Access Control (AC) — the process of granting or denying specific requests to obtain and use information and related information processing services; and/or entry to specific physical facilities (*e.g.,* Federal buildings, military establishments, or border crossing entrances), as defined in FIPS PUB 201-3 Jan2002 (incorporated by reference, see § 170.2).
32 CFR 170.4

Accreditation — a status pursuant to which a CMMC Assessment and Certification Ecosystem member (person or organization), having met all criteria for the specific role they perform including required ISO/IEC accreditations, may act in that role as set forth in § 170.8 for the Accreditation Body and § 170.9 for C3PAOs. (CMMC-custom term)
32 CFR 170.4

Accreditation Body — is defined in § 170.8 and means the one organization DoD contracts with to be responsible for authorizing and accrediting members of the CMMC Assessment and Certification Ecosystem, as required. The Accreditation Body must be approved by DoD. At any given point in time, there will be only one Accreditation Body for the DoD CMMC Program. (CMMC-custom term)
32 CFR 170.4

Adequate Security — protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.
DFARS 252.204-7012

Advanced Persistent Threat (APT) — an adversary that possesses sophisticated levels of expertise and significant resources that allow it to create opportunities to achieve its objectives by using multiple attack vectors (*e.g.,* cyber, physical, and deception). These objectives typically include establishing and extending footholds within the information technology infrastructure of the targeted organizations for purposes of exfiltrating information, undermining or impeding critical aspects of a mission, program, or organization; or positioning itself to carry out these objectives in the future. The advanced persistent threat pursues its objectives repeatedly over an extended period-of-time, adapts to defenders' efforts to resist it, and is determined to maintain the level of interaction needed to execute its objectives, as is defined in NIST SP 800-39 Mar2011 (incorporated by reference, see § 170.2).
32 CFR 170.4

Affirming Official — the senior level representative from within each Organization Seeking Assessment (OSA) who is responsible for ensuring the OSA's compliance with the CMMC Program requirements and has the authority to affirm the OSA's continuing compliance with the specified security requirements for their respective organizations. (CMMC-custom term)
32 CFR 170.4

Agency — (also Federal agency, executive agency, executive branch agency) is any “executive agency,” as defined in 5 U.S.C. 105; the United States Postal Service; and any other independent entity within the executive branch that designates or handles CUI.
32 CFR 2002.4

Agency CUI Policies — are the policies the agency enacts to implement the CUI Program within the agency. They must be in accordance with the Order, this part, and the CUI Registry and approved by the CUI EA.
32 CFR 2002.4

Agreements and Arrangements — are any vehicle that sets out specific CUI handling requirements for contractors and other information-sharing partners when the arrangement with the other party involves CUI. Agreements and arrangements include, but are not limited to, contracts, grants, licenses, certificates, memoranda of agreement/arrangement or understanding, and information-sharing agreements or arrangements. When disseminating or sharing CUI with non-executive branch entities, agencies should enter into written agreements or arrangements that include CUI provisions whenever feasible (see § 2002.16(a)(5) and (6) for details). When sharing information with foreign entities, agencies should enter agreements or arrangements when feasible (see § 2002.16(a)(5)(iii) and (a)(6) for details).
32 CFR 2002.4

Assessment — the testing or evaluation of security controls to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for an information system or organization, as defined in §§ 170.15 through 170.18. (CMMC-custom term)

> **Level 1 self-assessment** — the term for the activity performed by an OSA to evaluate its own information system when seeking a CMMC Status of Level 1 (Self).
>
> **Level 2 self-assessment** — the term for the activity performed by an OSA to evaluate its own information system when seeking a CMMC Status of Level 2 (Self).
>
> **Level 2 certification assessment** — the term for the activity performed by a C3PAO to evaluate the information system of an OSC when seeking a CMMC Status of Level 2 (C3PAO).
>
> **Level 3 certification assessment** — the term for the activity performed by the DCMA DIBCAC to evaluate the information system of an OSC when seeking a CMMC Status of Level 3 (DIBCAC).
>
> **POA&M closeout self-assessment** — the term for the activity performed by an OSA to evaluate only the NOT MET requirements that were identified with POA&M during the initial assessment, when seeking a CMMC Status of Final Level 2 (Self).
>
> **POA&M closeout certification assessment** — the term for the activity performed by a C3PAO or DCMA DIBCAC to evaluate only the NOT MET requirements that were identified with POA&M during the initial assessment, when seeking a CMMC Status of Final Level 2 (C3PAO) or Final Level 3 (DIBCAC) respectively.
> *32 CFR 170.4*

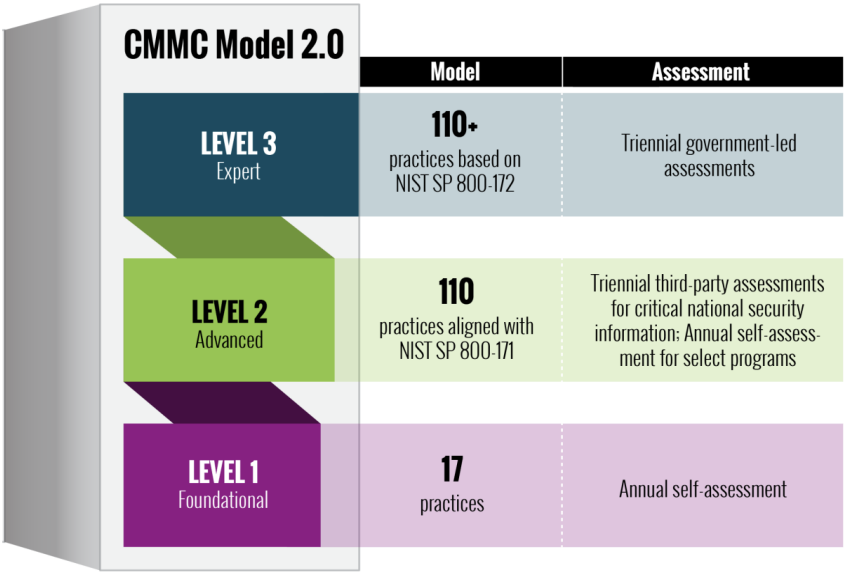

Figure 1. CMMC 2.0 Level Overview

Assessment Findings Report — the final written assessment results by the third-party or government assessment team. The Assessment Findings Report is submitted to the OSC and to the DoD via CMMC eMASS. (CMMC-custom term)
32 CFR 170.4

Assessment Objective (AO) — a set of determination statements that, taken together, expresses the desired outcome for the assessment of a security requirement. Successful implementation of the corresponding CMMC security requirement requires meeting all applicable assessment objectives defined in NIST SP 800-171A Jun2018 (incorporated by reference, see § 170.2) or NIST SP 800-172A Mar2022 (incorporated by reference, see § 170.2). (CMMC-custom term)
32 CFR 170.4

Assessment Team — participants in the Level 2 certification assessment (CMMC Certified Assessors and CMMC Certified Professionals) or the Level 3 certification assessment (DCMA DIBCAC assessors). This does not include the OSC participants preparing for or participating in the assessment. (CMMC-custom term)
32 CFR 170.4

Asset — an item of value to stakeholders. An asset may be tangible (*e.g.,* a physical item such as hardware, firmware, computing platform, network device, or other technology component) or intangible (*e.g.,* humans, data, information, software, capability, function, service, trademark, copyright, patent, intellectual property, image, or reputation). The value of an asset is determined by stakeholders in consideration of loss concerns across the entire system life cycle. Such concerns include but are not limited to business or mission concerns, as defined in NIST SP 800-160 V2R1 (incorporated by reference, see § 170.2).
32 CFR 170.4

Asset Categories — A grouping of assets that process, store or transmit information of similar designation, or provide security protection to those assets. (CMMC-custom term)
32 CFR 170.4

Authentication — Verifying the identity of a user, process, or device, often as a prerequisite to allowing access to resources in an information system.
FIPS PUB 200 Mar2006

Authorization — The right or a permission that is granted to a system entity to access a system resource.
NIST Glossary

Authorized — an interim status during which a CMMC Ecosystem member (person or organization), having met all criteria for the specific role they perform other than the required ISO/IEC accreditations, may act in that role for a specified time as set forth in § 170.8 for the Accreditation Body and § 170.9 for C3PAOs. (CMMC-custom term)
32 CFR 170.4

Authorized Holder —

1. an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with 32 Code of Federal Regulations (CFR) Part 2002.
DoD Mandatory CUI Training - Glossary, CDSE

2. is an individual, agency, organization, or group of users that is permitted to designate or handle CUI, in accordance with this part.
32 CFR 2002.4

Basic Assessment — a contractor's self-assessment of the contractor's implementation of NIST SP 800-171 that—
(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);
(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and
(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.
DFARS 252.204-7020

Capability — a combination of mutually reinforcing controls implemented by technical means, physical means, and procedural means. Such controls are typically selected to achieve a common information security or privacy purpose, as defined in NIST SP 800-37 R2 (incorporated by reference, see § 170.2).
32 CFR 170.4

Classified Information — is information that Executive Order 13526, "Classified National Security Information," December 29, 2009 (3 CFR, 2010 Comp., p. 298), or any predecessor or successor order, or the Atomic Energy Act of 1954, as amended, requires agencies to mark with classified markings and protect against unauthorized disclosure.
32 CFR 2002.4

Cloud Service Provider (CSP) — an external company that provides cloud services based on cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand

network access to a shared pool of configurable computing resources (*e.g.,* networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. This definition is based on the definition for cloud computing in NIST SP 800-145 Sept2011. (CMMC-custom term)
32 CFR 170.4

CMMC Assessment and Certification Ecosystem — means the people and organizations described in subpart C of this part. This term is sometimes shortened to CMMC Ecosystem. (CMMC-custom term)
32 CFR 170.4

CMMC Assessment Scope — the set of all assets in the OSA's environment that will be assessed against CMMC security requirements. (CMMC-custom term)
32 CFR 170.4

CMMC Assessor and Instructor Certification Organization (CAICO) — the organization responsible for training, testing, authorizing, certifying, and recertifying CMMC certified assessors, certified instructors, and certified professionals. (CMMC-custom term)
32 CFR 170.4

CMMC Instantiation of eMASS — a CMMC instance of the Enterprise Mission Assurance Support Service (eMASS), a government owned and operated system. (CMMC-custom term)
32 CFR 170.4

CMMC Security Requirements — the 15 Level 1 requirements listed in the 48 CFR 52.204-21(b)(1), the 110 Level 2 requirements from NIST SP 800-171 R2 (incorporated by reference, see § 170.2), and the 24 Level 3 requirements selected from NIST SP 800-172 Feb2021 (incorporated by reference, see § 170.2).

CMMC Status — the result of meeting or exceeding the minimum required score for the corresponding assessment. The CMMC Status of an OSA information system is officially stored in SPRS and additionally presented on a Certificate of CMMC Status, if the assessment was conducted by a C3PAO or DCMA DIBCAC. The potential CMMC Statuses are outlined in the paragraphs that follow. (CMMC-custom term)

Final Level 1 (Self) is defined in § 170.15(a)(1) and (c)(1). (CMMC-custom term)
Conditional Level 2 (Self) is defined in § 170.16(a)(1)(ii). (CMMC-custom term)
Final Level 2 (Self) is defined in § 170.16(a)(1)(iii). (CMMC-custom term)
Conditional Level 2 (C3PAO) is defined in § 170.17(a)(1)(ii). (CMMC-custom term)
Final Level 2 (C3PAO) is defined in § 170.17(a)(1)(iii). (CMMC-custom term)
Conditional Level 3 (DIBCAC) is defined in § 170.18(a)(1)(ii). (CMMC-custom term)
Final Level 3 (DIBCAC) is defined in § 170.18(a)(1)(iii). (CMMC-custom term)
32 CFR 170.4

CMMC Status Date — the date that the CMMC Status results are submitted to SPRS or the CMMC instantiation of eMASS, as appropriate. The date of the Conditional CMMC Status will remain as the CMMC Status Date after a successful POA&M closeout. A new date is not set for a Final that follows a Conditional. (CMMC-custom term)
32 CFR 170.4

CMMC Third-Party Assessment Organization (C3PAO) — an organization that has been authorized or accredited by the Accreditation Body to conduct Level 2 certification assessments and has the roles and responsibilities identified in § 170.9. (CMMC-custom term)
32 CFR 170.4

Compromise — disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.
DFARS 252.204-7012

Contractor — any individual or other legal entity that is awarded a Federal Government contract or subcontract under a Federal Government contract. The term *contractor* refers to both a prime contractor and all of its subcontractors of any tier on a contract with the Federal Government. The term *contractor* includes lessors and lessees, as well as employers of workers performing on covered Federal contracts whose wages are calculated pursuant to special certificates issued under 29 U.S.C. 214(c). The term *employer* is used interchangeably with the terms *contractor* and *subcontractor* in various sections of this part. The U.S. Government, its agencies, and instrumentalities are not contractors, subcontractors, employers, or joint employers for purposes of compliance with the provisions of the Executive Order.
29 CFR 10.2

Contractor Attributional/Proprietary Information — technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information would meet the criteria, if disseminated, for distribution statements B through F using the criteria set forth in DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.
DFARS 252.204-7012

Contractor Risk Managed Asset (CRMA) — Assets that can, but are not intended to, process, store, or transmit CUI because of security policy, procedures, and practices in place • Assets are not required to be physically or logically separated from CUI assets.
32 CFR 170.4

Controlled Environment — is any area or space an authorized holder deems to have adequate physical or procedural controls (e.g., barriers or managed access controls) to protect CUI from unauthorized access or disclosure.
32 CFR 2002.4

Control Level — is a general term that indicates the safeguarding and disseminating requirements associated with CUI Basic and CUI Specified.
32 CFR 2002.4

Controlled Unclassified Information (CUI) —

1. is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination

controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.
32 CFR 2002.4(h)

2. Unclassified information requiring safeguarding and dissemination controls, consistent with applicable law, regulation, or government-wide policy.
DoD Mandatory CUI Training - Glossary, CDSE

3. is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls. However, CUI does not include classified information (see paragraph (e) of this section) or information a non-executive branch entity possesses and maintains in its own systems that did not come from, or was not created or possessed by or for, an executive branch agency or an entity acting for an agency. Law, regulation, or Government-wide policy may require or permit safeguarding or dissemination controls in three ways: Requiring or permitting agencies to control or protect the information but providing no specific controls, which makes the information CUI Basic; requiring or permitting agencies to control or protect the information and providing specific controls for doing so, which makes the information CUI Specified; or requiring or permitting agencies to control the information and specifying only some of those controls, which makes the information CUI Specified, but with CUI Basic controls where the authority does not specify.
32 CFR 2002.4

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. Note: controls include any process, policy, device, practice, or other actions which modify risk. See also Security Control.
CMMC 2.0 Glossary (now deprecated).

*Editor comment: In the CMMC lexicon we commonly refer to the 110 items that NIST SP 800-171 by **three** different names. Control or Security Control derived from Financial Audit and NIST 800-53 common practice. Security Requirements as they are defined and labelled in NIST SP800-171. Finally, as Practices, a term introduced in CMMC 1.0 for this listing. The term Practices is a legacy term no longer used in the Assessment Guides for the purpose of labelling the 110 things that must be done. The Assessment Guides currently use the label, "requirement" for this purpose.*

Controls — are safeguarding or dissemination controls that a law, regulation, or Government-wide policy requires or permits agencies to use when handling CUI. The authority may specify the controls it requires or permits the agency to apply, or the authority may generally require or permit agencies to control the information (in which case, the agency applies controls from the Order, this part, and the CUI Registry).
32 CFR 2002.4

Controlled Unclassified Information Asset (CUIA) — assets that can process, store, or transmit CUI. (CMMC-custom term)
32 CFR 170.4

Covered Contractor 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.
DFARS 252.204-7012

Covered Defense Information (CDI) — unclassified controlled technical information or other information, as described in the Controlled Unclassified Information (CUI) Registry at http://www.archives.gov/cui/registry/category-list.html, that requires safeguarding or dissemination controls pursuant to and consistent with law, regulations, and Governmentwide policies, and is—
(1) Marked or otherwise identified in the contract, task order, or delivery order and provided to the contractor by or on behalf of DoD in support of the performance of the contract; or
(2) Collected, developed, received, transmitted, used, or stored by or on behalf of the contractor in support of the performance of the contract.
DFARS 252.204-7012

CUI Basic —

1. Subset of CUI for which the authorizing law, regulation, or government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in DoDI 5200.48 and the DoD CUI Registry.
   DoD Mandatory CUI Training - Glossary, CDSE

2. is the subset of CUI for which the authorizing law, regulation, or Government-wide policy does not set out specific handling or dissemination controls. Agencies handle CUI Basic according to the uniform set of controls set forth in this part and the CUI Registry. CUI Basic differs from CUI Specified (see definition for CUI Specified in this section), and CUI Basic controls apply whenever CUI Specified ones do not cover the involved CUI.
   32 CFR 2002.4

CUI Categories and Subcategories — those types of information for which laws, regulations, or Government-wide policies require or permit agencies to exercise safeguarding or dissemination controls, and which the CUI EA has approved and listed in the CUI Registry. The controls for any CUI Basic categories and any CUI Basic subcategories are the same, but the controls for CUI Specified categories and subcategories can differ from CUI Basic ones and from each other. A CUI category may be Specified, while some or all of its subcategories may

not be, and vice versa. If dealing with CUI that falls into a CUI Specified category or subcategory, review the controls for that category or subcategory on the CUI Registry. Also consult the agency's CUI policy for specific direction from the Senior Agency Official.
32 CFR 2002.4

CUI Category or Subcategory Markings — the markings approved by the CUI EA for the categories and subcategories listed in the CUI Registry.
32 CFR 2002.4

CUI Executive Agent (EA) — the National Archives and Records Administration (NARA), which implements the executive branch-wide CUI Program and oversees Federal agency actions to comply with the Order. NARA has delegated this authority to the Director of the Information Security Oversight Office (ISOO).
32 CFR 2002.4

CUI Program — the executive branch-wide program to standardize CUI handling by all Federal agencies. The Program includes the rules, organization, and procedures for CUI, established by the Order, this part, and the CUI Registry.
32 CFR 2002.4

CUI Program Manager — an agency official, designated by the agency head or CUI SAO, to serve as the official representative to the CUI EA on the agency's day-to-day CUI Program operations, both within the agency and in interagency contexts.
32 CFR 2002.4

CUI Registry — the online repository for all information, guidance, policy, and requirements on handling CUI, including everything issued by the CUI EA other than this part. Among other information, the CUI Registry identifies all approved CUI categories and subcategories, provides general descriptions for each, identifies the basis for controls, establishes markings, and includes guidance on handling procedures.
32 CFR 2002.4

CUI Senior Agency Official (SAO) — a senior official designated in writing by an agency head and responsible to that agency head for implementation of the CUI Program within that agency. The CUI SAO is the primary point of contact for official correspondence, accountability reporting, and other matters of record between the agency and the CUI EA.
32 CFR 2002.4

CUI Specified —

1. Subset of CUI in which the authorizing law, regulation, or government wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic.
   DoD Mandatory CUI Training - Glossary, CDSE

2. the subset of CUI in which the authorizing law, regulation, or Government-wide policy contains specific handling controls that it requires or permits agencies to use that differ from those for CUI Basic. The CUI Registry indicates which laws, regulations, and Government-wide policies include such specific requirements. CUI Specified controls may be more stringent than, or may simply differ from, those required by CUI Basic; the distinction is that the underlying authority spells out specific controls for CUI Specified information and does not for CUI Basic information. CUI Basic controls apply to those aspects of CUI Specified where the authorizing laws, regulations, and Government-wide policies do not provide specific guidance.

Customer Responsibility Matrix (CRM) — CRM is not explicitly defined in 32CFR170 however it is a critical term and used in 32CFR170 as follows: "customer responsibility matrix (CRM), which describes the responsibilities of the OSA and ESP with respect to the services provided."

32CFR170 also states: "In accordance with § 170.19(c)(2), the OSA's on-premises infrastructure connecting to the CSP's product or service offering is part of the CMMC Assessment Scope, which will also be assessed. As such, the security requirements from the *Customer Responsibility Matrix (CRM)* must be documented or referred to in the OSA's System Security Plan (SSP)." Cybersecurity Maturity Model Certification (CMMC) Program 170.16

The CRM is effectively an expression of "control inheritance." Inheritance is a practice in Federal Risk Management Framework (RMF) and is defined as: "A situation in which a system or application receives protection from security or privacy controls (or portions of controls) that are developed, implemented, assessed, authorized, and monitored by entities other than those responsible for the system or application; entities either internal or external to the organization where the system or application resides. See common control." NIST Glossary

The common practice for a CRM is for that matrix to exist as a spreadsheet or table that maps to the 171 control list or assessment objective list. In general mapping to assessment objectives is considered a superior approach. The mapping should include a description of which security requirements/controls/practices the CSP or ESP meets and the OSA may inherit, which the OSA/OSC must perform on their own, and which are shared. There is no established standard for the construction of a CRM, however a CRM must be provided to assessors as part of the documentation for each CSP and ESP in use by the OSA.

A CRM is sometimes also called a Shared Responsibility Matrix (SRM). 32CFR170 exclusively uses the term CRM. NIST does not use either term.

Cyber Incident — actions taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.
DFARS 252.204-7012

DCMA DIBCAC High Assessment — an assessment that is conducted by Government personnel in accordance with NIST SP 800-171A Jun2018 and leveraging specific guidance in the DoD Assessment Methodology that:
(i) Consists of:

(A) A review of a contractor's Basic Assessment;
(B) A thorough document review;
(C) Verification, examination, and demonstration of a contractor's system security plan to validate that NIST SP 800-171 R2 security requirements have been implemented as described in the contractor's system security plan; and
(D) Discussions with the contractor to obtain additional information or clarification, as needed; and
(ii) Results in a confidence level of “High” in the resulting score. (Source: 48 CFR 252.204-7020).
32 CFR 170.4

Decontrolling — occurs when an authorized holder, consistent with this part and the CUI Registry, removes safeguarding or dissemination controls from CUI that no longer requires such controls. Decontrol may occur automatically or through agency action. See § 2002.18.
32 CFR 2002.4

Defense Industrial Base (DIB) — the Department of Defense, Government, and private sector worldwide industrial complex with capabilities to perform research and development, design, produce, and maintain military weapon systems, subsystems, components, or parts to satisfy military requirements.
32 CFR 236.2

Designating CUI — occurs when an authorized holder, consistent with this part and the CUI Registry, determines that a specific item of information falls into a CUI category or subcategory. The authorized holder who designates the CUI must make recipients aware of the information's CUI status in accordance with this part.
32 CFR 2002.4

Designating Agency — the executive branch agency that designates or approves the designation of a specific item of information as CUI.
32 CFR 2002.4

Digital Media — A form of electronic media where data is stored in digital (as opposed to analog) form.
NIST Glossary

Disseminating — occurs when authorized holders provide access, transmit, or transfer CUI to other authorized holders through any means, whether internal or external to an agency.
32 CFR 2002.4

Document — any tangible thing which constitutes or contains information, and means the original and any copies (whether different from the originals because of notes made on such copies or otherwise) of all writings of every kind and description over which an agency has authority, whether inscribed by hand or by mechanical, facsimile, electronic, magnetic, microfilm, photographic, or other means, as well as phonic or visual reproductions or oral statements, conversations, or events, and including, but not limited to: Correspondence, email, notes, reports, papers, files, manuals, books, pamphlets, periodicals, letters, memoranda,

notations, messages, telegrams, cables, facsimiles, records, studies, working papers, accounting papers, contracts, licenses, certificates, grants, agreements, computer disks, computer tapes, telephone logs, computer mail, computer printouts, worksheets, sent or received communications of any kind, teletype messages, agreements, diary entries, calendars and journals, printouts, drafts, tables, compilations, tabulations, recommendations, accounts, work papers, summaries, address books, other records and recordings or transcriptions of conferences, meetings, visits, interviews, discussions, or telephone conversations, charts, graphs, indexes, tapes, minutes, contracts, leases, invoices, records of purchase or sale correspondence, electronic or other transcription of taping of personal conversations or conferences, and any written, printed, typed, punched, taped, filmed, or graphic matter however produced or reproduced. Document also includes the file, folder, exhibits, and containers, the labels on them, and any metadata, associated with each original or copy. Document also includes voice records, film, tapes, video tapes, email, personal computer files, electronic matter, and other data compilations from which information can be obtained, including materials used in data processing.
32 CFR 2002.4

DoD Assessment Methodology (DoDAM) — documents a standard methodology that enables a strategic assessment of a contractor's implementation of NIST SP 800-171 R2, a requirement for compliance with 48 CFR 252.204-7012. (Source: DoDAM Version 1.2.1)
32 CFR 170.4

Enduring Exception — a special circumstance or system where remediation and full compliance with CMMC security requirements is not feasible. Examples include systems required to replicate the configuration of `fielded' systems, medical devices, test equipment, OT, and IoT. No operational plan of action is required but the circumstance must be documented within a system security plan. Specialized Assets and GFE may be enduring exceptions. (CMMC-custom term)
32 CFR 170.4

Enterprise — an organization with a defined mission/goal and a defined boundary, using information systems to execute that mission, and with responsibility for managing its own risks and performance. An enterprise may consist of all or some of the following business aspects: acquisition, program management, financial management (*e.g.,* budgets), human resources, security, and information systems, information and mission management, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).
32 CFR 170.4

External Service Provider (ESP) — external people, technology, or facilities that an organization utilizes for provision and management of IT and/or cybersecurity services on behalf of the organization. In the CMMC Program, CUI or Security Protection Data (*e.g.,* log data, configuration data), must be processed, stored, or transmitted on the ESP assets to be considered an ESP. (CMMC-custom term)
32 CFR 170.4

Federal Contract Information (FCI) — information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or

service to the Government, but not including information provided by the Government to the public (such as that on public Web sites) or simple transactional information, such as that necessary to process payments.
48 CFR 4.1901

Federal Information System — an information system used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. 44 U.S.C. 3554(a)(1)(A)(ii).
32 CFR 2002.4

Forensic Analysis — the practice of gathering, retaining, and analyzing computer-related data for investigative purposes in a manner that maintains the integrity of the data.
DFARS 252.204-7012

Foreign Entity — a foreign government, an international organization of governments or any element thereof, an international or foreign public or judicial body, or an international or foreign private or non-governmental organization.
32 CFR 2002.4

Formerly Restricted Data (FRD) — a type of information classified under the Atomic Energy Act, and defined in 10 CFR 1045, Nuclear Classification and Declassification.
32 CFR 2002.4

Government Furnished Equipment (GFE) — property in the possession of, or directly acquired by, the Government and subsequently furnished to the contractor for performance of a contract. Government-furnished property includes, but is not limited to, spares and property furnished for repair, maintenance, overhaul, or modification. Government-furnished property also includes contractor-acquired property if the contractor-acquired property is a deliverable under a cost contract when accepted by the Government for continued use under the contract.
48 CFR 45.101

Handling — any use of CUI, including but not limited to marking, safeguarding, transporting, disseminating, re-using, and disposing of the information.
32 CFR 2002.4

High Assessment — an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—
(1) Consists of—
(i) A review of a contractor's Basic Assessment;
(ii) A thorough document review;
(iii) Verification, examination, and demonstration of a Contractor's system security plan to validate that NIST SP 800-171 security requirements have been implemented as described in the contractor's system security plan; and
(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and
(2) Results in a confidence level of "High" in the resulting score.
DFARS 252.204-7020

Identifier — unique data used to represent a person's identity and associated attributes. A name or a card number are examples of identifiers.
NIST Glossary

Industrial Control Systems (ICS) — means a general term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCS), and other control system configurations that are often found in the industrial sectors and critical infrastructures, such as Programmable Logic Controllers (PLC). An ICS consists of combinations of control components (*e.g.,* electrical, mechanical, hydraulic, pneumatic) that act together to achieve an industrial objective (*e.g.,* manufacturing, transportation of matter or energy), as defined in NIST SP 800-82r3 (incorporated by reference, see § 170.2).
32 CFR 170.4

Information System (IS) — A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.
NIST SP 800-171 R2
DFARS 252.204-7012

Internet of Things (IoT) — the network of devices that contain the hardware, software, firmware, and actuators which allow the devices to connect, interact, and freely exchange data and information, as defined in NIST SP 800-172A Mar2022 (incorporated by reference, see § 170.2).
32 CFR 170.4

ISOO Registry — Information Security Oversight Office online repository for Federal-level guidance regarding CUI policy and practice
DoD Mandatory CUI Training - Glossary, CDSE

Lawful Government Purpose — any activity, mission, function, operation, or endeavor that the U.S. Government authorizes or recognizes as within the scope of its legal authorities or the legal authorities of non-executive branch entities (such as state and local law enforcement).
32 CFR 2002.4

Legacy material — unclassified information that an agency marked as restricted from access or dissemination in some way, or otherwise controlled, prior to the CUI Program.
32 CFR 2002.4

Limited Dissemination Control (LDC) —

1. utilized within DoD to limit access to certain agency-specific CUI within an organization
   DoD Mandatory CUI Training - Glossary, CDSE
2. any CUI EA-approved control that agencies may use to limit or specify CUI dissemination.
   32 CFR 2002.4

Malicious Software — computer software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. This definition includes a virus, worm, Trojan horse, or other code-based entity that infects a host, as well as spyware and some forms of adware.

Media — physical devices or writing surfaces including, but is not limited to, magnetic tapes, optical disks, magnetic disks, large-scale integration memory chips, and printouts onto which covered defense information is recorded, stored, or printed within a covered contractor information system.
DFARS 252.204-7012

Media — physical devices or writing surfaces including, but not limited to, magnetic tapes, optical disks, magnetic disks, Large-Scale Integration (LSI) memory chips, and printouts (but not including display media) onto which information is recorded, stored, or printed within a system.
NIST Glossary

Medium Assessment — an assessment conducted by the Government that—
(1) Consists of—
(i) A review of a contractor's Basic Assessment;
(ii) A thorough document review; and
(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and
(2) Results in a confidence level of "Medium" in the resulting score.
DFARS 252.204-7020

Misuse of CUI — occurs when someone uses CUI in a manner not in accordance with the policy contained in the Order, this part, the CUI Registry, agency CUI policy, or the applicable laws, regulations, and Government-wide policies that govern the affected information. This may include intentional violations or unintentional errors in safeguarding or disseminating CUI. This may also include designating or marking information as CUI when it does not qualify as CUI.
32 CFR 2002.4

National Security System — a special type of information system (including telecommunications systems) whose function, operation, or use is defined in National Security Directive 42 and 44 U.S.C. 3542(b)(2).
32 CFR 2002.4

Non-Executive Branch Entity — a person or organization established, operated, and controlled by individual(s) acting outside the scope of any official capacity as officers, employees, or agents of the executive branch of the Federal Government. Such entities may include: Elements of the legislative or judicial branches of the Federal Government; state, interstate, tribal, or local government elements; and private organizations. Non-executive branch entity does not include foreign entities as defined in this part, nor does it include individuals or organizations when they receive CUI information pursuant to federal disclosure laws, including the Freedom of Information Act (FOIA) and the Privacy Act of 1974.
32 CFR 2002.4

On Behalf of an Agency — occurs when a non-executive branch entity uses or operates an information system or maintains or collects information for the purpose of processing, storing, or transmitting Federal information, and those activities are not incidental to providing a service or product to the Government.

32 CFR 2002.4

Operationally Critical Support — supplies or services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.
DFARS 252.204-7012

Operational Plan of Action (OPA) — as used in security requirement CA.L2-3.12.2, means the formal artifact which identifies temporary vulnerabilities and temporary deficiencies (*e.g.,* necessary information system updates, patches, or reconfiguration as threats evolve) in implementation of requirements and documents how they will be mitigated, corrected, or eliminated. The OSA defines the format (*e.g.,* document, spreadsheet, database) and specific content of its operational plan of action. An operational plan of action does not identify a timeline for remediation and is not the same as a POA&M, which is associated with an assessment for remediation of deficiencies that must be completed within 180 days. (CMMC-custom term)
32 CFR 170.4

Operational Technology (OT) — means programmable systems or devices that interact with the physical environment (or manage devices that interact with the physical environment). These systems or devices detect or cause a direct change through the monitoring or control of devices, processes, and events. Examples include industrial control systems, building management systems, fire control systems, and physical access control mechanisms, as defined in NIST SP 800-160 V2R1 (incorporated by reference, see § 170.2).
32 CFR 170.4

Order is Executive Order 13556, Controlled Unclassified Information, November 4, 2010 (3 CFR, 2011 Comp., p. 267), or any successor order.
32 CFR 2002.4

Organization-Defined — as determined by the OSA except as defined in the case of Organization-Defined Parameter (ODP). (CMMC-custom term)
32 CFR 170.4

Organization Defined Parameter (ODP) — selected enhanced security requirements contain selection and assignment operations to give organizations flexibility in defining variable parts of those requirements, as defined in NIST SP 800-172A Mar2022 (incorporated by reference, see § 170.2). *Note 1 to ODPs:* The organization defining the parameters is the DoD.
32 CFR 170.4

Organization Seeking Assessment (OSA) — the entity seeking to undergo a self-assessment or certification assessment for a given information system for the purposes of achieving and maintaining any CMMC Status. The term OSA includes all Organizations Seeking Certification (OSCs). (CMMC-custom term)
32 CFR 170.4

Organization Seeking Certification (OSC) — the entity seeking to undergo a certification assessment for a given information system for the purposes of achieving and maintaining the CMMC Status of Level 2 (C3PAO) or Level 3 (DIBCAC). An OSC is also an OSA. (CMMC-custom term)

32 CFR 170.4

Out Of Scope (OOS) Asset — assets that cannot process, store, or transmit CUI because they are physically or logically separated from information systems that do process, store, or transmit CUI, or are inherently unable to do so; except for assets that provide security protection for a CUI asset (see the definition for *Security Protection Assets*). (CMMC-custom term)
32 CFR 170.4

Periodically — occurring at a regular interval as determined by the OSA that may not exceed one year. (CMMC-custom term)
32 CFR 170.4

Personally Identifiable — information that can be used to distinguish or trace an individual's identity, either alone or when combined with other information that is linked or linkable to a specific individual, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).
32 CFR 170.4

Plan of Action and Milestones (POA&M) — a document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones, as defined in NIST SP 800-115 Sept2008 (incorporated by reference, see § 170.2).
32 CFR 170.4

Portion — ordinarily a section within a document, and may include subjects, titles, graphics, tables, charts, bullet statements, sub-paragraphs, bullets points, or other sections.
32 CFR 2002.4

Practice — An activity or set of activities that are performed to meet the defined CMMC objectives.
CMMC 2.0 Glossary (now deprecated)

*Editor comment: In the CMMC lexicon we commonly refer to the 110 items that NIST SP 800-171 by **three** different names. Control or Security Control derived from Financial Audit and NIST 800-53 common practice. Security Requirements as they are defined and labelled in NIST SP800-171. Finally, as Practices, a term introduced in CMMC 1.0 for this listing. The term Practices is a legacy term no longer used in the Assessment Guides for the purpose of labelling the 110 things that must be done. The Assessment Guides currently use the label, "requirement" for this purpose.*

Prime Contractor — a person who has entered into a prime contract with the United States.
48 CFR 3.502-1

Process, Store, or Transmit — data can be used by an asset (*e.g.,* accessed, entered, edited, generated, manipulated, or printed); data is inactive or at rest on an asset (*e.g.,* located on electronic media, in system component memory, or in physical format such as paper documents); or data is being transferred from one asset to another asset (*e.g.,* data in transit using physical or digital transport methods). (CMMC-custom term)
32 CFR 170.4

Protection — includes all controls an agency applies or must apply when handling information that qualifies as CUI.
32 CFR 2002.4

Protocol — a set of rules (i.e., formats and procedures) for communications that computers use when sending signals between themselves.
NIST Glossary

Public Release — occurs when the agency that originally designated particular information as CUI makes that information available to the public through the agency's official public release processes. Disseminating CUI to non-executive branch entities as authorized does not constitute public release. Releasing information to an individual pursuant to the Privacy Act of 1974 or disclosing it in response to a FOIA request also does not automatically constitute public release, although it may if that agency ties such actions to its official public release processes. Even though an agency may disclose some CUI to a member of the public, the Government must still control that CUI unless the agency publicly releases it through its official public release processes.
32 CFR 2002.4

Rapidly Report — within 72 hours of discovery of any cyber incident.
DFARS 252.204-7012

Records — agency records and Presidential papers or Presidential records (or Vice-Presidential), as those terms are defined in 44 U.S.C. 3301 and 44 U.S.C. 2201 and 2207. Records also include such items created or maintained by a Government contractor, licensee, certificate holder, or grantee that are subject to the sponsoring agency's control under the terms of the entity's agreement with the agency.
32 CFR 2002.4

Restricted Information Systems — systems (and associated IT components comprising the system) that are configured based on government requirements (*e.g.,* connected to something that was required to support a functional requirement) and are used to support a contract (*e.g.,* fielded systems, obsolete systems, and product deliverable replicas). (CMMC-custom term)
32 CFR 170.4

Required or Permitted (by a Law, Regulation, or Government-wide Policy) — the basis by which information may qualify as CUI. If a law, regulation, or Government-wide policy requires that agencies exercise safeguarding or dissemination controls over certain information, or specifically permits agencies the discretion to do so, then that information qualifies as CUI. The term 'specifically permits' in this context can include language such as “is exempt from” applying certain information release or disclosure requirements, “may” release or disclose the information, “may not be required to” release or disclose the information, “is responsible for protecting” the information, and similar specific but indirect, forms of granting the agency discretion regarding safeguarding or dissemination controls. This does not include general agency or agency head authority and discretion to make decisions, risk assessments, or other broad agency authorities, discretions, and powers, regardless of the source. The CUI Registry reflects all appropriate authorizing authorities.

32 CFR 2002.4

Restricted Data (RD) — a type of information classified under the Atomic Energy Act, defined in 10 CFR part 1045, Nuclear Classification and Declassification
32 CFR 2002.4
.

Re-Use — incorporating, restating, or paraphrasing information from its originally designated form into a newly created document.
32 CFR 2002.4

Risk — a measure of the extent to which an entity is threatened by a potential circumstance or event, and is typically a function of:
(i) The adverse impacts that would arise if the circumstance or event occurs; and
(ii) The likelihood of occurrence, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).
32 CFR 170.4

Risk Assessment (RA) — the process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of a system. Risk Assessment is part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis, as defined in NIST SP 800-39 Mar2011 (incorporated by reference, see § 170.2).
32 CFR 170.4

Security Control — The safeguards or countermeasures prescribed for an information system or an organization to protect the confidentiality, integrity, and availability of the system and its information.
NIST Glossary

*Editor comment: In the CMMC lexicon we commonly refer to the 110 items that NIST SP 800-171 by **three** different names. Control or Security Control derived from Financial Audit and NIST 800-53 common practice. Security Requirements as they are defined and labelled in NIST SP800-171. Finally, as Practices, a term introduced in CMMC 1.0 for this listing.*

Security Protection Assets (SPA) — assets providing security functions or capabilities for the OSA's CMMC Assessment Scope. (CMMC-custom term). Also as outlined in the CMMC Level 2 Scoping Guide 2.13 2024, Security Protection Assets are part of the CMMC Assessment Scope and are assessed against Level 2 security requirements that are relevant to the capabilities provided. For example, an External Service Provider (ESP), defined in 32 CFR §170.4, that provides a security information and event management (SIEM) service may be separated logically and may not process CUI, but the SIEM does contribute to meeting the CMMC requirements within the OSA's CMMC Assessment Scope.
32 CFR 170.4 and CMMC Level 2 Scoping Guide 2.13

Security Protection Data (SPD) — data stored or processed by Security Protection Assets (SPA) that are used to protect an OSC's assessed environment. SPD is security relevant information and includes but is not limited to: configuration data required to operate an SPA, log

files generated by or ingested by an SPA, data related to the configuration or vulnerability status of in-scope assets, and passwords that grant access to the in-scope environment. (CMMC-custom term)
32 CFR 170.4

Security Requirement — A requirement levied on a system or an organization that is derived from applicable laws, Executive Orders, directives, regulations, policies, standards, procedures, or mission/business needs to ensure the confidentiality, integrity, and availability of information that is being processed, stored, or transmitted.
NIST SP 800-171 r2

*Editor comment: In the CMMC lexicon we commonly refer to the 110 items that NIST SP 800-171 by **three** different names. Control or Security Control derived from Financial Audit and NIST 800-53 common practice. Security Requirements as they are defined and labelled in NIST SP800-171. Finally, as Practices, a term introduced in CMMC 1.0 for this listing. The term Practices is a legacy term no longer used in the Assessment Guides for the purpose of labelling the 110 things that must be done. The Assessment Guides currently use the label, "requirement" for this purpose.*

Self-Inspection — an agency's internally managed review and evaluation of its activities to implement the CUI Program.
32 CFR 2002.4

Services — a software component participating in a service-oriented architecture that provides functionality or participates in realizing one or more capabilities.
NIST Glossary

Shared Responsibility Matrix (SRM) — Another term for Customer Responsibility Matrix (CRM) which is the term used in CMMC as defined by 32CFR170. NIST does not use or define either term.

Specialized Asset (SA) —

1. assets that can process, store, or transmit FCI but are unable to be fully secured, including: Internet of Things (IoT) devices, Industrial Internet of Things (IIoT) devices, Operational Technology (OT), Government Furnished Equipment (GFE), Restricted Information Systems, and Test Equipment
   32 CFR 170.19

2. types of assets considered specialized assets for CMMC: Government Furnished Equipment, Internet of Things (IoT) or Industrial Internet of Things (IIoT), Operational Technology (OT), Restricted Information Systems, and Test Equipment. (CMMC-custom term)
   32 CFR 170.4

3. Assets that can process, store, or transmit CUI but are unable to be fully secured. These include:

a. People — EX. Consultants who provide cybersecurity service, Managed service provider personnel who implement system maintenance, Enterprise network administrators
b. Technology — EX. Cloud-based security solutions, Hosted Virtual Private Network (VPN) services, SIEM solutions
c. Facilities — EX. Co-located data centers, Security Operations Centers (SOCs), OSA office buildings

CMMC Scoping Guide Level 2 Version 2.13, Table 2

Subcontractor — any person, other than the prime contractor, who offers to furnish or furnishes any supplies, materials, equipment, or services of any kind under a prime contract or a subcontract entered into in connection with such prime contract; and includes any person who offers to furnish or furnishes general supplies to the prime contractor or a higher tier subcontractor.
48 CFR 3.502-1

Supervisory Control and Data Acquisition (SCADA) — a generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (*e.g.,* delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated, as defined in NIST SP 800-82r3 (incorporated by reference, see § 170.2).
32 CFR 170.4

System Security Plan (SSP) — the formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The system security plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).
32 CFR 170.4

Technical Information — technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013 , Rights in Technical Data—Other Than Commercial Products and Commercial Services, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.
DFARS 252.204-7012

Temporary Deficiency — a condition where remediation of a discovered deficiency is feasible, and a known fix is available or is in process. The deficiency must be documented in an operational plan of action. A temporary deficiency is not based on an `in progress' initial implementation of a CMMC security requirement but arises after implementation. A temporary deficiency may apply during the initial implementation of a security requirement if, during roll-out, specific issues with a very limited subset of equipment is discovered that must be separately addressed. There is no standard duration for which a temporary deficiency may be

active. For example, FIPS-validated cryptography that requires a patch and the patched version is no longer the validated version may be a temporary deficiency. (CMMC-custom term)
32 CFR 170.4

Test Equipment — hardware and/or associated IT components used in the testing of products, system components, and contract deliverables. (CMMC-custom term)
32 CFR 170.4

Unauthorized Disclosure — occurs when an authorized holder of CUI intentionally or unintentionally discloses CUI without a lawful Government purpose, in violation of restrictions imposed by safeguarding or dissemination controls, or contrary to limited dissemination controls.
32 CFR 2002.4

Uncontrolled Unclassified Information — information that neither the Order nor the authorities governing classified information cover as protected. Although this information is not controlled or classified, agencies must still handle it in accordance with Federal Information Security Modernization Act (FISMA) requirements.
32 CFR 2002.4

User — an individual, or (system) process acting on behalf of an individual, authorized to access a system, as defined in NIST SP 800-53 R5 (incorporated by reference, see § 170.2).
32 CFR 170.4

Working papers — documents or materials, regardless of form, that an agency or user expects to revise prior to creating a finished product.
32 CFR 2002.4

From the Federal Register — Acronyms

AC — Access Control
32 CFR 170.4

APT — Advanced Persistent Threat
32 CFR 170.4

AT — Awareness and Training
32 CFR 170.4

C3PAO — CMMC Third-Party Assessment Organization
32 CFR 170.4

CFR — Code of Federal Regulations
32 CFR 170.4

CA — Security Assessment
32 CFR 170.4

CAICO — CMMC Assessors and Instructors Certification Organization
32 CFR 170.4

CAGE — Commercial and Government Entity
32 CFR 170.4

CCA — CMMC-Certified Assessor
32 CFR 170.4

CCI — CMMC-Certified Assessor
32 CFR 170.4

CCP — CMMC-Certified Assessor
32 CFR 170.4

CFR — Code of Federal Regulations
32 CFR 170.4

CIO — Chief Information Officer
32 CFR 170.4

CM — Configuration Management
32 CFR 170.4

CMMC — Cybersecurity Maturity Model Certification
32 CFR 170.4

CMMC PMO — CMMC Program Management Office
32 CFR 170.4

CNC — Computerized Numerical Control
32 CFR 170.4

CoPC — Code of Professional Conduct
32 CFR 170.4

CSP — Cloud Service Provider
32 CFR 170.4

CUI — Controlled Unclassified Information
32 CFR 170.4

DCMA — Defense Contract Management Agency
32 CFR 170.4

DD — Represents any two-character CMMC Domain acronym
32 CFR 170.4

DFARS — Defense Federal Acquisition Regulation Supplement
32 CFR 170.4

DIB — Defense Industrial Base
32 CFR 170.4

DIBCAC — DCMA's Defense Industrial Base Cybersecurity Assessment Center
32 CFR 170.4

DoD — Department of Defense
32 CFR 170.4

DoDI — Department of Defense Instruction
32 CFR 170.4

eMASS —Enterprise Mission Assurance Support Service
32 CFR 170.4

ESP — External Service Provider
32 CFR 170.4

FAR — Federal Acquisition Regulation
32 CFR 170.4

FCI — Federal Contract Information
32 CFR 170.4

FedRAMP — Federal Risk and Authorization Management Program. Sometimes abbreviated FR.
32 CFR 170.4

FRME — Federal Risk and Authorization Management Program (FedRAMP) Moderate Equivalent as outlined in DFARS 252.204-7012 and the DoD Memo of 21DEC2023 that further defines what exactly constitutes equivalency.
DFARS 252.204-7012 and https://dodcio.defense.gov/Portals/0/Documents/Library/FEDRAMP-EquivalencyCloudServiceProviders.pdf

FOIA — Freedom of Information Act
DoD Mandatory CUI Training - Glossary, CDSE

GFE — Government Furnished Equipment
32 CFR 170.4

IA — Identification and Authentication
32 CFR 170.4

ICS —Industrial Control System
32 CFR 170.4

IIoT — Industrial Internet of Things
32 CFR 170.4

IoT — Internet of Things
32 CFR 170.4

IR — Incident Response
32 CFR 170.4

IS — Information System
32 CFR 170.4

IEC — International Electrotechnical Commission
32 CFR 170.4

ISO/IEC — International Organization for Standardization/International Electrotechnical Commission
32 CFR 170.4

IT — Information Technology
32 CFR 170.4

L# — CMMC Level Number
32 CFR 170.4

MA — Maintenance
32 CFR 170.4

MP — Media Protection
32 CFR 170.4

MSSP —Managed Security Service Provider
32 CFR 170.4

NARA — National Archives and Records Administration
32 CFR 170.4

NAICS — North American Industry Classification System
32 CFR 170.4

NIST — National Institute of Standards and Technology
32 CFR 170.4

N/A —Not Applicable
32 CFR 170.4

ODP — Organization-Defined Parameter
32 CFR 170.4

OSA — Organization Seeking Assessment
32 CFR 170.4

OSC — Organization Seeking Certification
32 CFR 170.4

OT — Operational Technology
32 CFR 170.4

PI — Provisional Instructor
32 CFR 170.4

PIEE — Procurement Integrated Enterprise Environment
32 CFR 170.4

PII — Personally Identifiable Information
32 CFR 170.4

PLC — Programmable Logic Controller
32 CFR 170.4

POA&M — Plans of Action and Milestones
32 CFR 170.4

PRA —Paperwork Reduction Act
32 CFR 170.4

RM — Risk Management
32 CFR 170.4

SAM —System of Award Management
32 CFR 170.4

SC —System and Communications Protection
32 CFR 170.4

SCADA — Supervisory Control and Data Acquisition
32 CFR 170.4

SI — System and Information Integrity
32 CFR 170.4

SIEM — Security Information and Event Management
32 CFR 170.4

SOC — Security Operations Center
NIST SP 800-53

SP — Special Publication
32 CFR 170.4

SPD — Security Protection Data
32 CFR 170.4

SPRS —Supplier Performance Risk System
32 CFR 170.4

SSP — System Security Plan
32 CFR 170.4

VDI — Virtual Desktop Infrastructure (for discussion of VDI requirements see 32 CFR 170)
32 CFR 170.4