Who Owns the Control

A Departmental Responsibility Matrix for CMMC Level 2 in Aerospace Manufacturing

---

David W. Koran

CyberAB Registered Practitioner Advanced

June 2026

The Ownership Problem

Most CMMC Level 2 readiness efforts begin with a technical inventory and end with a technical owner. The 110 security requirements drawn from NIST SP 800-171 Revision 2 arrive as a single list, the list is handed to whoever runs the network, and the organization proceeds as though information technology owns the entire standard. That assumption holds for roughly half of the control families and breaks for the other half, and the families where it breaks are the ones that quietly stall a readiness program.

The standard does not distribute evenly across a manufacturing business. Awareness training is delivered and tracked by the people who run onboarding and annual training, which in most shops is human resources rather than the network administrator. Personnel screening and the removal of access on termination depend on the same function. Physical protection of the production area is the responsibility of whoever controls the building. The handling, marking, and disposal of removable media and printed drawings happen on the production floor, in the hands of machinists and engineers who generate and consume technical data every day. When each of these requirements is assigned by default to information technology, it does not receive a function suited to perform them, and it is left without an effective owner.

In practice, establishing this point is among the most difficult parts of beginning a new engagement. A manufacturer most often arrives convinced that CMMC is a project for the information technology department to complete, and the initial readiness work is often not technical at all. It is the work of showing the organization that compliance is a responsibility shared across the entire company, and that the controls must be assigned to the departments that actually perform them, before the program can move forward with any durability.

This paper maps the fourteen CMMC Level 2 control families to the functions that actually perform the work inside a typical aerospace manufacturer. The result is a departmental responsibility matrix that shows primary ownership, the supporting functions that contribute to each family, and the narrow set of decisions that belong to executive leadership. The matrix is built for a shop that already operates under AS9100, because the document control, configuration control, and records retention disciplines that an AS9100 manufacturer runs every day turn out to be assets that several CMMC families can reuse rather than rebuild.

A note on what this reference is and is not. It is a starting point for assigning responsibility, not a prescription that survives contact with every architecture. Ownership shifts when a managed service provider runs the technical stack, when a managed security operations center handles monitoring, or when the environment that

holds Controlled Unclassified Information is isolated within an enclave. Those arrangements redraw the lines, and the closing sections address how. The purpose here is to give a manufacturer a defensible first draft of who owns what, so that the readiness conversation starts from the organization rather than from the network diagram.

Why Ownership Is a Compliance Question

The assignment of responsibility is not an administrative convenience. The standard does not prescribe a departmental ownership chart, but the documentation it requires and the program that enforces it both depend on knowing which function performs each requirement.

NIST SP 800-171 Revision 2 expects an organization to document, within a system security plan, the system boundary, its operating environment, and how each requirement is implemented. A description of how a requirement is implemented cannot stay accurate when no function has been assigned to perform it, because there is nothing for the description to capture. The system security plan becomes a record of intent rather than of operation, and that gap is precisely what an assessor probes.

The Cybersecurity Maturity Model Certification Program, codified at 32 CFR Part 170, reinforces the point through the affirmation requirement. Under 32 CFR 170.22, a senior official affirms continuing compliance at the time of assessment and annually thereafter, and that official carries personal responsibility for the accuracy of the affirmation. An affirming official cannot reasonably attest to the continuing operation of controls for which no function has been assigned to operate. The annual affirmation depends on a chain of functional owners who maintain their portion of the program throughout the year and report up; where that chain has missing links, the affirmation rests on assumptions.

The result is that ownership is a readiness question rather than a paperwork question. A control without an owner drifts, and the families most prone to drift are those whose work lies outside information technology. Awareness training lapses when no one is accountable for the annual cycle, access lingers after an employee departs when termination and deprovisioning are not connected, and media accumulates on the floor without marking when no one there has been told that marking is part of the job. Each of these is an ownership failure before it is a technical failure, and each is invisible on a network diagram.

CMMC as a Company-Wide Project

Because the work is distributed across the business, implementing CMMC is a company-wide project rather than a technical deployment. A program that touches access, training, screening, facilities, engineering data, the production floor, the quality system, and contract obligations has the structure of a cross-functional undertaking, and it succeeds or fails on the same conditions that govern any such undertaking, which are a sponsor with authority, a named owner for each part of the work, a schedule that respects dependencies, and a regular accounting of progress. Run as a task list within information technology, the effort stalls with the very families that live outside it, which are the families most often left without an owner.

The discipline this requires is ordinary project management applied to a compliance objective. The sponsor is the executive who answers for the business and who will sign the affirmation, and the sponsor charters the work, assigns the owners, and holds each owner to the portion of the standard they carry. The responsibility matrix that follows is the project's assignment of work, the document that tells the project lead who owns each family and which functions have to coordinate. Sequence matters as much as assignment because several families depend on earlier decisions. The scope of the assessment and the inventory of assets that hold Controlled Unclassified Information govern almost everything downstream, and policy precedes the implementation it describes, so a schedule that treats controls as a flat list rather than a set of dependencies allocates effort in the wrong order. The project doesn't close at certification, because the annual affirmation converts the implementation into an operating program that the same owners sustain.

The Eight Functions in an Aerospace Manufacturer

A responsibility matrix needs a stable set of functions to assign work to. The eight below describe how responsibility is typically distributed in a small- to mid-sized aerospace manufacturer operating under AS9100. A smaller shop will combine several of these into one person, and the closing sections address those combinations. The functions are defined by the work they perform rather than by the titles on an organization chart.

Function	Scope of ownership within a CMMC Level 2 program
IT / Security	Designs, operates, and monitors the technical controls across access, authentication, audit, configuration, communications, and system integrity, and owns the largest share of the standard.
Human Resources	Delivers and tracks awareness training, performs screening before access is granted, and triggers the removal of access when an individual departs or changes role.
Facilities	Controls physical access to the building and to the areas where Controlled Unclassified Information is processed, stored, or produced, including badges, locks, visitor handling, and the physical environment.
Engineering	Generates and consumes technical data, owns the baselines for engineering workstations and design software, and handles drawings and specifications that frequently carry CUI markings.
Operations	Runs the production floor where technical data becomes parts, owns removable media handling at the machine, and coordinates maintenance of production equipment.
Quality	Operates the AS9100 document control, configuration control, and records retention systems that several CMMC families reuse for marking, versioning, and evidence.
Contracts	Identifies Controlled Unclassified Information obligations as they arrive in contract flowdowns, manages incident reporting obligations to the customer, and connects compliance posture to award eligibility.
Executive	Holds the decisions that cannot be delegated, including acceptance of residual risk, approval of the plan of action, authorization of incident response, and the annual affirmation.

Two of these functions earn a place that guidance built around information technology routinely overlooks. Quality is named because an AS9100 shop already runs the controlled processes that media protection and configuration management depend on, and naming Quality lets the manufacturer extend a mature system rather than build a parallel one. Contracts is named because the obligation to protect Controlled Unclassified Information, and to report incidents involving it, enters the business through contract language and must be connected back to it.

The Responsibility Matrix

The matrix below assigns each of the fourteen control families a primary owner, supporting functions, and, where applicable, an accountable executive. The function names appear in the header, and the responsibility codes are defined in the key below.

Responsibility codes

P	Primary owner. Owns the family and performs the core work.
S	Supporting. Contributes execution, input, or data.
O	Oversight. Independent oversight or review, not execution.
E	Executive accountability. A decision leadership holds and cannot delegate.

Control Family	IT / Security	Human Resources	Facilities	Engineering	Operations	Quality	Contracts	Executive
AC Access Control	**P**			S	S			
AT Awareness and Training	S	**P**						
AU Audit and Accountability	**P**					S		**O**
CA Security Assessment	**P**						S	***E***
CM Configuration Management	**P**			S	S	S		
IA Identification and Authentication	**P**							
IR Incident Response	**P**				S		S	***E***
MA Maintenance	**P**		S		S			
MP Media Protection	**P**			S	S	S		
PE Physical Protection	S		**P**		S			
PS Personnel Security	S	**P**						
RA Risk Assessment	**P**						S	***E***
SC System and Communications Protection	**P**			S				
SI System and Information Integrity	**P**				S			

Audit and accountability carry an oversight mark, shown as O, because separation of duties at requirement 3.1.4 requires that the individual who administers the audit function be distinct from the individual who administers access, so that the record of privileged activity does not rest solely with the administrator it documents. This requirement is examined in the section on where the standard requires two owners.

Read down a column to see everything a single function touches, and read across a row to see how many functions a single family requires.

Three Bands of Ownership

When the supporting marks are visible, the fourteen families sort into three bands, and the band a family falls into predicts how much organizational coordination it demands.

The first band is cleanly owned by information technology and requires little coordination beyond that. Identification and authentication sit entirely within the technical stack. System and communications protection and system and information integrity are managed by information technology, with only limited input from other functions, such as operations related to the integrity of the software that runs production equipment. These families are where the default assumption of technical ownership is correct, and they are not where readiness programs fail. Audit and accountability are operated within the technical stack as well, but they carry a separation requirement that sets them apart from this band, addressed in the section on where the standard requires two owners.

The second band depends on a clean handoff between two or three functions, typically triggered by a discrete event. Awareness training and personnel security depend on human resources executing a cycle and a checklist that information technology then acts on. Physical protection depends on facilities maintaining the building envelope, while operational controls govern who moves through the production area. Access control depends on information technology provisioning accounts that engineering and operations request and justify. The work in this band is not difficult, but it fails silently when the trigger fires and the handoff doesn't, most commonly when an individual leaves and access removal lags behind the departure.

The third band is where ownership genuinely distributes across three or four functions, and these are the families that stall when any contributing owner is unnamed. Configuration management and media protection each draw on information technology, engineering, operations, and quality, because a controlled drawing is a configuration item, an engineering artifact, a floor document, and a quality record. Maintenance draws on information technology, facilities, and operations because the equipment under maintenance ranges from servers to building systems to production machinery. Incident response draws on information technology to detect and contain, operations to sustain production through a disruption, contracts to meet the customer reporting obligation, and executive leadership to authorize the response. A family in this band cannot be assigned to a single owner without leaving part of the work undone.

Where the Standard Requires Two

The bands describe families that need more than one owner because the work is large or distributed. A separate, smaller group of requirements needs more than one owner for a different reason: the standard does not permit a single individual to hold both the action and its record. These are the requirements at the intersection of access and audit, and they invert the usual problem. The risk is not a family with no owner, but a family with one owner where the standard requires two.

Four requirements define this intersection. Requirement 3.1.4 separates individuals' duties to reduce the risk of malevolent activity without collusion, and its discussion identifies the controlling example: personnel who administer access control functions should not also administer audit functions. Requirement 3.1.7 prevents non-privileged users from executing privileged functions and records their execution in the audit log. Requirement 3.3.8 protects audit information and the logging tools from unauthorized access, modification, and deletion. Requirement 3.3.9 limits management of the logging functionality to a subset of privileged users.

Read together, these requirements establish a principle that a single owner cannot satisfy. The administrator who holds privileged access cannot also be the sole custodian of the logs that record how that access is used, because an administrator who can act and then alter the record of the action defeats the purpose of the audit trail. The practical failure is common and specific. Audit logs are stored in the same environment and under the same administrative account they are meant to monitor, which causes requirements 3.3.8 and 3.3.9 to fail together. Audit and accountability are among the families most often missed in Level 2 assessments; not because the logging is absent, but because the separation that protects it has not been established.

This is the strongest illustration of why CMMC is a responsibility distributed across the organization rather than a task assigned to a single administrator. It is also where the responsibility matrix must be read with care, because the single column for information technology and security contains two roles that requirement 3.1.4 does not allow to collapse into one person. How the separation is achieved depends on the organization's size, as addressed in the closing sections. In a shop large enough to staff the roles separately, the system administrator is not the audit administrator. In a shop with a single administrator, the separation cannot be created internally and becomes an oversight responsibility held by management, expressed on the matrix as the oversight mark (O) for audit and accountability.

The Families in Detail

The details below are a working reference for assigning responsibility, and the assignments should be adjusted to the architecture and staffing of the individual shop.

Access Control (AC)

Access control is owned by information technology, which provisions accounts, enforces least privilege, and manages the separation of duties across the systems that hold Controlled Unclassified Information. The supporting work belongs to engineering and operations, because the decision about who needs access to a given drawing, machine program, or production system originates with the people who use that data rather than with the administrator who grants it. The family operates correctly when access requests include a justification from the requesting function and when changes in role or assignment are reported to information technology promptly enough to adjust access. The point of failure is rarely the technical mechanism and is usually the flow of information from the floor to the administrator. Access control also carries the separation of duties requirement at 3.1.4 and the capture of privileged actions at 3.1.7, which together require that privileged access not rest with a single unchecked individual, as set out above.

Awareness and Training (AT)

Awareness and training are owned by human resources, which already runs onboarding and the annual training cycle for the workforce. Information technology supports the family by supplying security-specific content and confirming that role-based training reaches people with privileged access, but delivery, scheduling, and tracking fall to the function that runs training for every other purpose in the business. The family fails when security awareness is treated as a technical task and therefore never folded into the established training calendar, leaving completion unrecorded and the annual cycle unmanaged.

Audit and Accountability (AU)

Audit and accountability are owned by information technology, which configures logging, protects the integrity of audit records, and reviews events for indications of compromise. Quality contributes to the retention decision because the retention period for audit records is a records management matter that the existing retention schedule can accommodate. The family carries a second, less obvious owner in executive oversight, because requirements 3.3.8 and 3.3.9 protect audit information and limit who may manage logging, and separation of duties at 3.1.4 requires that the audit function be administered by someone other than the administrator whose activity it records. In a shop with a single administrator, that independent check is an oversight responsibility

held by management rather than a task that can be delegated back to the person being logged. Audit and accountability are among the families most often missed in assessment, not for want of logging but for want of the separation that keeps the log trustworthy.

Security Assessment (CA)

Security assessment is owned by information technology for conducting the assessment and maintaining the system security plan and the plan of action and milestones, while executive leadership is accountable for the decisions those instruments entail. Contracts support the family by linking assessment results to award eligibility and tracking the customer-facing obligations associated with a given status. The accountable decision is the leadership choice to proceed with open items in the plan of action and to sign the affirmation, as discussed in the discussion of executive accountability.

Configuration Management (CM)

Configuration management is distributed across four functions, which places it among the families most likely to stall when any contributor is unnamed. Information technology owns the baselines for the information systems and enforces change control on them. Engineering contributes the baselines for design and engineering workstations and the controlled software that runs on them. Operations contribute to configuring production equipment and the systems that drive it. Quality contributes to the controlled change process that an AS9100 shop already runs, which gives configuration management a discipline and a paper trail that the organization doesn't have to invent. A controlled drawing is at once a configuration item, an engineering artifact, a floor document, and a quality record, and the family is satisfied only when each of those functions performs its portion.

Identification and Authentication (IA)

Identification and authentication sit entirely within information technology, which manages identities, enforces multifactor authentication, and governs the authenticators that protect access to Controlled Unclassified Information. The family is the cleanest in the standard from an ownership perspective because the work begins and ends within the technical stack and requires no handoff to another function. It is named here for completeness rather than for any coordination it demands.

Incident Response (IR)

Incident response draws on four functions because an incident is simultaneously a technical event, an operational disruption, a contractual obligation, and a leadership decision. Information technology is responsible for detection, containment, and recovery. Operations supports the family by sustaining production through disruptions

and by preserving the evidence residing on production systems. Contracts support the family by managing the reporting obligation that a cyber incident creates, which, under DFARS 252.204-7012, makes the incident a contractual event with a defined reporting path. Executive leadership is accountable for authorizing the response and, with contracts and counsel as needed, determining whether the event meets the contractual reporting threshold established by the clause. The family is one of the clearest illustrations of why a single technical owner is insufficient.

Maintenance (MA)

Maintenance is owned by information technology for the systems that process Controlled Unclassified Information, but the family reaches beyond the information systems into the building and onto the floor. Facilities support the family because building systems and the physical environment fall under maintenance as defined by the standard. Operations supports the family because production machinery and the controlled tooling that drives it require maintenance that often involves outside vendors and remote connections. The family is satisfied when maintenance of every system in scope, from servers to production equipment, follows the controls required by the standard, including supervision of maintenance personnel and sanitization of equipment leaving the site.

Media Protection (MP)

Media protection is distributed across the same four functions as configuration management, for the same reason: media in an aerospace shop is rarely confined to information systems. Information technology is responsible for the protection, marking, and sanitization of digital media. Engineering contributes because drawings and specifications bearing markings pass through engineering hands. Operations contribute because removable media at the machine, and printed technical data on the floor, are handled by production staff who must know that marking, control, and disposal are part of their work. Quality contributes to the marking and retention discipline that the document control system already enforces. The family is the most physically distributed in the standard, and it fails most often where printed and removable media on the floor have no named owner.

Physical Protection (PE)

Physical protection is owned by facilities, which control the building envelope, the badges and locks that govern entry, and visitor handling. Operations supports the family by controlling movement through the production area where Controlled Unclassified Information becomes parts, because access to the floor is access to the data. Information technology supports the family where physical protection meets equipment, such as the security of network hardware and the spaces that house it. The family depends on a

clear division between who controls the building and who controls the area within it where controlled work occurs.

Personnel Security (PS)

Personnel security is owned by human resources, which performs the screening that precedes access and manages changes in access following a departure or a change in role. Information technology supports the family by executing the deprovisioning initiated by human resources. The family contains only two requirements, but it is among the most common sources of drift because the removal of access upon termination depends on a handoff that fails silently whenever the departure is communicated to payroll but not to the administrator who holds the keys to the systems.

Risk Assessment (RA)

Risk assessment is owned by information technology for the identification and documentation of risk and for the vulnerability management that supports it, while executive leadership is accountable for the acceptance of residual risk. Contracts support the family by surfacing the risk that specific contract obligations introduce. The accountable decision is the leadership judgment about which risks to accept and which to fund for reduction, which is a business decision rather than a technical one and is addressed in the discussion of executive accountability.

System and Communications Protection (SC)

System and communications protection is owned by information technology, which manages boundary protection, encryption, and the separation of the environment that holds Controlled Unclassified Information. Engineering provides a narrow supporting contribution where the design environment and its connections fall within the protected boundary. The family is otherwise contained within the technical stack and is among those for which the default assumption of technical ownership holds.

System and Information Integrity (SI)

System and information integrity is managed by information technology, which oversees flaw remediation, malicious code protection, and anomaly detection. Operations provides a supporting contribution when the integrity of software running production equipment falls within scope, because a machine controller is a system whose integrity matters as much as that of a server. The family otherwise sits within information technology and requires limited coordination beyond the floor.

The Aerospace Advantage: Quality as an Existing System

The Quality column is the single most useful insight a manufacturer can take from this matrix, because it converts a perceived burden into an existing capability.

An AS9100 manufacturer already operates document control, configuration control, and records retention as audited disciplines. Drawings carry revision levels and approval signatures; changes move through a controlled, traceable process; and records are retained for defined periods and produced on demand during quality audits. These are the same behaviors that configuration management and media protection require under CMMC, expressed in the language of aerospace quality rather than information security.

The practical consequence is that several CMMC requirements can be satisfied by extending the quality system rather than standing up a separate one. The marking of technical data as controlled can ride on the existing document control header, the baseline and change control that configuration management expects can be expressed through the configuration control the shop already runs for engineering changes, and the retention of audit and assessment evidence can use the records retention schedule that already exists for quality records. A manufacturer that recognizes this overlap reduces both the cost and the friction of readiness, because the people who run the quality system are accustomed to controlled processes and to producing evidence for an auditor.

This is also why Quality earns a column of its own rather than being folded into Engineering. The two functions touch different parts of the standard, since engineering generates and consumes the technical data while quality controls how that data is versioned, marked, and retained. Separating them on the matrix keeps the reuse opportunity visible.

Executive Accountability: Three Decisions

The executive column is deliberately sparse. Marking leadership accountable for every family would be accurate in the abstract, because the affirming official carries responsibility for the whole program, but it would also be useless, as it would not tell anyone where a leadership decision must be made. The matrix reserves the accountable mark for the three families that contain a decision leadership that cannot be delegated.

Risk assessment carries an accountable mark because the acceptance of residual risk is a leadership decision. A practitioner can identify and document risk, but the choice to

accept a level of risk, or to fund its reduction, belongs to the person who answers for the business.

Security assessment carries an accountable mark because the plan of action and the affirmation are leadership instruments. The decision to proceed with open items in a plan of action and the signature on the annual affirmation under 32 CFR 170.22 rest with the affirming official rather than with the staff who prepared the assessment.

Incident response carries an accountable mark because the authorization to respond and the determination of whether the event meets the contractual reporting threshold extend beyond the technical team. The reporting obligation under DFARS 252.204-7012 makes the incident a contractual event as well as a technical one, and that determination is a leadership responsibility informed by contracts and counsel.

Showing executive accountability as three sharp decisions, rather than a blanket responsibility, makes the matrix more honest and usable. It tells leadership exactly where its signature and its judgment are required, and it keeps the rest of the program in the hands of the functions that operate it. Beyond these three decisions, executive responsibility appears once more on audit and accountability as an oversight role, marked O, which is the independent review that separation of duties requires, rather than a discrete decision.

Scaling the Model to the Shop

The eight-function matrix describes a manufacturer large enough to staff each function distinctly. Many shops are smaller, and the model collapses cleanly when needed.

In a smaller manufacturer, quality and engineering frequently report to the same leader, and the document control work assigned to quality by the matrix may be performed by an engineering manager. The two columns merge, but the underlying work doesn't disappear, and keeping it visible during readiness ensures that marking and configuration control aren't lost during the merge. Contracts are often not a department at all, but a responsibility carried by the owner or a general manager, and the contract review and incident reporting obligations fall on that person. Facilities may be a single office manager who also holds the keys. The collapse is a matter of assigning the same work to fewer people rather than of removing the work.

Architecture redraws the lines more substantially than headcount does. When a managed service provider operates the technical stack, much of the information technology column shifts to the provider, and the manufacturer retains responsibility for oversight of the controls the provider doesn't cover and for the shared responsibilities defined in a customer responsibility matrix. A particular caution applies

where the same provider both operates the systems and holds the only copy of the audit logs, because that arrangement places the action and the record of the action in the same hands and undermines the separation required by requirements 3.1.4 and 3.3.9. The manufacturer retains the obligation to independently review the audit trail produced by the provider. When a managed security operations center handles monitoring, audit review, and a share of incident response that moves outside the building, the manufacturer retains the obligation to act on what the center reports. When the environment that holds Controlled Unclassified Information is isolated within an enclave, the families that depend on physical and media handling are limited to the enclave boundary, and the population of people and machines in scope shrinks accordingly.

None of these arrangements removes ownership from the manufacturer. They relocate the performance of the work while leaving accountability in place, and the matrix remains the tool for confirming that every relocated control still has a named owner on the manufacturer side who can speak to it during an assessment and affirm it annually.

Ownership as Drift Prevention

A responsibility matrix earns its place not at the moment of assessment but in the period between assessments, where compliance quietly erodes.

A CMMC certification reflects the state of a program on the day it is assessed, and the affirmation that follows, together with the annual affirmation after that, attests that the program has continued to operate. The distance between a point-in-time assessment and a continuing attestation is where drift occurs, and drift is almost always an ownership failure expressed over time. Training cycles lapse, departed employees retain access, configuration baselines diverge from their documented state, and media accumulates without marking. Each of these is a control that had an owner on assessment day and lost effective ownership in the months that followed.

A matrix that names a primary owner for every family and a supporting owner for every contributing function gives the program a self-sustaining structure. Each owner knows which portion of the standard they are responsible for, and the affirming official knows whom to ask before signing. The annual affirmation becomes a summary of functional owners confirming their portion rather than an act of faith by a single executive. The matrix, in other words, is not only a readiness tool. It is the organizational backbone that makes a continuing attestation defensible.

Conclusion

CMMC Level 2 is written as a technical standard, and that framing leads organizations to assign it to a technical owner. The standard, when read against how a manufacturer actually operates, is distributed across the business. Roughly half of it belongs to information technology, and the other half is shared with human resources, facilities, engineering, operations, quality, contracts, and executive leadership. The families that stall a readiness program are almost always the ones in that second half, orphaned by the assumption that information technology owns everything.

A departmental responsibility matrix corrects the assumption before it does damage. It names a primary owner for every family, makes the supporting functions visible, reserves executive accountability for the decisions that require it, and gives an AS9100 manufacturer credit for the quality system it already runs. It scales down to a small shop and adapts to a managed or enclaved architecture without losing its purpose: ensuring that no control is left without someone who owns it. That assurance is what readiness requires and what the annual affirmation depends on.

About the Author

David W. Koran holds the CyberAB Registered Practitioner Advanced credential and is the founder of a consulting practice serving Defense Industrial Base contractors and the legal counsel who support them, with a focus on 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. He can be reached at dkoran@davidkoran.com or (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.

Cybersecurity Maturity Model Certification (CMMC) Program. 32 CFR Part 170.

Affirmation. 32 CFR 170.22.

Safeguarding Covered Defense Information and Cyber Incident Reporting. DFARS 252.204-7012.

SAE International and International Aerospace Quality Group. AS9100D. Quality Management Systems, Requirements for Aviation, Space, and Defense Organizations (2016).