HANDBOOK

A PRACTITIONER'S HANDBOOK FOR **CMMC**

Leveraging NIST Resources to Achieve CMMC Level 2 Readiness. Developed to Aide Information Systems Security Managers, Architects, Engineers and Administrators.

ERIC CATALINE | CISSP, CGRC

Contents

Background

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) PROGRAM

The Federal Register's final rule for CMMC contains an informative history section. This handbook highly recommends familiarizing yourself with that history because it explains the overall intent of the CMMC program as it dates back to the 2010 Executive Order titled *Controlled Unclassified information* (CUI). The order's intent: "establish an open and uniform program for managing [unclassified] information that requires safeguarding or dissemination controls."[1] The section goes on to say that "In 2019, DoD announced the development of CMMC in order to move away from a 'self-attestation' model of security."[2] Updated in 2021, the CMMC primary goals are:[3]

- Safeguard sensitive information to enable and protect the warfighter
- Enforce DIB cybersecurity standards to meet evolving threats
- Ensure accountability while minimizing barriers to compliance with DoD requirements
- Perpetuate a collaborative culture of cybersecurity and cyber resilience
- Maintain public trust through high professional and ethical standards

HANDBOOK PURPOSE

This handbook has been developed based on best practices, use cases and experience with the intent to assist organizations in achieving Level 2 Cybersecurity Maturity Model Certification (CMMC) certification and full implementation of the 110 security requirements described in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171r2: *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*. This handbook is meant to be supplemental to official CMMC guidance and should not be considered authoritative. Cadre has no official affiliation with the CMMC program, the Federal Register or the Department of Defense (DoD).

HANDBOOK TERMINOLOGY, CITATIONS AND QUOTATIONS

In an effort to avoid ambiguity: standardized terminology will be used. In this handbook, if a defined term is used, it will be *green and italicized*. Defined terms in this handbook are used deliberately and with the intent to align directly to their respective definitions, from their respective sources. A glossary with sources is provided further on in the handbook.

Acronyms will be introduced in the standard format. For specific considerations of emphasis or reader comprehension, full unabbreviated terms may still be used throughout this document.

This handbook will make numerous references to its sources. References are made throughout this handbook using endnotes. Quotations are also italicized and cited using endnotes. Links will also be used throughout the handbook.

HANDBOOK AUDIENCE

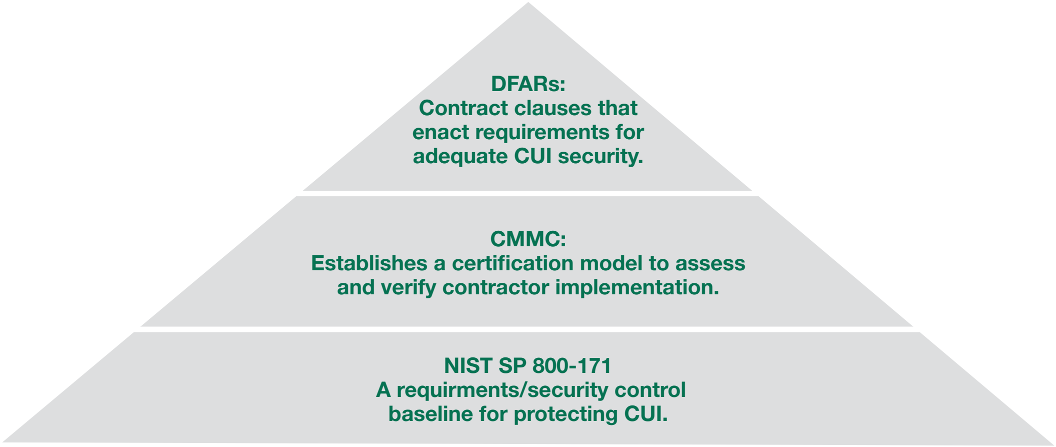
The audience for this handbook are individuals and organizations who perform work under the requirements of the Defense Federal Acquisition Regulation Supplement (DFARS) clauses 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting (or 7012), 252.204-7019 Notice of NIST SP 800-171 DoD Assessment Requirements (or 7019), and 252.204-7020 NIST SP 800-171 DoD Assessment Requirements (or 7020). Specific roles targeted are *Information System* (or *System*) managers, architects, engineers and administrators.

Guidance and Governance

DFARS CLAUSES, CMMC AND NIST SP 800-171

If working under a contract where there is a need for the storage, processing or transmission of *CUI*, then a *Covered Contractor Information System*[4] must be used and *Adequate Security* for that *CUI* must be provided. The 7012 clause defines *Adequate Security* as "protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information."[5] However valuable the information, place equal value on the protection of it.

In practice, *Adequate Security* is the implementation of the NIST SP 800-171r2 and its 110 Security Requirements (or *Controls*). CMMC is a DoD program that "aligns with the DoD's existing information security requirements for the DIB… [and] provides the DoD with increased assurance that contractors and subcontractors are meeting the cybersecurity requirements for nonfederal *Systems* processing [*CUI*]."[6]



DFARs:
Contract clauses that enact requirements for adequate CUI security.

CMMC:
Establishes a certification model to assess and verify contractor implementation.

NIST SP 800-171
A requirments/security control baseline for protecting CUI.

DFARS clauses 7019 and 7020 focus mainly on the assessment of an organization's implementation of SP 800-171. To summarize, clause 7012 is about safeguarding *CUI* and properly reporting incidents, while the 7019 and 7020 clauses define assessment requirements. As an organization works to bring a discrete set of components to a life as a *Contractor Covered Information System*, it must abide strictly by the assessment requirements and frequencies described in the CMMC level that it seeks to achieve. This handbook focuses on achieving Level 2 readiness. The bulk of the day-to-day workload under CMMC will likely be an organization's activities involving their SP 800-171 implementation.

Table 1: CMMC Level and Assessment Requirements

CMMC Status	Source & Number of Security Reqts.	Assessment Reqts.	Plan of Action & Milestones (POA&M) Reqts.	Affirmation Reqts.
Level 1 (Self)	• 15 required by FAR clause 52.204-21	• Conducted by Organization Seeking Assessment (OSA) annually • Results entered into the Supplier Performance Risk System (SPRS)	• Not permitted	• After each assessment • Entered into SPRS
Level 2 (Self)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by OSA every 3 years • Results entered into SPRS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 2 (C3PAO)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012	• Conducted by C3PAO every 3 years • Results entered into CMMC Enterprise Mission Assurance Support Service (eMASS) • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(2) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Entered into SPRS
Level 3 (DIBCAC)	• 110 NIST SP 800-171 R2 required by DFARS clause 252.204-7012 • 24 selected from NIST SP 800-172 Feb2021, as detailed in table 1 to § 170.14(c)(4)	• Pre-requisite CMMC Status of Level 2 (C3PAO) for the same CMMC Assessment Scope, for each Level 3 certification assessment • Conducted by DIBCAC every 3 years • Results entered into CMMC eMASS • CMMC Status will be valid for three years from the CMMC Status Date as defined in § 170.4	• Permitted as defined in § 170.21(a)(3) and must be closed out within 180 days • Final CMMC Status will be valid for three years from the Conditional CMMC Status Date	• After each assessment and annually thereafter • Assessment will lapse upon failure to annually affirm • Level 2 (C3PAO) affirmation must also continue to be completed annually • Entered into SPRS

Source: CMMC Final Rule

RECEIVING GUIDANCE

The majority of the guidance for CMMC is publicly available on posted websites hosted by the DoD itself, as well as reliable links through the NIST and other cooperative federal agencies. It is vital for a prime contractor to communicate with their respective government customers and properly receive any additional guidance they may provide. Depending on the government customer, they may have certain templates and *System Security Plan* structures they would like to see submitted for assessment as well as possible security enhancements (e.g., controls tailored in) that exceed the standard described in the DFARS. Similarly, subcontractors should communicate with their respective prime contractors and seek out any and all additional guidance.

ESTABLISHING CYBERSECURITY GOVERNANCE BASED ON GUIDANCE: CONCEPTS OF OPERATIONS

Upon receiving proper guidance, the organization may then work to formally establish governance based on that guidance. There is no singular way to establish governance, however, one particularly useful method is to develop a *Concept of Operations* or *ConOps*. "The [*ConOps*] provides the basis for bounding the operating space, system capabilities, interfaces, and operating environment."[7] The *ConOps* is a great place to introduce all users and stakeholders to the operating space or boundary of the *System*. High-level diagrams of *CUI* data flow work well in a *ConOps* to provide a visual depiction and build context for stakeholders, administrators and users. Analysis is the best way to understand programmatic, architectural, operational, and threat contexts and to prioritize *Cybersecurity* practices.

Table 2: A Tailorable Process for Cyber Resiliency Analysis

Analysis Step	Motivating Question	Tasks
Understand the context	How do stakeholder concerns and priorities translate into cyber resiliency constructs and priorities?	• Identify the programmatic context. • Identify the architectural context. • Identify the operational context. • Identify the threat context. • Interpret and prioritize cyber resiliency constructs.

Source: NIST SP 800-160v2r1

PUTTING CYBERSECURITY GOVERNANCE INTO ACTION: SYSTEM SECURITY PLANS

CMMC compliance simply cannot be achieved without having an *SSP*;[8] and that plan must "describe system boundaries, system environments of operation, how security requirements are implemented, and the relationships with or connections to other systems."[9]

When it comes to plan development, a key concept to understand is that *SSPs* can be more than one document.

> "Security plans need not be single documents; the plans can be a collection of various documents including documents that already exist. Effective security plans make extensive use of references to policies, procedures, and additional documents (e.g., design and implementation specifications) where more detailed information can be obtained."[10]

With that in mind, the aforementioned *ConOps* may be part of the overarching *SSP*. In terms of *SSP* document structure, composition and order, it may be logical to make the first piece of documentation the *ConOps*.

It would not be appropriate for this handbook to describe a singular way to develop and structure the *SSP*. What this handbook recommends is to develop and write the *SSP* with the perspective of the *System* managers, architects, engineers, administrators and users in mind. Follow the guidance and develop the *SSP* into an initial version, then as an organization, analyze the question: "If the *SSP* were the only reference source disseminated to the roles listed above, would the personnel in those roles be able to carry out their respective responsibilities of the *Information System*?" Now, consider that the 'ease' by which an organization can answer a 'yes' to that question might be in proportion to how effective the *SSP* truly is.

In the *SSP*, the organization should "provide a thorough description of how all the minimum security *controls* in the applicable baseline are being implemented or planned to be implemented."[11] Include titles of the security controls, and how they are "…being implemented or planned to be implemented."[12] Consider applicable scoping guidance and tailoring in the *SSP*, and also include roles and responsible personnel.[13]

POLICIES AND PROCEDURES

If you have ever had to rely on a well written *Standard Operating Procedure (SOP)* or prescribed *Tactics Techniques and Procedures (TTPs)* to perform your daily tasks, then you might already understand the importance of policies and procedures. It might be helpful to think of the *System Security Plan* as a security focused *TTP*. The *SSP* is really the foundational document package that meets the administrative requirements of SP 800-171.

Table 3: The SP 800-171 Security Requirements Families

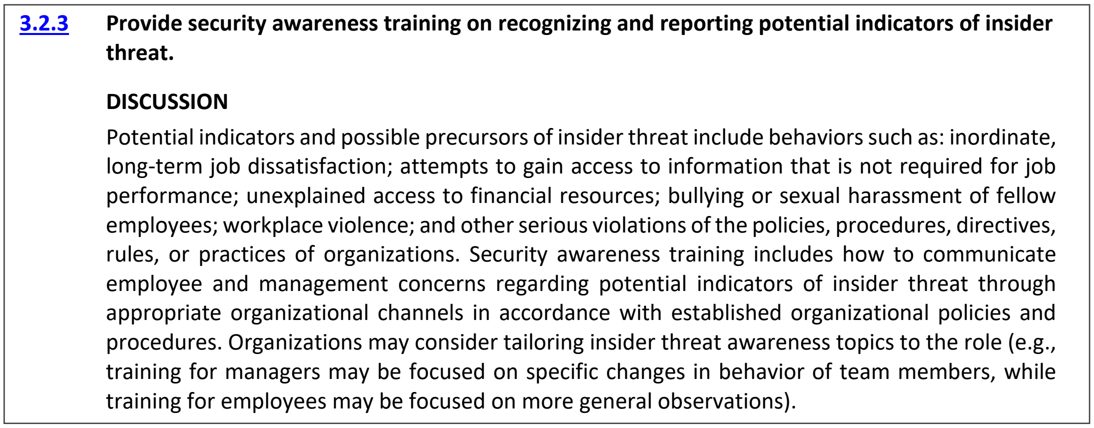
Family	Family
Access Control	Media Protection
Awareness and Training	Personnel Security
Audit and Accountability	Physical Protection
Configuration Management	Risk Assessment
Identification and Authentication	Security Assessment
Incident Response	System and Communications Protection
Maintenance	System and Infromation Integrity

Source: NIST SP 800-171r2

SP 800-171 describes 14 families of security requirements (Figure 1) which breaks down to 110 total requirements. Create an *SSP* that has written policies and/or procedures for all 110 requirements. Doing this aides the management and operation of the System as well as the assessment.

The following example of an organizational policy statement examines the 3.2.3 requirement from SP 800-171. The requirement states, “Provide security awareness training on recognizing and reporting potential indicators of insider threat.” Figure 1 shows the requirement as written in SP 800-171, while Figure 2 shows an example policy statement that might be documented and disseminated by an organization.

Figure 1: The SP 800-171, 3.2.3 requirement



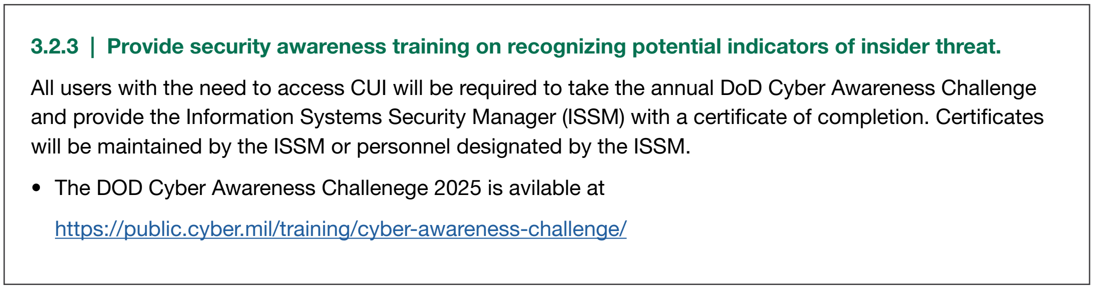
3.2.3 **Provide security awareness training on recognizing and reporting potential indicators of insider threat.**

DISCUSSION

Potential indicators and possible precursors of insider threat include behaviors such as: inordinate, long-term job dissatisfaction; attempts to gain access to information that is not required for job performance; unexplained access to financial resources; bullying or sexual harassment of fellow employees; workplace violence; and other serious violations of the policies, procedures, directives, rules, or practices of organizations. Security awareness training includes how to communicate employee and management concerns regarding potential indicators of insider threat through appropriate organizational channels in accordance with established organizational policies and procedures. Organizations may consider tailoring insider threat awareness topics to the role (e.g., training for managers may be focused on specific changes in behavior of team members, while training for employees may be focused on more general observations).

Source: NIST SP 800-171r2

Figure 2: Example organizational policy statement



3.2.3 | Provide security awareness training on recognizing potential indicators of insider threat.

All users with the need to access CUI will be required to take the annual DoD Cyber Awareness Challenge and provide the Information Systems Security Manager (ISSM) with a certificate of completion. Certificates will be maintained by the ISSM or personnel designated by the ISSM.

- The DOD Cyber Awareness Challenege 2025 is avilable at

  https://public.cyber.mil/training/cyber-awareness-challenge/

CONFIGURING TO A STANDARD

The goal here is to implement the technical configurations that meet the requirements of SP 800-171. This is also where a proper self-assessment[14] becomes critical. However strong or weak an organization might consider its defenses, a self-assessment will identify two key things:

- What technical requirements are the organization meeting with the current configuration? Or what controls are implemented.
- What technical requirements are the organization NOT meeting with the current configuration? Or what controls need to be implemented.

Post self-assessment, weaknesses or deficiencies should be documented in the *Plan of Action & Milestones (POA&M.)*[15] It is important to understand the *POA&M* is a useful tool or mechanism to track progress towards compliance. The due diligence to identify gaps and subsequently close them is documented primarily with the *POA&M*.

For every *System*, the technical configurations will vary. Fortunately, there are many vendor products on the market that provide solutions for meeting technical requirements. In many cases, vendor products have capabilities and user interfaces designed to more easily meet technical standards, to include NIST. If a vendor solution is purchased, it still must be configured to align with the requirements. An implemented vendor solution is great, but that does not necessarily mean that implementation meets the configuration requirements of CMMC. Best practice is to conduct a self-assessment after a vendor solution is implemented.

The NIST Special Publication 800 Series

There may be times during the process where SP 800-171 alone does not provide enough guidance on how to specifically meet a requirement or implement a *control*. The SP 800-171 is designed to reference other NIST special publications. They are extremely useful in scenarios where more detailed information is needed. The 800 series has been in existence since 1990 and "*…reports on the Information Technology Laboratory's research, guidelines, and outreach efforts in computer security, and its collaborative activities with industry, government, and academic organizations.*"[16]

This handbook will feature two other NIST SPs as they are some conceptual basis of SP 800-171. These SPs are NIST SP 800-53 Revision 5: *Security and Privacy Controls for Information Systems and Organization* and *NIST SP 800-160: NIST SP 800-160v1r1: Engineering Trustworthy Secure Systems.*

Table 4: SP 800-53r5 and SP 800-160v1r1 Characteristics

SP 800-53r5	SP 800-160v1r1
• Mappable to SP 800-171. • "*…establishes controls for systems and organizations. The controls can be implemented within any organization or system that processes, stores, or transmits information.*"[17] • Enables the use of the Control Correlation Identifier (CCI) that "*bridges the gap between high-level policy expressions and low-level technical implementations.*"[18]	• Expanded guidance applicable to SP 800-171 requirements for secure engineering principles. • "*The system life cycle processes described in this publication can take advantage of any system or software development methodology.*"[19] • "*The processes can be applied recursively, iteratively, concurrently, sequentially, or in parallel and to any system regardless of its size, complexity, purpose, scope, operational environment, or special nature.*"[20]

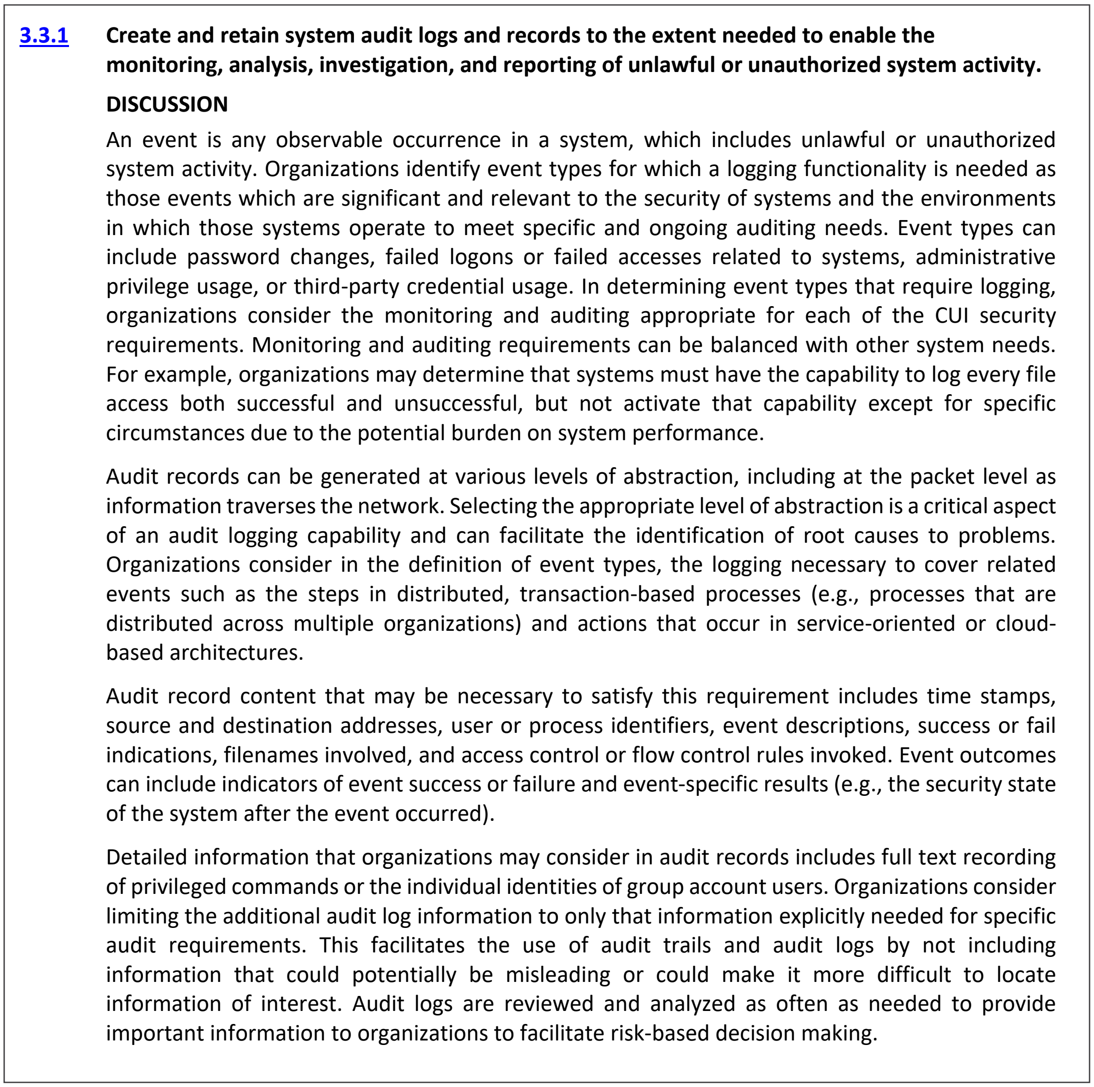
NIST SP 800-53R5: SECURITY AND PRIVACY CONTROLS FOR INFORMATION SYSTEMS AND ORGANIZATIONS

SP 800-171 is effectively a baseline of security *controls*. "*The derived security requirements, which supplement the basic security requirements, are taken from the security controls in [SP 800-53].*" Appendix D in SP 800-171 provides "a mapping of the basic and derived security requirements to the security controls in [SP 800-53]."[22]
As a practitioner, knowledge of the SP 800-53 becomes foundational within SP 800-171.

For someone who has previous experience using SP 800-53, the correlations may already be understood. Whereas, for someone who is beginning with SP 800-171, the picture might not fully be clear. In either scenario, the mapping table in appendix D will be helpful.

Figure 3 is an example of SP 800-171 requirement 3.3.1 from the Audit and Accountability family. While SP 800-171 does provide further guidance in a discussion section of the requirement (not dissimilar to SP 800-53), the question of what specific content an audit record should contain is not completely answered.

Figure 3: SP 800-171 Audit and Accountability Requirement 3.3.1



3.3.1 **Create and retain system audit logs and records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful or unauthorized system activity.**

DISCUSSION

An event is any observable occurrence in a system, which includes unlawful or unauthorized system activity. Organizations identify event types for which a logging functionality is needed as those events which are significant and relevant to the security of systems and the environments in which those systems operate to meet specific and ongoing auditing needs. Event types can include password changes, failed logons or failed accesses related to systems, administrative privilege usage, or third-party credential usage. In determining event types that require logging, organizations consider the monitoring and auditing appropriate for each of the CUI security requirements. Monitoring and auditing requirements can be balanced with other system needs. For example, organizations may determine that systems must have the capability to log every file access both successful and unsuccessful, but not activate that capability except for specific circumstances due to the potential burden on system performance.

Audit records can be generated at various levels of abstraction, including at the packet level as information traverses the network. Selecting the appropriate level of abstraction is a critical aspect of an audit logging capability and can facilitate the identification of root causes to problems. Organizations consider in the definition of event types, the logging necessary to cover related events such as the steps in distributed, transaction-based processes (e.g., processes that are distributed across multiple organizations) and actions that occur in service-oriented or cloud-based architectures.

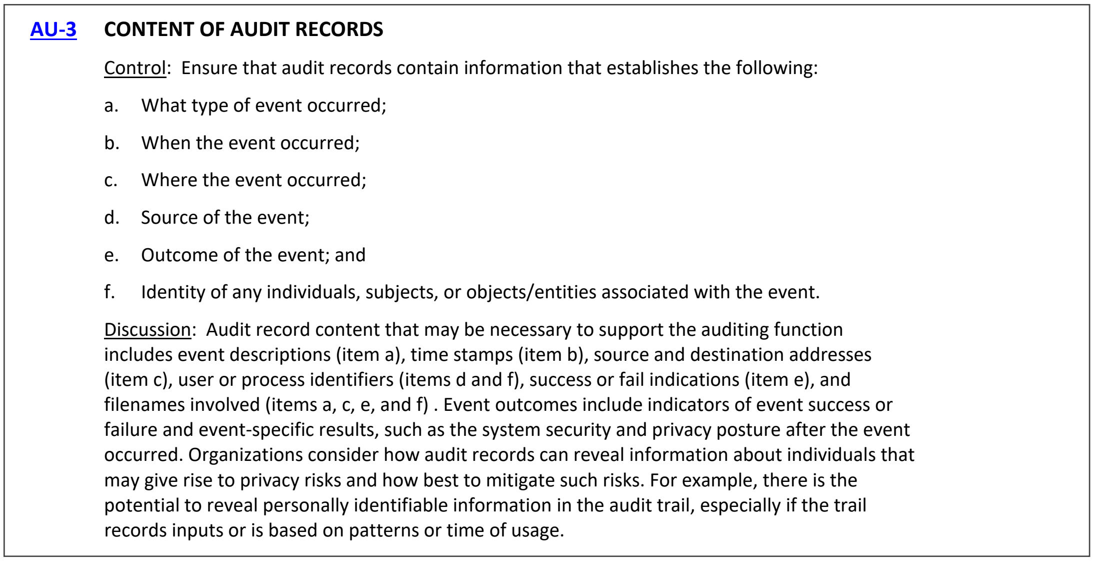
Audit record content that may be necessary to satisfy this requirement includes time stamps, source and destination addresses, user or process identifiers, event descriptions, success or fail indications, filenames involved, and access control or flow control rules invoked. Event outcomes can include indicators of event success or failure and event-specific results (e.g., the security state of the system after the event occurred).

Detailed information that organizations may consider in audit records includes full text recording of privileged commands or the individual identities of group account users. Organizations consider limiting the additional audit log information to only that information explicitly needed for specific audit requirements. This facilitates the use of audit trails and audit logs by not including information that could potentially be misleading or could make it more difficult to locate information of interest. Audit logs are reviewed and analyzed as often as needed to provide important information to organizations to facilitate risk-based decision making.

Source: NIST SP 800-171r2

Figure 4 shows AU-3 from SP 800-53 which maps to requirement 3.3.1 of SP 800-171 and answers the question of what content an audit record should contain.

Figure 4: SP 800-53 Audit and Accountability Control AU-3



AU-3 **CONTENT OF AUDIT RECORDS**

Control: Ensure that audit records contain information that establishes the following:

a. What type of event occurred;

b. When the event occurred;

c. Where the event occurred;

d. Source of the event;

e. Outcome of the event; and

f. Identity of any individuals, subjects, or objects/entities associated with the event.

Discussion: Audit record content that may be necessary to support the auditing function includes event descriptions (item a), time stamps (item b), source and destination addresses (item c), user or process identifiers (items d and f), success or fail indications (item e), and filenames involved (items a, c, e, and f) . Event outcomes include indicators of event success or failure and event-specific results, such as the system security and privacy posture after the event occurred. Organizations consider how audit records can reveal information about individuals that may give rise to privacy risks and how best to mitigate such risks. For example, there is the potential to reveal personally identifiable information in the audit trail, especially if the trail records inputs or is based on patterns or time of usage.

Source: NIST SP 800-53r5

For the 3.3.1 requirement, almost any modern Security Information and Event Management (SIEM) solution can be configured to meet it, and SP 800-53 can help clarify how the organization aligns to a configurable standard. These mappings become helpful throughout the 110 requirements in SP 800-171. SP 800-53 is helpful for the implementation of SP 800-171, that is by design.

A tool called STIG Viewer, created by the Defense Information Systems Agency (DISA), may be helpful when standardizing configurations. The tool uses what are called Secure Technical Implementation Guidelines (STIGs) and Security Requirements Guides (SRGs) and was developed to support the Risk Management Framework (RMF) which leverages SP 800-53 controls. Along with the Control Correlation Identifier (CCI), an organization can leverage STIG Viewer to identify secure, compliant configurations. "*The STIG, once written, will reflect what a specific product CAN do, in a specific release and possible patch level. Published STIGs will only contain requirements that fall into the 'applicable and configurable' category.*"[23]

Download SP 800-53 here: https://csrc.nist.gov/pubs/sp/800/53/r5/upd1/final.

Download STIG Viewer here: https://public.cyber.mil/stigs/srg-stig-tools/.

Download the CCI list here: https://public.cyber.mil/stigs/cci/.

NIST SP 800-160V1R1: *ENGINEERING TRUSTWORTHY SECURE SYSTEMS*

SP 800-160v1 is useful in the CMMC process because like SP 800-53, concepts and principles in SP 800-171 are derived from SP 800-160v1. There are important security requirements described in SP 800-171 that align to specific principles for trustworthy security design described in SP 800-160v1. Furthermore, SP 800-171 requirement 3.13.2 in the System and Communications Protection family explicitly states to employ these principles. One helpful characteristic of the principles described in SP 800-160v1 is that they "*represent the end objectives that the system must satisfy for trustworthy control of adverse effects.*"[25]

Table 5: Requirements in SP 800-171 that correlate to principles in SP 800-160v1

CUI Protection Requirement (Source: SP 800-171)	Principle or Concept (Source: SP 800-160v1r1)
3.1.4: Separate the duties of individuals to reduce the risk of malevolent activity without collusion.	E.10. Distributed Privilege Principle: Multiple authorized entities act in a coordinated manner before an operation on the system is allowed to occur.
3.1.5: Employ the principle of least privilege, including for specific security functions and privileged accounts.	E.16. Least Privilege Principle: Each system element is allocated privileges that are necessary to accomplish its specified functions but no more.
3.4.6: Employ the principle of least functionality by configuring organizational systems to provide only essential capabilities.	E.14. Least Functionality Principle: Each system element has the capability to accomplish its required functions but no more.
Developed Layered Protections.[26]	E.9. Defense In Depth Principle: Loss is prevented or minimized by employing multiple coordinated mechanisms.
Delineating physical and logical security boundaries.[27]	E.2. Clear Abstractions Principle: The abstractions used to characterize the system are simple, well-defined, accurate, precise, necessary, and sufficient.

Download SP 800-160v1r1 here: https://csrc.nist.gov/pubs/sp/800/160/v1/r1/final

Other Notable NIST SPs

The following is a brief list of NIST SPs that are available to the public and are useful in the CMMC process. This list is not intended to be comprehensive or authoritative; however, they are all officially listed references. Be sure to familiarize the organization with all applicable references specific to the contract(s) that your organization works under.

NIST SP 800-171A: "ASSESSING SECURITY REQUIREMENTS FOR CONTROLLED UNCLASSIFIED INFORMATION"

The implementor, as well as the assessor, may reference the 'alpha' SP of the 800-171.

> *"The assessment procedures are flexible and can be customized to the needs of the organizations and the assessors conducting the assessments. Security assessments can be conducted as self-assessments; independent, third-party assessments; or government-sponsored assessments and can be applied with various degrees of rigor, based on customer-defined depth and coverage attributes. The findings and evidence produced during the security assessments can facilitate risk-based decisions by organizations related to the CUI requirements."*[28]

Download the SP 800-171A here: https://csrc.nist.gov/pubs/sp/800/171/a/final

NIST SP 800-160V2R1: DEVELOPING CYBER-RESILIENT SYSTEMS: A SYSTEMS SECURITY ENGINEERING APPROACH

Explore the concepts of Cyber-Resilience, as well as its constructs and engineering principles. Use it to supplement the previously introduced NIST SP 800-160v1r1: Engineering Trustworthy Secure Systems. Gain an understanding of an organization's programmatic, architectural, operational and threat contexts that may be particularly useful in a *ConOps* or *SSP*.

Download the SP 800-160v2r1 here: https://csrc.nist.gov/pubs/sp/800/160/v2/r1/final

NIST SP 800-30R1: GUIDE FOR CONDUCTING RISK ASSESSMENTS

Referenced in the Risk Assessment requirement of SP 800-171r2,[29] this SP can help an organization frame, assess, respond to, and monitor risk. SP 800-30r1 contains information on semi-qualitative and semi-quantitative approaches, how to make proper risk determinations based on inputs such as impact, likelihood, adversarial and non-adversarial risks, and more.

Download the SP 800-30r1 here: https://csrc.nist.gov/pubs/sp/800/30/r1/final

Assessment Activities

GENERATING AND SECURING ARTIFACTS FOR ASSESSMENTS

"*During control selection and implementation, it is important for organizations to consider the evidence (e.g., Artifacts, documentation) that will be needed to support current and future control assessments.*"[30] Properly maintain and secure *Artifacts* before, during and after the assessment process.

Artifacts or evidence can come in various forms, and each *System* will have its own *Artifacts* to support an assessment. The *SSP* itself will be examined as an *Artifact* for assessment. Screen captures and configuration exports can be helpful for examining technical configurations, although technical configurations may also be tested as opposed to examined. For administrative requirements, documentation will likely be examined, some examples are:

- Published organizational policy (*SSP*/*ConOps*)
- Published organizational procedure sets (infrastructure power up/down, upgrading, updates/patching, scans, etc.)
- Plan of Action and Milestones (*POA&M*)
- Logs (e.g., visitor access, maintenance, training, etc.)
- Inventories and baselines
- Forms (e.g., system access request forms, configuration management request forms, etc.)
- Diagrams (e.g., network, workflow, facility, etc.)

An organization must also secure assessment *Artifacts*. This may seem obvious to some, but in practice it must be explicitly understood. This handbook cannot say what security must be applied to an organization's *Artifacts*. The DFARS does clarify some guidance on Certified Third-Party Assessment Organization (C3PAO) assessment *Artifacts* by saying, "A C3PAO is permitted to possess OSC *CUI* and *Artifacts* during an assessment. CMMC Certified Assessors must use the C3PAO's information technology which has received a CMMC Level 2 certification assessment as stated in § 170.11(b)(7) and any copies of the OSC's original *[A]rtifacts* must be destroyed when the assessment is complete as defined in § 170.9(1)."[31]

In an ideal scenario there would be an equivalent of a data classification guide for each contract to broadly identify data sets that equate to *CUI*. A resource like this can answer the question of "what specific information is stored, processed, and/or transmitted on this *Covered Contractor Information System*?" That question should not be assumed easy to answer over the course of a *System* life cycle, and a guide for *CUI* data sets can help. When it comes to assessment *Artifacts*, it might be helpful to have a policy statement in the *SSP* on how the organization secures them.

HITTING THE TARGET: SUBMITTAL, APPROVAL AND CERTIFICATION

The prescribed NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 is how the *System* will be assessed. Referencing the official assessment methodology throughout the implementation process is highly recommended. In doing so, you can more effectively align your organization's *System* to the requirements.

> *"DFARS provision 252.204-7019 complements DFARS clause 252.204-7012 by requiring contractors to have a NIST SP 800-171 assessment (basic, medium, or high) according to NIST SP 800-171 DoD Assessment Methodology. Assessment scores must be reported to the Department via SPRS. SPRS scores must be submitted by the time of contract award and not be more than three years old."*[32]

An assessor may examine, interview, and test to determine whether or not a control is being implemented, and requirements are met.

Table 6: Assessment Methods

Assessment Method	Process and Purpose
Examine	The process of reviewing, inspecting, observing, studying, or analyzing assessment objects (i.e., specifications, mechanisms, activities). The purpose of the examine method is to facilitate understanding, achieve clarification, or obtain evidence.
Interview	The process of holding discussions with individuals or groups of individuals to facilitate understanding, achieve clarification, or obtain evidence.
Test	The process of exercising assessment objects (i.e., activities, mechanisms) under specified conditions to compare actual with expected behavior.

Source: NIST SP 800-171A

As *controls* are implemented to meet requirements, consider how the implementation will be proved to an assessor. Conduct self-assessments by examination, interviews and tests and according to the prescribed methodology. Conducting a proper self-assessment should be considered an important activity when it comes to achieving CMMC Level 2 certification. Passing a proper self-assessment can bring high assurance to an organization that they will in turn pass a C3PAO assessment and allow for the storage, processing, and transmission of *CUI*, fulfilling contractual requirements and supporting the organization's mission and business goals.

Developer Bio

Eric Cataline is an experienced professional with over 15 years in cybersecurity, network operations, and DoD communications networks. A former Army service member, Cataline served on active duty from 2005 to 2011, primarily stationed out of Fort Huachuca, AZ, where he contributed to the Warfighter Information Network – Tactical (WIN-T).

During his military service, Cataline supported tactical and strategic communications assets and had assignments in South Korea, Kuwait, Bahrain and Iraq. He was a key contributor to the engineering and procedural development for the transition of Camp Victory's tactical communications before its closure in December 2011.

After leaving active duty, Cataline continued as a cleared civilian contractor and WIN-T Instructor. In the role, he trained military units on the operation and maintenance of newly fielded network equipment such as Command Post Nodes, Joint Network Nodes, and Hub Nodes, while also helping establish and lead the WIN-T regional training site in Fort Drum, NY.

Cataline then worked as an Information Systems Security Engineer, implementing NIST 800-53 security controls on classified networks supporting operational and DevOps ISR systems. He was responsible for technical configurations, policy writing, and supporting compliance with the National Industrial Security Program Operating Manual. Cataline helped successfully achieve ATOs on multiple systems under the NIST RMF and assisted numerous organizations through DCSA assessments and DoD Command Cyber Readiness Inspections.

Currently, Cataline manages Cadre's professional engineering services, drawing on his extensive background in tactical network operations, information security, and systems engineering. Cataline remains dedicated to enhancing and securing Cadre clients.

References

Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations:
800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2
https://doi.org/10.6028/NIST.SP.800-171r2

Enhanced Security Requirements for Protecting Controlled Unclassified Information:
National Institute of Standards and Technology Special Publication 800-172
https://doi.org/10.6028/NIST.SP.800-172

Security and Privacy Controls for Information Systems and Organizations:
800-53r5: National Institute of Standards and Technology Special Publication 800-53, Revision 5
https://doi.org/10.6028/NIST.SP.800-53r5

Engineering Trustworthy Secure Systems:
800-160v1r1: Ross R, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1.
https://doi.org/10.6028/NIST.SP.800-160v1r1

Developing Cyber-Resilient Systems:
800-160v2r1: National Institute of Standards and Technology Special Publication 800-160, Vol. 2, Rev. 1
https://doi.org/10.6028/NIST.SP.800-160v2r1

Guide for Conducting Risk Assessments:
NIST Special Publication 800-30, 95 pages
https://csrc.nist.gov/pubs/sp/800/30/r1/final

Assessing Security Requirements for Controlled Unclassified Information:
800-171A: National Institute of Standards and Technology Special Publication 800-171A
https://doi.org/10.6028/NIST.SP.800-171A

Cybersecurity Maturity Model Certification (CMMC) Program:
Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905:
https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

Defense Federal Acquisition Regulation Supplement Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting:
Defense Federal Acquisition Regulation Supplement, Part 252, Sub-part 252.2, Sub-topic, 252.204: 252.204-7012:
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

Defense Federal Acquisition Regulation Supplement Clause 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements.
Defense Federal Acquisition Regulation Supplement, Part 252, Sub-part 252.2, Sub-topic, 252.204: 252.204-7019:
https://www.acquisition.gov/dfars/252.204-7019-notice-nistsp-800-171-dod-assessment-requirements.

Defense Federal Acquisition Regulation Supplement Clause 252.204-7020, NIST SP 800-171DoD Assessment Requirements.
Defense Federal Acquisition Regulation Supplement, Part 252, Sub-part 252.2, Sub-topic, 252.204: 252.204-7020:
https://www.acquisition.gov/dfars/252.204-7020-nist-sp-800-171dod-assessment-requirements.

Glossary

ADEQUATE SECURITY

Protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

Source: DFARS: 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting. Change Number: DFARS Change 01/17/2025.

ARTIFACTS

Work products that are produced and used during a project to capture and convey information (e.g., models, source code).

Source: NIST SP 800-160v1r1: Engineering Trustworthy Secure Systems.

CONCEPT OF OPERATIONS (ConOps or CONOPS)

Verbal and graphic statement, in broad outline, of an organization's assumptions or intent in regard to an operation or series of operations of new, modified, or existing organizational systems.

Source: NIST SP 800-160v1r1: Engineering Trustworthy Secure Systems.

CONTRACTOR COVERED INFORMATION SYSTEM

An unclassified information system that is owned, or operated by or for, a contractor and that processes, stores, or transmits covered defense information.

Source: DFARS: 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting. Change Number: DFARS Change 01/17/2025.

CONTROL (SECURITY CONTROL)

The methods, policies, and procedures—manual or automated—used by an organization to safeguard and protect assets, promote efficiency, or adhere to standards. A measure that is modifying risk.

Source: CMMC Glossary and Acronyms 2.0

CONTROLLED UNCLASSIFIED INFORMATION (CUI)

Information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended.

Source: CMMC Glossary and Acronyms 2.0

COVERED DEFENSE INFORMATION

A term used to identify information that requires protection under DFARS Clause 252.204-7012. Unclassified controlled technical information (CTI) or other information, as described in the CUI Registry, that requires safeguarding, or dissemination controls pursuant to and consistent with law, regulations, and Government wide policies and is:

- Marked or otherwise identified in the contract, task order, or delivery order and provided to contractor by or on behalf of, DoD in support of the performance of the contract; OR
- Collected, developed, received, transmitted, used, or stored by—or on behalf of—the contractor in support of the performance of the contract.

Source: CMMC Glossary and Acronyms 2.0

CYBERSECURITY

Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation.

Source: CMMC Glossary and Acronyms 2.0

INFORMATION SYSTEM (SYSTEM)

A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Source: CMMC Glossary and Acronyms 2.0

STANDARD OPERATING PROCEDURES (SOP)

A set of instructions used to describe a process or procedure that performs an explicit operation or explicit reaction to a given event.

Source: NIST Glossary of Terms

SYSTEM BOUNDARY

The scope of the system and environment being assessed. All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected. The System Boundary is equivalent to the defined CMMC Assessment Scope.

Source: CMMC Glossary and Acronyms 2.0

SYSTEM SECURITY PLAN (SSP)

The formal document prepared by the information system owner (or common security controls owner for inherited controls) that provides an overview of the security requirements for the system and describes the security controls in place or planned for meeting those requirements. The plan can also contain as supporting appendices or as references, other key security-related documents such as a risk assessment, privacy impact assessment, system interconnection agreements, contingency plan, security configurations, configuration management plan, and incident response plan.

Source: CMMC Glossary and Acronyms 2.0

TACTICS, TECHNIQUES AND PROCEDURES (TTP)

The behavior of an actor. A tactic is the highest-level description of the behavior; techniques provide a more detailed description of the behavior in the context of a tactic; and procedures provide a lower-level, highly detailed description of the behavior in the context of a technique.

Source: NIST Special Publication 800-172: Enhanced Security Requirements for Protecting Controlled Unclassified Information.

Endnotes

[1] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: SUPPLEMENTARY INFORMATION: History of the Program:
https://www.federalregister.gov/d/2024-22905/p-6

[2] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: SUPPLEMENTARY INFORMATION: History of the Program:
https://www.federalregister.gov/d/2024-22905/p-11

[3] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: SUPPLEMENTARY INFORMATION: History of the Program:
https://www.federalregister.gov/d/2024-22905/p-13

[4] Defense Federal Acquisition Regulation Supplement, Part 252, Sub-part 252..2, Sub-topic, 252.204: 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting: 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting: (a) Definitions: Contractor Covered Information System:
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[5] Defense Federal Acquisition Regulation Supplement, Part 252, Sub-part 252..2, Sub-topic, 252.204: 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting: 252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting: (a) Definitions: Adequate Security:
https://www.acquisition.gov/dfars/252.204-7012-safeguarding-covered-defense-information-and-cyber-incident-reporting.

[6] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: About CMMC:
https://dodcio.defense.gov/cmmc/About/

[7] 800-160v1r1: Ross R, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1: Glossary: Concept of Operations: Note 2:
https://doi.org/10.6028/NIST.SP.800-160v1r1

[8] NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1: Assessment Scoring Template "*The absence of a system security plan would result in a finding that 'an assessment could not be completed due to incomplete information and noncompliance with DFARS clause 252.204-7012.*"':
https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf

[9] 800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2: Security Assessment: 3.12.4:
https://doi.org/10.6028/NIST.SP.800-171r2

[10] 800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2: Security Assessment: 3.12.4: Discussion:
https://doi.org/10.6028/NIST.SP.800-171r2

[11] National Institute of Standards and Technology Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems: Appendix A: Minimum Security Controls:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

[12] National Institute of Standards and Technology Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems: Appendix A: Minimum Security Controls:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

[13] National Institute of Standards and Technology Special Publication 800-18, Revision 1, Guide for Developing Security Plans for Federal Information Systems: Appendix A: Minimum Security Controls:
https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-18r1.pdf

[14] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: "*The security requirements for a CMMC Level 2 self-assessment and a CMMC Level 2 certification assessment are the same, the only difference in these assessments is whether it is performed by the OSA or by an independent C3PAO.*"
https://www.federalregister.gov/d/2024-22905/p-355

[15] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: Current Status of the CMMC Program:
https://www.federalregister.gov/d/2024-22905/p-36

[16] NIST Information Technology Laboratory: NIST Special Publication 800-series General Information
https://www.nist.gov/itl/publications-0/nist-special-publication-800-series-general-information

[17] 800-53r5: National Institute of Standards and Technology Special Publication 800-53, Revision 5: Purpose and Applicability:
https://doi.org/10.6028/NIST.SP.800-53r5

[18] DoD Cyber Exchange Public: Control Correlation Identifier:
https://public.cyber.mil/stigs/cci/

[19] 800-160v1r1: Ross R, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1: How to Use this Publication:
https://doi.org/10.6028/NIST.SP.800-160v1r1

[20] 800-160v1r1: Ross R, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1: How to Use this Publication:
https://doi.org/10.6028/NIST.SP.800-160v1r1

[21] 800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2: Development of Security Requirements:
https://doi.org/10.6028/NIST.SP.800-171r2

[22] 800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2: Appendix D: Mapping Tables:
https://doi.org/10.6028/NIST.SP.800-171r2

[23] DoD Cyber Exchange Public: Security Technical Implementation Guides (STIGs): Vendor Process:
https://public.cyber.mil/stigs/vendor-process/

[24] 800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2: Security Assessment: 3.12.2: "*Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.*":
https://doi.org/10.6028/NIST.SP.800-171r2

[25] 800-160v1r1: Ross R, McEvilley M, Winstead M (2022) Engineering Trustworthy Secure Systems. (National Institute of Standards and Technology, Gaithersburg, MD), NIST Special Publication (SP) NIST SP 800-160v1r1: Appendix E:
https://doi.org/10.6028/NIST.SP.800-160v1r1

[26] 800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2: 3.13.2 Example:
https://doi.org/10.6028/NIST.SP.800-171r2

[27] 800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2: 3.13.2 Example:
https://doi.org/10.6028/NIST.SP.800-171r2

[28] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: Summary of Provisions Contained in This Rule:
https://www.federalregister.gov/d/2024-22905/p-88

[29] 800-171r2: National Institute of Standards and Technology Special Publication 800-171, Revision 2: Risk Assessment: 3.11.1: Discussion:
https://doi.org/10.6028/NIST.SP.800-171r2

[30] 800-53r5: National Institute of Standards and Technology Special Publication 800-53, Revision 5: The Fundamentals: Trustworthiness and Assurance:
https://doi.org/10.6028/NIST.SP.800-53r5

[31] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: The CMMC Ecosystem Roles, Responsibilities and Requirements: C3PAO:
https://www.federalregister.gov/d/2024-22905/p-428

[32] CMMC Final Rule: Department of Defense, Office of the Secretary, 32 CFR Part 170, [Docket ID: DoD-2023-OS-0063], RIN 0790-AL49, Document Citation: 89 FR 83092, Document Number: 2024-22905: Overview of Revised CMMC Program Current Requirements for Defense Contractors and Subcontractors:
https://www.federalregister.gov/d/2024-22905/p-51