambiguity that makes SIEM alerts hard to interpret without a policy reference makes scattered documentation hard to evaluate as a definition of authorized use. What the baseline adds is not net new content. It is the connective tissue that lets the assembled documentation function as a single reference point. A contractor with mature documentation for related controls has most of the baseline in hand already. The remaining work is aggregation and cross-referencing, not creation.

One distinction is worth making explicit because it is the source of most confusion about 3.14.7. Access control and authorized use address different questions. Access control specifies who may reach what resources. Authorized use specifies what users may do with the resources they can reach. An engineer with authorized access to a CAD system may or may not be authorized to export files from that system to a personal cloud account. Access control policies alone do not answer the export question. The authorization baseline does.

Six elements make up a complete authorization baseline for most small and mid-size contractors. The paragraphs that follow introduce each element and illustrate it with a worked example. The example uses a fictional ten-person CNC machine shop referred to as Cogswell Cogs. The Shop holds CUI subcontracts from a tier-one aerospace prime and operates a standard small-contractor IT environment: Microsoft 365 GCC High for productivity and email, dedicated CAD and CAM workstations, a SIEM platform, endpoint detection and response, and a managed service provider under contract for IT support. The profile is familiar to most practitioners advising the defense industrial base.

The acceptable use policy is the foundational document. It states what users may and may not do with organizational systems, covering personal use, prohibited activity, expected conduct, and consequences for violation. This is the document most contractors already have in some form. The question is whether it is specific

enough to serve as a reference point for detection. Cogswell Cogs's acceptable use policy prohibits personal cloud storage accounts on company systems, prohibits use of personal email for any work purpose, prohibits use of personal devices to handle CUI, and states termination consequences for CUI violations. The policy is signed by each employee at hire and reviewed annually.

Role-based access expectations document what each role is authorized to access and what each role is authorized to do. An engineer's authorized use looks different from a finance user's authorized use, and the baseline specifies the difference. This element connects to AC.L2-3.1.1 and AC.L2-3.1.2 and reuses the same analysis the contractor already performs for those controls. Cogswell Cogs documents five roles. Engineers are authorized to access the CUI project folders, CAD, and the prime's collaboration portal. CNC operators are authorized to access CAM files and machine controllers, but not the broader project folders. Quality inspectors are authorized to read CAD files and access inspection data. The office manager has no CUI access. The IT contractor has administrative access for system maintenance but no routine access to CUI content.

The approved application inventory is the list of applications users are authorized to run. It covers operating system components, productivity software, line-of-business applications, and approved communication tools. Applications outside the list are unauthorized by definition, which gives the detection layer a concrete target. This element connects to CM.L2-3.4.8 and CM.L2-3.4.9. Cogswell Cogs's approved application list includes SolidWorks, Mastercam, Microsoft 365 GCC High, its endpoint detection platform, and the prime's collaboration portal client. Applications outside the list are blocked by application control at the endpoint.

Approved data movement patterns describe where CUI and other sensitive data may move. Covered items include approved destinations, approved protocols, and approved collaboration platforms. Unapproved data movement is unauthorized use that the detection layer can identify against this element. Cogswell Cogs's approved data movement patterns state that CUI enters the environment through the prime's collaboration portal or approved SFTP channel, resides on a designated file server, and leaves the environment only through the prime's portal or GCC

High encrypted email. USB removable media is prohibited for CUI. Consumer cloud destinations are blocked at the network edge.

Approved remote access conditions state the conditions under which remote access is permitted. This includes approved endpoints, approved locations, approved time windows if the contractor uses them, and approved authentication paths. The element connects to AC.L2-3.1.12 and AC.L2-3.1.14. Cogswell Cogs permits remote access only from company-issued laptops over VPN with multi-factor authentication. Remote access to CUI project folders is restricted to the engineering role. Personal devices cannot connect to the production network.

Approved third-party and ESP interactions document what external service providers and partners are authorized to access and how. The element connects to AC.L2-3.1.20 and is important for contractors using managed service providers or external security service providers, because the authorized activity of those providers must be defined before unauthorized activity can be identified. Cogswell Cogs's third-party register lists the managed service provider, the SIEM vendor's support organization, the cloud provider, and the prime contractor. Each entry specifies what the third party is authorized to access, through what channel, and under what contractual terms.

Baseline Element	Supports 3.14.7 Objective	Related Controls
Acceptable use policy	[a]	PS.L2-3.9.2
Role-based access expectations	[a]	AC.L2-3.1.1, AC.L2-3.1.2
Approved application inventory	[a]	CM.L2-3.4.8, CM.L2-3.4.9
Approved data movement patterns	[a]	AC.L2-3.1.3, MP.L2-3.8.1
Approved remote access	[a]	AC.L2-3.1.12, AC.L2-3.1.14

Baseline Element	Supports 3.14.7 Objective	Related Controls
conditions		
Approved third-party and ESP interactions	[a]	AC.L2-3.1.20

Each baseline element draws on documentation the contractor already produces for related controls. The acceptable use policy connects to personnel security requirements. Role-based access expectations connect to the access control analysis the contractor performs for AC.L2-3.1.1 and AC.L2-3.1.2. Approved application inventories connect to the configuration management work performed for CM.L2-3.4.8 and CM.L2-3.4.9. A contractor with mature documentation for these related controls has most of the baseline content in hand already. The work required to produce the baseline is aggregation and cross-referencing, not creation. The six elements are not the only way to structure the content. A contractor with a different governance framework may distribute the content differently. What matters is that each element is documented coherently and that the detection layer can reference it.

The baseline is not a one-time deliverable. It changes as the organization changes. New applications get approved, roles get added and retired, and remote access conditions evolve. The baseline requires an owner and a review cadence. Most contractors can handle the review annually with interim updates as material changes occur. The cadence itself should be documented as part of the baseline because the assessor will ask how the baseline stays current.

The Detection Layer

Once the authorization baseline exists, the detection layer has a reference point. The practical question is how to configure detection to compare observed activity against the baseline and surface deviations.

No single tool covers the full baseline. Detection is layered because the baseline has multiple dimensions and different tools observe different dimensions. SIEM correlation rules can be written against the role-based access expectations and the acceptable use policy. The rules flag authentication events, privilege use, and access patterns that deviate from what the role is authorized to perform.

Data Loss Prevention tools observe data movement. DLP policies configured against the approved data movement patterns identify attempts to move CUI to unapproved destinations, over unapproved protocols, or through unapproved channels. Cloud Access Security Broker platforms observe interaction with cloud services. CASB policies configured against the approved application inventory and approved data movement patterns identify unsanctioned cloud application use and unsanctioned data movement to cloud destinations.

User and Entity Behavior Analytics platforms observe behavioral patterns. UEBA tuned against role-based access expectations identifies users whose behavior deviates from their role baseline. Manual review processes cover what tooling cannot. Review of privileged account activity, review of exception grants, and review of third-party access patterns all require human judgment against the authorization baseline.

The layered approach has a consequence the assessor will notice. The contractor must be able to demonstrate that each element of the baseline is covered by at least one detection mechanism. A baseline element with no corresponding detection is a gap the assessor can identify. That does not mean every element requires a dedicated tool. One tool can cover multiple elements, and manual review covers elements that tooling cannot reach. What matters is that the coverage is complete and documented.

Applied to Cogswell Cogs, the coverage map shows how each baseline element connects to a specific detection mechanism. The approved application inventory is enforced at the endpoint through application control, which blocks unlisted executables and generates alerts when blocked launches occur. The approved data movement patterns are enforced through DLP policies configured against CUI-tagged files. The approved remote access conditions are monitored through SIEM correlation rules that alert on VPN connections from unmanaged devices and

authentication patterns that deviate from the role baseline. Role-based access expectations are monitored through combined SIEM and UEBA coverage. Third-party interactions are reviewed monthly against the third-party register. The acceptable use policy is enforced through endpoint DLP rules covering prohibited activity categories and periodic manual review.

Baseline Element	Detection Mechanism	Example Rule
Acceptable use policy	Endpoint DLP and manual review	Alert on prohibited activity categories
Role-based access expectations	SIEM and UEBA	Alert on access patterns outside role baseline
Approved application inventory	Endpoint application control	Block unlisted executable, alert on blocked launch
Approved data movement patterns	Data Loss Prevention	Block CUI-tagged files to non-approved destinations
Approved remote access conditions	SIEM correlation	Alert on VPN login from non-managed device
Approved third-party and ESP interactions	Access log review	Monthly review against third-party register

The coverage map is itself an evidence artifact. The assessor will ask how detection coverage tracks to the baseline. A contractor who can produce the map demonstrates that detection is not generic security monitoring, but is tied to the specific authorization decisions the contractor has documented. The map connects objective [a] evidence to objective [b] evidence and produces the coherence the assessment methodology looks for.

Evidence the Assessor Will Examine

The 800-171A assessment methodology uses three evidence categories: examine, interview, and test. For 3.14.7, each category produces a different type of evidence the contractor must prepare.

Examine evidence covers the policy and procedure artifacts. The authorization baseline itself, the detection configuration documentation, the review procedures, and the records of identified unauthorized use and its disposition all fall within this category. This is the documentation layer.

Interview evidence comes from personnel with responsibility for defining authorized use, personnel with responsibility for operating the detection layer, and personnel with responsibility for investigating identified events. The assessor will ask questions that test whether personnel understand both halves of the control and can describe how their activity connects to the baseline.

Test evidence covers operational demonstration that the detection layer functions as documented. The assessor may ask to see the current SIEM rule set, the current DLP policy, the current CASB configuration, and the disposition record for a sample of recent events.

The evidence package for 3.14.7 should include, at a minimum, the authorization baseline documentation, the detection layer configuration documentation, a map showing which detection mechanism covers which baseline element, the review procedures that keep the baseline current, a sample of identified unauthorized use events with disposition, and the procedural record showing the organization acted on what the detection layer produced.

A contractor who can produce all six items has satisfied both objectives and demonstrated the coherence between them. A contractor who can produce only the detection configuration and event records has produced evidence for objective [b] and nothing for objective [a]. That is the gap the assessor will identify.

Applied to the Cogswell Cogs example, the evidence package consists of the signed acceptable use policy, the role matrix, the approved application inventory, the data

flow documentation showing approved CUI paths, the remote access policy, the third-party register, the baseline-to-detection coverage map, a sample of recent detected events with disposition records, and the procedures governing baseline maintenance and event review. Each artifact is traceable to one or more assessment objective elements. Together they produce a coherent story for both objective [a] and objective [b]. A contractor who has assembled this package is prepared for the control regardless of how the assessor chooses to sequence the examine, interview, and test methods.

Where Revision 3 Takes the Requirement

NIST SP 800-171 Revision 3 consolidates the monitoring content from Revision 2 and aligns more closely with NIST SP 800-53 Revision 5. The SI-4 family in 800-53 covers system monitoring with explicit enhancements including SI-4(13), which addresses analysis of traffic and event patterns for unauthorized activity.

The direction of travel in Revision 3 is toward more specific Organization-Defined Parameters with DoD-specified values for defense contractors. That narrows contractor discretion on the quantitative parameters. It does not eliminate the authorization baseline requirement. The baseline is qualitative policy content, not a numeric parameter. No ODP replaces it.

Contractors preparing for the Revision 2 to Revision 3 transition should treat the authorization baseline as forward-compatible. The content the baseline contains remains required under Revision 3 even as the surrounding control structure changes. Contractors who invest in the baseline now will find the investment holds its value through the transition.

Anticipated Objections

Two objections to the reading advanced in this paper are predictable and worth addressing directly.

The first objection is that the paper reads the 800-171A objectives too literally. Practitioners who treat 3.14.7 as a monitoring control argue that objective [a] is a

procedural gloss on objective [b] rather than a separate determination. The response is that the objective wording separates them as distinct determinations, the CAP directs assessors to evaluate each separately, and the examine method for objective [a] points to policy artifacts. Reading the two objectives as one collapses the methodology NIST published. A practitioner who disagrees with this reading is disagreeing with the published methodology rather than with the paper.

The second objection is that assessors will not evaluate the control this carefully in practice. The prediction that early wave C3PAO assessors will focus on detection capability and overlook the authorization baseline is not unreasonable as a prediction. It is also speculation on all sides. The contractor bears the asymmetric risk. The cost of preparing the authorization baseline is a policy document and modest governance effort. The cost of not preparing it, if the assessor does evaluate objective [a], is a control finding and a SPRS score impact. The risk-adjusted choice is the same regardless of which prediction about assessor behavior turns out to be correct.

There is a third consideration worth naming. The practitioner community has not converged on a consistent reading of 3.14.7. Different advisors give different guidance. This paper proposes the authorization-first reading as the more defensible interpretation and welcomes the counter-argument. The purpose of the paper is to advance the conversation, not to close it.

Closing

SI.L2-3.14.7 has two halves. The first requires the contractor to define authorized use. The second requires the contractor to identify use that falls outside that definition. Both halves appear as separate objectives in the 800-171A assessment methodology. Both halves require evidence. An implementation that addresses only the second half has satisfied only half of what the assessor is directed to evaluate.

The authorization baseline is one way to satisfy the first half coherently. Six elements make up a complete baseline for most small and mid-size contractors. Each element maps to one dimension of authorized use and connects to related

controls the contractor already documents. The baseline is a policy artifact the organization produces and maintains, not a technical configuration.

The detection layer gives the baseline operational effect. Multiple tools cover different dimensions of the baseline. Manual review covers what tooling cannot. Complete coverage is demonstrated through a documented map from baseline elements to detection mechanisms. The Cogswell Cogs example shows what the resulting implementation looks like in practice for a small contractor.

The full reading of 3.14.7 is straightforward once the two halves are separated. This paper has proposed the authorization-first reading as the more defensible interpretation and has outlined what the corresponding implementation contains. Contractors who produce the baseline that gives objective [a] its evidence, and who map their detection layer against that baseline, have a defensible implementation regardless of how early wave assessment rigor turns out. The paper does not claim this is the only way to satisfy the control. It claims this is the approach most likely to withstand scrutiny, to age well as CMMC enforcement matures, and to produce the evidence the assessment methodology directs assessors to evaluate.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced and the founder of a consulting firm serving Defense Industrial Base contractors and their legal counsel. His practice focuses on CMMC 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.

Contact: dkoran@davidkoran.com, (802) 335-2662.

References

National Institute of Standards and Technology. NIST SP 800-171 Revision 2, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

National Institute of Standards and Technology. NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171A.pdf

National Institute of Standards and Technology. NIST SP 800-171 Revision 3, Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r3.pdf

National Institute of Standards and Technology. NIST SP 800-53 Revision 5, Security and Privacy Controls for Information Systems and Organizations. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Cyber AB. CMMC Assessment Process (CAP). https://cyberab.org/

Department of Defense. DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements. https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.