CMMC Glossary and Acronyms

Version 2.0 | December 2021

NOTICES

This material is based upon work funded and supported by the Department of Defense under Contract No. FA8702-15-D-0002 with Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center, and under Contract No. HQ0034-13-D-0003 and Contract No. N00024-13-D-6400 with the Johns Hopkins University Applied Physics Laboratory LLC, a University Affiliated Research Center.

TABLE OF CONTENTS

This page intentionally left blank.

Glossary

This glossary of terms used in the Cybersecurity Maturity Model Certification (CMMC) model has been derived from the sources cited.

Access

Ability to make use of any information system (IS) resource.

Source: CNSSI 4009, NIST SP 800-32

Access Authority

An entity responsible for monitoring and granting access privileges for other authorized entities.

Source: CNSSI 4009

Access Control (AC)

The process of granting or denying specific requests to:

- obtain and use information and related information processing services; and
- enter specific physical facilities (e.g., federal buildings, military establishments, border crossing entrances).

Source: FIPS 201, CNSSI 4009

Access Control Policy (Access Management Policy)

The set of rules that define the conditions under which an access may take place.

Source: NISTIR 7316

Access Profile

Association of a user with a list of protected objects the user may access.

Source: CNSSI 4009

Accountability

The security goal that generates the requirement for actions of an entity to be traced uniquely to that entity. This supports nonrepudiation, deterrence, fault isolation, intrusion detection and prevention, and after-action recovery and legal action.

Source: NIST SP 800-27

Activity / Activities

Set of actions that are accomplished within a practice in order to make it successful. Multiple activities can make up a practice. Practices may have only one activity or a set of activities.

Source: CMMC

Administrative Safeguards

Administrative actions and policies and procedures to manage the selection, development, implementation, and maintenance of security measures to protect any electronic information that is by definition "protected information" (e.g., protected health information) and to manage the conduct of the covered entity's workforce in relation to the protection of that information.

Source: NIST SP 800-66 Rev 1 (adapted)

Advanced Persistent Threat (APT)

An adversary that possesses sophisticated levels of expertise and significant resources which 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.

Source: NIST SP 800-39

Adversary

Individual, group, organization, or government that conducts or has the intent to conduct detrimental activities.

Source: CNSSI 4009

Adversarial Assessment

Assesses the ability of an organization equipped with a system to support its mission while withstanding cyber threat activity representative of an actual adversary.

Source: DoDI 5000.02 Enclosure 14 (adapted)

Air Gap

An interface between two systems that:

- are not connected physically and
- do not have any logical connection automated (i.e., data is transferred through the interface only manually, under human control).

Source: IETF RFC 4949 v2

Alert

An internal or external notification that a specific action has been identified within an organization's information systems.

Source: CNSSI 4009 (adapted)

Anti-Malware Tools

Tools that help identify, prevent execution, and reverse engineer malware.

Source: CMMC

Anti-Spyware Software

A program that specializes in detecting both malware and non-malware forms of spyware.

Source: NIST SP 800-69

Anti-Tamper

Systems engineering activities intended to deter and/or delay exploitation of technologies in a system in order to impede countermeasure development, unintended technology transfer, or alteration of a system.

Source: DoDI 5200.39 (adapted)

Anti-Virus Software

A program that monitors a computer or network to identify all major types of malware and prevent or contain malware incidents.

Source: NIST SP 800-83

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.

Source: NIST SP 800-37 Rev. 2

Assessment is the term used by CMMC for the activity performed by the C3PAO to evaluate the CMMC level of a DIB contractor. *Self-assessment* is the term used by CMMC for the activity performed by a DIB contractor to evaluate their own CMMC level.

Source: CMMC

Asset (Organizational Asset)

Anything that has value to an organization, including, but not limited to, another organization, person, computing device, information technology (IT) system, IT network, IT circuit, software (both an installed instance and a physical instance), virtual computing platform (common in cloud and virtualized computing), and related hardware (e.g., locks, cabinets, keyboards).

Source(s): NISTIR 7693, NISTIR 7694

Asset Custodian (Custodian)

A person or group responsible for the day-to-day management, operation, and security of an asset.

Source: CMMC

Asset Management (AM)

Management of organizational assets. This may include inventory, configuration, destruction, disposal, and updates to organizational assets.

Source: CERT RMM v1.2

Asset Owner (Information Asset Owner)

A person or organizational unit (internal or external to the organization) with primary responsibility for the viability, productivity, security, and resilience of an organizational asset. For example, the accounts payable department is the owner of the vendor database.

Source: CERT RMM v1.2

Asset Types

The following asset types should be included when classifying assets:

- People – employees, contractors, vendors, and external service provider personnel;
- Technology – servers, client computers, mobile devices, network appliances (e.g., firewalls, switches, APs, and routers), VoIP devices, applications, virtual machines, and database systems;
- Facilities – physical office locations, satellite offices, server rooms, datacenters, manufacturing plants, and secured rooms; and

- External Service Provider (ESP) – external people, technology, or facilities that the organization utilizes, including Cloud Service Providers, Managed Service Providers, Managed Security Service Providers, Cybersecurity-as-a-Service Providers.

  Source: CMMC

Attack Surface

The set of points on the boundary of a system, a system element, or an environment where an attacker can try to enter, cause an effect on, or extract data from.

Source: NIST SP 800-160 Vol. 2

Attribute-Based Access Control (ABAC)

Access control based on attributes associated with and about subjects, objects, targets, initiators, resources, or the environment. An access control rule set defines the combination of attributes under which an access may take place.

See Glossary: *Identity, Credential, and Access Management (ICAM)*

Source: CNSSI 4009

Availability

- Ensuring timely and reliable access to and use of information.
- Timely, reliable access to data and information services for authorized users.

  Source: CNSSI 4009

Audit

Independent review and examination of records and activities to assess the adequacy of system controls, to ensure compliance with established policies and operational procedures, and to recommend necessary changes in controls, policies, or procedures.

Source: NIST SP 800-32

Audit Log

A chronological record of system activities. Includes records of system accesses and operations performed in a given period.

Source: CNSSI 4009

Audit Record

An individual entry in an audit log related to an audited event.

Source: NIST SP 800-53 Rev 5

Authentication

A security measure designed to protect a communications system against acceptance of fraudulent transmission or simulation by establishing the validity of a transmission, message, originator, or a means of verifying an individual's eligibility to receive specific categories of information.

Source: CNSSI 4005, NSA/CSS Manual Number 3-16

Authenticator

Something that the claimant possesses and controls (typically a cryptographic module or password) that is used to authenticate the claimant's identity. This was previously referred to as a token.

Source: NIST SP 800-53 Rev 5

Authoritative Source (Trusted Source)

An entity that has access to, or verified copies of, accurate information from an issuing source such that a Credential Service Provider (CSP) can confirm the validity of the identity evidence supplied by an applicant during identity proofing. An issuing source may also be an authoritative source. Often, authoritative sources are determined by a policy decision of the agency or CSP before they can be used in the identity proofing validation phase.

Source: NIST SP 800-63-3

Authorization

The right or a permission that is granted to a system entity (user, program, or process) to access a system resource.

Source: NIST SP 800-82 Rev 2 (adapted)

Awareness

A learning process that sets the stage for training by changing individual and organizational attitudes to realize the importance of security and the adverse consequences of its failure.

Source: NIST SP 800-16

Awareness and Training Program

Explains proper rules of behavior for the use of agency information systems and information. The program communicates information technology (IT) security policies and procedures that need to be followed. (i.e., NSTISSD 501, NIST SP 800-50).

Source: CNSSI 4009

Backup

A copy of files and programs made to facilitate recovery, if necessary.

Source: NIST SP 800-34, CNSSI 4009

Baseline

Hardware, software, databases, and relevant documentation for an information system at a given point in time.

Source: CNSSI 4009

Baseline Configuration

A set of specifications for a system, or Configuration Item (CI) within a system, that has been formally reviewed and agreed on at a given point in time, and which can be changed only through change control procedures. The baseline configuration is used as a basis for future builds, releases, and/or changes.

Source: NIST SP 800-128

Baseline Security

The minimum security controls required for safeguarding an IT system based on its identified needs for confidentiality, integrity, and/or availability protection.

Source: NIST SP 800-16

Baselining

Monitoring resources to determine typical utilization patterns so that significant deviations can be detected.

Source: NIST SP 800-61

Blacklist

A list of discrete entities, such as IP addresses, host names, applications, software libraries, and so forth that have been previously determined to be associated with malicious activity thus requiring access or execution restrictions.

Source: NIST SP 800-114 (adapted), NIST SP 800-94 (adapted), CNSSI 4009 (adapted)

Blacklisting Software

A list of applications (software) and software libraries that are forbidden to execute on an organizational asset.

Source: NIST SP 800-94 (adapted)

Blue Team

- The group responsible for defending an organization's use of information systems by maintaining its security posture against a group of mock attackers (i.e., the Red Team). Typically, the Blue Team and its supporters must defend against real or simulated attacks:
  - over a significant period of time;
  - in a representative operational context (e.g., as part of an operational exercise); and
  - according to rules established and monitored with the help of a neutral group refereeing the simulation or exercise (i.e., the White Team).

- The term Blue Team is also used for defining a group of individuals who conduct operational network vulnerability evaluations and provide mitigation techniques to customers who have a need for an independent technical review of their network security posture. The Blue Team identifies security threats and risks in the operating environment, and in cooperation with the customer, analyzes the network environment and its current state of security readiness. Based on the Blue Team findings and expertise, they provide recommendations that integrate into an overall community security solution to increase the customer's cyber security readiness posture. Often, a Blue Team is employed by itself or prior to a Red Team employment to ensure that the customer's networks are as secure as possible before having the Red Team test the systems.

Source: CNSSI 4009 (adapted)

Breach

An incident where an adversary has gained access to the internal network of an organization or an organizationally owned asset in a manner that breaks the organizational policy for accessing cyber assets and results in the loss of information, data, or asset. A breach usually consists of the loss of an asset due to the gained access.

Source: CMMC

Change Control (Change Management)

The process of regulating and approving changes to hardware, firmware, software, and documentation throughout the development and operational life cycle of an information system.

Source: NIST SP 800-128, CNSSI 4009

Change Management

See Glossary: *Change Control*

Cipher

- Any cryptographic system in which arbitrary symbols or groups of symbols, represent units of plain text, or in which units of plain text are rearranged, or both.
- A series of transformations that converts plaintext to ciphertext using the Cipher Key.

Source: FIPS 197

Ciphertext

A term that describes data in its encrypted form.

Source: NIST SP 800-57 Part 1 Rev 3

CMMC Assessment Scope

Includes all assets in the contractor's environment that will be assessed.

Source: CMMC

CMMC Asset Categories

CMMC defined five asset categories for scoping activities: CUI Assets, Security Protection Assets, Contractor Risk Managed Assets, Specialized Assets, and Out-of-Scope Asset. Asset categories determine: assessment, segmentation, documentation, and management of assets.

Source: CMMC

Compliance

Conformity in fulfilling official requirements.

Source: Merriam-Webster

Component

A discrete identifiable information technology asset that represents a building block of a system and may include hardware, software, and firmware.

Source: NIST SP 800-171 Rev. 2 under system component NIST SP 800-128

Confidentiality

Preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information.

Source: 44 U.S.C. 3542

Configuration Item (CI)

An aggregation of system components that is designated for configuration management and treated as a single entity in the configuration management process.

Source: NIST SP 800-53 Rev 5

Configuration Management (CM)

A collection of activities focused on establishing and maintaining the integrity of information technology products and systems, through control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the system development life cycle.

Source: NIST SP 800-53 Rev 5

Consequence

Effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, caused, prevented, changed, or contributed to by the event, condition, or system.

Source: NIST SP 800-160

Container (Information Asset Container)

A physical or logical location where assets are stored, transported, and processed. A container can encompass technical containers (servers, network segments, personal computers), physical containers (paper, file rooms, storage spaces, or other media such as CDs, disks, and flash drives), and people (including people who might have detailed knowledge about the information asset).

Source: CERT RMM v1.2

Context Aware

The ability of a system or a system component to gather information about its environment at any given time and adapt behaviors accordingly. Contextual or context-aware computing uses software and hardware to automatically collect and analyze data to guide responses.

Source: CMMC

Continuity of Operations

An organization's ability to sustain assets and services in response to a disruptive event. It is typically used interchangeably with service continuity or continuity of service.

Source: CERT RMM v1.2 (adapted)

Consequence

Effect (change or non-change), usually associated with an event or condition or with the system and usually allowed, facilitated, caused, prevented, changed, or contributed to by the event, condition, or system.

Source: NIST SP 800-160

Continuous

Continuing without stopping; ongoing.

Source: Merriam-Webster (adapted)

Continuous Monitoring

Maintaining ongoing awareness to support organizational risk decisions. Maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions.

Source(s): CNSSI 4009-2015, NIST SP 800-137, NIST SP 800-150

Contractor Risk Managed Assets

Contractor Risk Managed Assets are capable of, but are not intended to, process, store, or transmit CUI because of the security policy, procedures, and practices in place.

Source: CMMC

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.

Source: NISTIR 8053 (adapted)

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: NIST SP 800-171 Rev 2

Covered Defense Information (CDI)

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: DFARS Clause 252.204-7012

Cryptographic Hashing Function

The process of using a mathematical algorithm against data to produce a numeric value that is representative of that data.

Source: CNSSI 4009

CUI Assets

Assets that process, store, or transmit CUI.

Source: CMMC

Custodian

See Glossary: *Asset Custodian*

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: NSPD-54/HSPD-23

Defense Industrial Base (DIB)

The worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements.

Source: DIB Sector-Specific Plan, DHS CISA

Dependency

When an entity has access to, control of, ownership in, possession of, responsibility for, or other defined obligations related to one or more assets or services of the organization.

Source: CERT RMM v1.2 (adapted)

Demilitarized Zone (DMZ)

A perimeter network segment that is logically between internal and external networks. Its purpose is to enforce the internal network's Information Assurance (IA) policy for external information exchange and to provide external, untrusted sources with restricted access to releasable information while shielding the internal networks from outside attacks.

Source: CNSSI 4009

Domain

Grouping of like practices based on the 14 control families set forth in NIST SP 800-171.

Source: CMMC

Encryption

The process of changing plaintext into cipher text.

Source: NISTIR 7621 Rev 1, CNSSI 4009

Encryption Policies

Policies that manage the use, storage, disposal, and protection of cryptographic keys used to protect organization data and communications.

Source: CERT RMM v1.2

Endorse

Declare one's public approval or support of.

Source: Oxford Dictionary

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.

Source: CNSSI 4009

Enterprise Architecture

The description of an enterprise's entire set of information systems: how they are configured, how they are integrated, how they interface to the external environment at the enterprise's boundary, how they are operated to support the enterprise mission, and how they contribute to the enterprise's overall security posture.

Source: CNSSI 4009

Environment

See Glossary: *Environment of Operations*

Environment of Operations

The physical and logical surroundings in which an information system processes, stores, and transmits information.

Source: NIST 800-53 Rev 5 (adapted)

Establish and Maintain

Whenever "establish and maintain" (or "established and maintained") is used as a phrase, it refers not only to the development and maintenance of the object of the practice (such as a policy) but to the documentation of the object and observable usage of the object. For example, "Formal agreements with external entities are established and maintained" means that not only are the agreements formulated, but they also are documented, have assigned ownership, and are maintained relative to corrective actions, changes in requirements, or improvements.

Source: CERT RMM v1.2

Event

Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring.

See Glossary: *Incident*

Source: CNSSI 4009

Event Correlation

Finding relationships between two or more events.

Source: NIST SP 800-92

Exercise

A simulation of an emergency designed to validate the viability of one or more aspects of an information technology plan.

Source: NIST SP 800-84

Facility

Physical means or equipment for facilitating the performance of an action, e.g., buildings, instruments, tools.

Source: NIST SP 800-160

Federal Contract Information (FCI)

Federal contract information means 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 on public websites) or simple transactional information, such as necessary to process payments.

Source: 48 CFR § 52.204-21

Federated Trust

Trust established within a federation or organization, enabling each of the mutually trusting realms to share and use trust information (e.g., credentials) obtained from any of the other mutually trusting realms. This trust can be established across computer systems and networks architectures.

Source: NIST SP 800-95

Federation

A collection of realms (domains) that have established trust among themselves. The level of trust may vary, but typically includes authentication and may include authorization.

Source: NIST SP 800-95

Firewall

A device or program that controls the flow of network traffic between networks or hosts that employ differing security postures.

Source: NIST SP 800-41 Rev 1

Flash Drive

A removable storage device that utilizes the USB port of a system for data transfer.

Source: CMMC

Government Property

All property owned or leased by the Government. Government property includes both Government-furnished and Contractor-acquired property. Government property includes material, equipment, special tooling, special test equipment, and real property. Government property does not include intellectual property or software.

Source: FAR 52.245-1

High-Value Asset (HVA)

Asset, organization information system, information, and data for which an unauthorized access, use, disclosure, disruption, modification, or destruction could cause a significant impact to the organization's interests, relations, economy, or to the employee or stockholder confidence, civil liberties, or health and safety of the organization's people. An HVA may

contain sensitive controls, instructions, data used in critical organization operations, or unique collections of data (by size or content), or support an organization's mission essential functions, making it of specific value to criminal, politically motivated, or state sponsored actors for either direct exploitation or to cause a loss of confidence in the organization.

Source: OMB M-17-09 (adapted)

High-Value Service

Service on which the success of the organization's mission depends.

Source: CERT RMM v.12

Identification

The process of discovering the true identity (i.e., origin, initial history) of a person or item from the entire collection of similar persons or items.

Source: CNSSI 4009-2015, FIPS 201-1, NIST SP 800-79-2

Identity

The set of attribute values (i.e., characteristics) by which an entity is recognizable and that, within the scope of an identity manager's responsibility, is sufficient to distinguish that entity from any other entity.

Note: This also encompasses non-person entities (NPEs).

Source: NIST SP 800-161, NISTIR 7622, CNSSI 4009

Identity-Based Access Control (IBAC)

Access control based on the identity of the user (typically relayed as a characteristic of the process acting on behalf of that user) where access authorizations to specific objects are assigned based on user identity.

Source: CERT RMM v1.2

Identity, Credential, and Access Management (ICAM)

Programs, processes, technologies, and personnel used to create trusted digital identity representations of individuals and non-person entities (NPEs), bind those identities to credentials that may serve as a proxy for the individual or NPE in access transactions, and leverage the credentials to provide authorized access to an organization‘s resources.

See Glossary: *Attribute-Based Access Control (ABAC)*

Source: CNSSI 4009 (adapted)

Identity Management System

Identity management system comprised of one or more systems or applications that manages the identity verification, validation, and issuance process.

Source: NISTIR 8149

Incident

An occurrence that actually or potentially jeopardizes the confidentiality, integrity, or availability of a system or the information the system processes, stores, or transmits or that constitutes a violation or imminent threat of violation of security policies, security procedures, or acceptable use policies.

Source: NIST SP 800-171 Rev 2

Incident Handling (Incident Response)

The actions the organization takes to prevent or contain the impact of an incident to the organization while it is occurring or shortly after it has occurred

Source: CERT RMM v1.2

Incident Response (IR)

See Glossary: *Incident Handling*

Incident Stakeholder

A person or organization with a vested interest in the management of an incident throughout its life cycle.

Source: CERT RMM v1.2

Industrial Control System (ICS)

General term that encompasses several types of control systems, including supervisory control and data acquisition (SCADA) systems, distributed control systems (DCSs), and other control system configurations such as programmable logic controllers (PLCs) found in the industrial sectors and critical infrastructures. An industrial control system 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).

Source: NIST SP 800-53 Rev 5

Industrial Internet of Things (IIoT)

See Glossary: *Internet of Things (IoT)*

Information Asset Container

See Glossary: *Container*

Information Asset Owner

See Glossary: *Asset Owner*

Information Flow

The flow of information or connectivity from one location to another. This can be related to data as well as connectivity from one system to another, or from one security domain to another. The authorization granting permission for information flow comes from a control authority granting permission to an entity, asset, role, or group.

Source: CMMC

Information System (IS)

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

Source: NIST 800-171 Rev 2

Information System Component

A discrete, identifiable information technology asset (e.g., hardware, software, firmware) that represents a building block of an information system, excluding separately authorized

systems to which the information system is connected. Information system components include commercial information technology products.

Source: CNSSI 4009-2015, NIST SP 800-53 Rev 4 (adapted)

Insider

Any person with authorized access to any organization or United States Government resource to include personnel, facilities, information, equipment, networks, or systems.

Source: CNSSD No. 504

Insider Threat

The threat that an insider will use her/his authorized access, wittingly or unwittingly, to do harm to the security of the organization or the United States. This threat can include damage to the United States through espionage, terrorism, unauthorized disclosure, or through the loss or degradation of departmental resources or capabilities.

Source: CNSSD No. 504 (adapted)

Insider Threat Program

A coordinated collection of capabilities authorized by the Department/Agency (D/A) that is organized to deter, detect, and mitigate the unauthorized disclosure of sensitive information.

Source: CNSSD No. 504

Integrity

The security objective that generates the requirement for protection against either intentional or accidental attempts to violate data integrity (the property that data has not been altered in an unauthorized manner) or system integrity (the quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation).

Source: NIST SP 800-33

Internet of Things (IoT)

Interconnected devices having physical or virtual representation in the digital world, sensing/actuation capability, and programmability features. They are uniquely identifiable and may include smart electric grids, lighting, heating, air conditioning, and fire and smoke detectors.

Source: iot.ieee.org/definition; NIST SP 800-183

Inventory

The physical or virtual verification of the presence of each organizational asset.

Source: CNSSI 4005 (adapted)

Least Privilege

A security principle that restricts the access privileges of authorized personnel (e.g., program execution privileges, file modification privileges) to the minimum necessary to perform their jobs.

Source: NIST SP 800-57 Part 2

Life Cycle

Evolution of a system, product, service, project, or other human-made entity from conception through retirement.

Source: NIST SP 800-161

Maintenance

Any act that either prevents the failure or malfunction of equipment or restores its operating capability.

Source: NIST SP 800-82 Rev 2

Malicious Code

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code.

Source: CNSSI 4009

Malware

Software or firmware intended to perform an unauthorized process that will have adverse impact on the confidentiality, integrity, or availability of an information system. A virus, worm, Trojan horse, or other code-based entity that infects a host. Spyware and some forms of adware are also examples of malicious code (malware).

Source: NIST SP 800-82 Rev 2

Maturity Model

A maturity model is a set of characteristics, attributes, or indicators that represent progression in a particular domain. A maturity model allows an organization or industry to have its practices, processes, and methods evaluated against a clear set of requirements (such as activities or processes) that define specific maturity levels. At any given maturity level, an organization is expected to exhibit the capabilities of that level. A tool that helps assess the current effectiveness of an organization, and supports determining what capabilities they need in order to obtain the next level of maturity in order to continue progression up the levels of the model.

Source: CERT RMM v1.2

Media

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

Source: FIPS 200

Media Sanitization

The actions taken to render data written on media unrecoverable by both ordinary and extraordinary means.

Source: NIST SP 800-88 Rev 1

Mobile Code

Software programs or parts of programs obtained from remote systems, transmitted across a network, and executed on a local system without explicit installation or execution by the recipient.

Note: Some examples of software technologies that provide the mechanisms for the production and use of mobile code include Java, JavaScript, ActiveX, VBScript, etc.

Source: NIST SP 800-53 Rev 5, NIST SP 800-18, CNSSI 4009

Mobile Device

A portable computing device that:

- has a small form factor such that it can easily be carried by a single individual;
- is designed to operate without a physical connection (e.g., wirelessly transmit or receive information);
- possesses local, non-removable data storage; and
- is powered on for extended periods of time with a self-contained power source.

Mobile devices may also include voice communication capabilities, on-board sensors that allow the device to capture (e.g., photograph, video, record, or determine location) information, and/or built-in features for synchronizing local data with remote locations. Examples include smart phones, tablets, and e-readers.

Note: If the device only has storage capability and is not capable of processing or transmitting/receiving information, then it is considered a portable storage device, not a mobile device.

See Glossary: *Portable Storage Device*

Note: Laptops are excluded from the scope of this definition (see NIST SP 800-124).

Source: NIST SP 800-53 Rev 5

Monitor

The act of continually checking, supervising, critically observing, or determining the status in order to identify change from the performance level required or expected at an *organizationally defined* frequency and rate.

Source: NIST SP 800-160 (adapted)

Multifactor Authentication (MFA)

An authentication system or an authenticator that requires more than one authentication factor for successful authentication. Multifactor authentication can be performed using a single authenticator that provides more than one factor or by a combination of authenticators that provide different factors.

The three authentication factors are something you know, something you have, and something you are.

See Glossary: *Authenticator*

Source: NIST SP 800-53 Rev 5

Ongoing Basis

Actions occurring, indefinitely. Actions that do not stop unless a stop action is purposely put in place.

Source: CMMC

Operational Resilience

The ability of systems to resist, absorb, and recover from or adapt to an adverse occurrence during operation that may cause harm, destruction, or loss of ability to perform mission-related functions.

Source: CNSSI 4009

Operational Technology (OT)

Hardware and software that detects or causes a change through the direct monitoring and/or control of physical devices, processes and events in the enterprise.

Source: DOE O 205.1C, Department of Energy Cyber Security Program

Organization

An entity of any size, complexity, or positioning within an organizational structure (e.g., a federal agency, or, as appropriate, any of its operational elements).

See Glossary: *Enterprise*

Source: NIST SP 800-37 Rev 1

Organization Seeking Certification (OSC)

The entity that is going through the CMMC assessment process to receive a level of certification for a given environment.

Source: CMMC

Organizational Asset

See Glossary: *Asset*

Source(s): NISTIR 7693, NISTIR 7694

Organizational System(s)

The term organizational system is used in many of the CUI security requirements in NIST Special Publication 800-171. This term has a specific meaning regarding the scope of applicability for the CUI security requirements. The requirements apply only to components of nonfederal systems that process, store, or transmit CUI, or that provide security protection for such components. The appropriate scoping for the security requirements is an important factor in determining protection-related investment decisions and managing security risk for nonfederal organizations that have the responsibility of safeguarding CUI.

Source: NIST SP 800-171 Rev 1

Organizationally Defined

As determined by the contractor being assessed. This can be applied to a frequency or rate at which something occurs within a given time period, or it could be associated with describing the configuration of a contractor's solution.

Source: CMMC

Out-of-Scope Asset

Out-of-Scope Assets cannot process, store, or transmit CUI because they are physically or logically separated from CUI Assets or are inherently unable to do so.

Source: CMMC

Patch

An update to an operating system, application, or other software issued specifically to correct particular problems with the software.

Source: NIST SP 800-123

Penetration Testing (Pentesting)

Security testing in which evaluators mimic real-world attacks in an attempt to identify ways to circumvent the security features of an application, system, or network. Penetration testing often involves issuing real attacks on real systems and data, using the same tools and techniques used by actual attackers. Most penetration tests involve looking for combinations of vulnerabilities on a single system or multiple systems that can be used to gain more access than could be achieved through a single vulnerability.

Source: NIST SP 800-115

Periodically

Occurring at regular intervals. As used in many practices within CMMC, the interval length is *organizationally defined* to provided contractor flexibility, with an interval length of no more than one year.

Source: Oxford Dictionary (adapted)

Personally Identifiable Information (PII)

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.

Source: NIST SP 800-53 Rev 5

Plan

An artifact or collection of artifacts that provides oversight for implementing defined CMMC policies. A plan should include a mission and/or vision statement, strategic goals/objectives, relevant standards and procedures, and the people, funding, and tool resources needed to implement the defined CMMC policies.

Source: CMMC

Policy

An artifact or collection of artifacts that establishes governance over the implementation of CMMC practices and activities. The policy should include the stated purpose, the defined scope, roles and responsibilities of the activities covered by the policy, and any included regulatory guidelines. The policy should establish or direct the establishment of procedures to carry out and meet the intent of the policy and should be endorsed by senior management to show its support of the policy.

Source: CMMC

Portable Storage Device

A system component that can be inserted into and removed from a system, and that is used to store data or information (e.g., text, video, audio, and/or image data). Such components are typically implemented on magnetic, optical, or solid-state devices (e.g., floppy disks,

compact/digital video disks, flash/thumb drives, external hard disk drives, and flash memory cards/drives that contain nonvolatile memory).

Source: NIST SP 800-171 Rev 2

Practice

An activity or set of activities that are performed to meet the defined CMMC objectives.

Source: CMMC

Privilege

A right granted to an individual, a program, or a process.

Source: CNSSI 4009, NIST SP 800-12 Rev 1

Privileged Account

A user, system, or network account authorized (and, therefore, trusted) to perform security-relevant functions that ordinary accounts are not authorized to perform.

Source: NIST SP 800-171 Rev. 2 (adapted)

Privileged User

A user who is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

Source: NIST SP 800-171 Rev. 2

Procedure

The documented details for how an activity is implemented to achieve a desired outcome. A procedure should provide enough detail for a trained individual to perform the activity.

Source: CMMC

Process

A procedural activity that is performed to implement a defined objective.

Source: CMMC

Proxy (Web Proxy)

An application that "breaks" the connection between client and server. The proxy accepts certain types of traffic entering or leaving a network and processes it and forwards it.

Note: This effectively closes the straight path between the internal and external networks making it more difficult for an attacker to obtain internal addresses and other details of the organization's internal network. Proxy servers are available for common Internet services; for example, a hypertext transfer protocol (HTTP/HTTPS) proxy used for Web access.

Source: CNSSI 4009 (adapted)

Real Time, Real-Time (modifier)

Pertaining to the performance of a computation during the actual time that the related physical process transpires so that the results of the computation can be used to guide the physical process.

Source(s): NIST SP 800-82 Rev. 2, NISTIR 6859

Recovery

Actions necessary to restore data files of an information system and computational capability after a system failure.

Source: CNSSI 4009

Red Team

A group of people authorized and organized to emulate a potential adversary's attack or exploitation capabilities against an enterprise's security posture. The Red Team's objective is to improve enterprise Information Assurance by demonstrating the impacts of successful attacks and by demonstrating what works for the defenders (i.e., the Blue Team) in an operational environment.

Source: CNSSI 4009

Red Teaming

The act(s) performed by a "red team" in order to identify weaknesses, vulnerabilities, procedural shortcomings, and misconfigurations within an organization's cyber environment. Red Teaming includes creation of a "Rules of Engagement" document by which the red team honors over the course of their actions. It is expected that the Red Team will produce a final report at the end of the event period.

Source: CMMC

Regularly

On a regular basis: at regular intervals.

Source: Oxford Dictionary

Remote Access

Access to an organizational system by a user (or a process acting on behalf of a user) communicating through an external network (e.g., the Internet).

Source: NIST SP 800-171 Rev. 2

Removable Media

Portable data storage medium that can be added to or removed from a computing device or network.

Note: Examples include, but are not limited to: optical discs (CD, DVD, Blu-ray); external/removable hard drives; external/removable Solid-State Disk (SSD) drives; magnetic/optical tapes; flash memory devices (USB, eSATA, Flash Drive, Thumb Drive); flash memory cards (Secure Digital, CompactFlash, Memory Stick, MMC, xD); and other external/removable disks (floppy, Zip, Jaz, Bernoulli, UMD).

See Glossary: *Portable Storage Device*

Source: CNSSI 4009

Reporting [forensics]

The final phase of the computer and network forensic process, which involves reporting the results of the analysis; this may include describing the actions used, explaining how tools and procedures were selected, determining what other actions need to be performed (e.g., forensic examination of additional data sources, securing identified vulnerabilities, improving existing security controls), and providing recommendations for improvement to

policies, guidelines, procedures, tools, and other aspects of the forensic process. The formality of the reporting step varies greatly depending on the situation.

Source: NIST SP 800-86

Residual Risk

Portion of risk remaining after security measures have been applied.

Source: NIST SP 800-33 (adapted)

Resilience

The ability to prepare for and adapt to changing conditions and withstand and recover rapidly from disruptions. Resilience includes the ability to withstand and recover from deliberate attacks, accidents, or naturally occurring threats or incidents.

Source: PPD 21

Restricted Information Systems

Systems (and associated IT components comprising the system) that are configured based on government requirements (i.e., 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).

Source: CMMC

Risk

A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of:

- the adverse impacts that would arise if the circumstance or event occurs and
- the likelihood of occurrence.

System-related security risks are those risks that arise from the loss of confidentiality, integrity, or availability of information or systems. Such risks reflect the potential adverse impacts to organizational operations, organizational assets, individuals, other organizations, and the Nation.

Source: FIPS 200 (adapted)

Risk Analysis

The process of identifying the risks to system security and determining the likelihood of occurrence, the resulting impact, and the additional safeguards that mitigate this impact. Part of risk management and synonymous with risk assessment.

Source: NIST SP 800-27

Risk Assessment

- 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.
- Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place. Synonymous with risk analysis.

Source: NIST SP 800-171

Risk Management (RM)

The program and supporting processes to manage information security risk to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, and includes:

- establishing the context for risk-related activities,
- assessing risk,
- responding to risk once determined, and
- monitoring risk over time.

Source: CNSSI 4009

Risk Mitigation

Prioritizing, evaluating, and implementing the appropriate risk-reducing controls/ countermeasures recommended from the risk management process.

Source: CNSSI 4009

Risk Mitigation Plan

A strategy for mitigating risk that seeks to minimize the risk to an acceptable level.

Source: CERT RMM v1.2

Risk Tolerance

The level of risk an entity is willing to assume in order to achieve a potential desired result.

Source: CNSSI 4009

Root-Cause Analysis

An approach for determining the underlying causes of events or problems as a means of addressing the symptoms of such events as they manifest in organizational disruptions.

Source: CERT RMM v1.2

Root Directory

The top-level directory in a folder hierarchy.

Source: CMMC

Safeguards

The protective measures prescribed to meet the security requirements (i.e., confidentiality, integrity, and availability) specified for an information system. Safeguards may include security features, management constraints, personnel security, and security of physical structures, areas, and devices. Synonymous with security controls and countermeasures.

Source: FIPS 200

Sandboxing

A restricted, controlled execution environment that prevents potentially malicious software, such as mobile code, from accessing any system resources except those for which the software is authorized.

Source: CNSSI 4009

Scanning

Sending packets or requests to another system to gain knowledge about the asset, processes, services, and operations.

Source: CNSSI 4009 (adapted)

Security Assessment

See Glossary: *Security Control Assessment*

Security Control Assessment (Security Assessment, Security Practice 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 a system or organization.

Source: CNSSI 4009 (adapted)

Security Domain

An environment or context that includes a set of system resources and a set of system entities that have the right to access the resources as defined by a common security policy, security model, or security architecture.

Source: CNSSI 4009

Security Operations Center (SOC)

A centralized function within an organization utilizing people, processes, and technologies to continuously monitor and improve an organization's security posture while preventing, detecting, analyzing, and responding to cybersecurity incidents.

Source: CMMC

Security Policy

Security policies define the objectives and constraints for the security program. Policies are created at several levels, ranging from organization or corporate policy to specific operational constraints (e.g., remote access). In general, policies provide answers to the questions "what" and "why" without dealing with "how." Policies are normally stated in terms that are technology-independent.

Source: NIST SP 800-82 Rev 2

Security Protection Assets

Security provide security functions or capabilities within the contractor's CMMC Assessment Scope.

Source: CMMC

Security Practice Assessment

See Glossary: *Security Control Assessment*

Sensitive Information

Information where the loss, misuse, or unauthorized access or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under 5 U.S.C. Section 552a (the Privacy Act).

Source: NIST SP 800-53 Rev 4 (adapted)

Separation of Duties

Refers to the principle that no user should be given enough privileges to misuse the system on their own. For example, the person authorizing a paycheck should not also be the one who can prepare them. Separation of duties can be enforced either statically (by defining conflicting roles, i.e., roles which cannot be executed by the same user) or dynamically (by enforcing the control at access time).

Source: NIST SP 800-192

Service Continuity Plan

A service-specific plan for sustaining services and associated assets under degraded conditions.

Source: CERT RMM v1.2

SHA-256

A Secure Hash Algorithm (SHA) that produces a condensed representation of electronic data, or message digest, 256 bits in length.

Source: FIPS 180-4

Situational Awareness (SA)

Within a volume of time and space, the perception of an enterprise's security posture and its threat environment; the comprehension/meaning of both taken together (risk); and the projection of their status into the near future.

Source: CNSSI 4009

Specialized Asset

The following are considered specialized assets for CMMC: Government Property, Internet of Things (IoT) or Industrial Internet of Things (IIoT), Operational Technology (OT), and Restricted Information Systems.

Source: CMMC

Split Tunneling

The process of allowing a remote user or device to establish a non-remote connection with a system and simultaneously communicate via some other connection to a resource in an external network. This method of network access enables a user to access remote devices (e.g., a networked printer) at the same time as accessing uncontrolled networks.

Source: NIST SP 800-171

Spyware

Software that is secretly or surreptitiously installed into an information system to gather information on individuals or organizations without their knowledge; a type of malicious code.

Source: NIST SP 800-53 Rev 5

Standards

A document, established by consensus and approved by a recognized body, that provides for common and repeated use, rules, guidelines or characteristics for activities or their results, aimed at the achievement of the optimum degree of order in a given context.

Note: Standards should be based on the consolidated results of science, technology and experience, and aimed at the promotion of optimum community benefits.

Source: NISTIR 8074 Vol. 2

Standard Process

An operational definition of the basic process that guides the establishment of a common process in an organization. A standard process describes the fundamental process elements that are expected to be incorporated into any defined process. It also describes relationships (e.g., ordering, interfaces) among these process elements.

See Glossary: *Defined Process*

Source: CERT RMM v1.2

Subnetwork

A subordinate part of an organization's enterprise network.

Source: CMMC

Supply Chain

A system of organizations, people, activities, information, and resources, possibly international in scope, that provides products or services to consumers.

Source: CNSSI 4009

Supply Chain Attack

Attacks that allow the adversary to utilize implants or other vulnerabilities inserted prior to installation in order to infiltrate data, or manipulate information technology hardware, software, operating systems, peripherals (information technology products) or services at any point during the life cycle.

Source: CNSSI 4009

Supply Chain Risk Management (SCRM)

A systematic process for managing supply chain risk by identifying susceptibilities, vulnerabilities, and threats throughout the supply chain and developing mitigation strategies to combat those threats whether presented by the supplier, the supplied product and its subcomponents, or the supply chain (e.g., initial production, packaging, handling, storage, transport, mission operation, and disposal).

Source: CNSSD No. 505

Sustain

Maintain a desired operational state.

Source: CERT RMM v1.2

System Assets

Any software, hardware (IT, OT, IoT), data, administrative, physical, communications, or personnel resource within an information system.

Source: CNSSI 4009

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.

See Glossary: *CMMC Assessment Scope*

Source(s): CNSSI 4009-2015 under authorization boundary NIST SP 800-53 Rev. 4, NIST SP 800-53A Rev. 1, NIST SP 800-37 Rev. 1.

System Integrity

The quality that a system has when it performs its intended function in an unimpaired manner, free from unauthorized manipulation of the system, whether intentional or accidental.

Source: NIST SP 800-27

System Interconnection

A system interconnection is defined as the direct connection of two or more IT systems for the purpose of sharing data and other information resources.

Source: NIST 800-47

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: CNSSI 4009

Tampering

An intentional but unauthorized act resulting in the modification of a system, components of systems, its intended behavior, or data.

Source: NIST SP 800-53 Rev 5

Test Equipment

Hardware and/or associated IT components used in the testing of products, system components, and contract deliverables (e.g., oscilloscopes, spectrum analyzers, power meters, and special test equipment).

Source: CMMC

Threat

Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, or the Nation through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service.

Source: NIST SP 800-30 Rev 1

Threat Actor

An individual or a group posing a threat.

Source: NIST SP 800-150

Threat Intelligence

Threat information that has been aggregated, transformed, analyzed, interpreted, or enriched to provide the necessary context for decision-making processes.

Source: NIST SP 800-150

Threat Monitoring

Analysis, assessment, and review of audit trails and other information collected for the purpose of searching out system events that may constitute violations of system security.

Source: CNSSI 4009

Trigger

A set of logic statements to be applied to a data stream that produces an event when an anomalous incident or behavior occurs.

Source: CNSSD No. 504 (adapted)

Trojan Horse

A computer program that appears to have a useful function, but also has a hidden and potentially malicious function that evades security mechanisms, sometimes by exploiting legitimate authorizations of a system entity that invokes the program.

Source: CNSSI 4009

Tunneling

Technology enabling one network to send its data via another network's connections. Tunneling works by encapsulating a network protocol within packets carried by the second network.

Source: CNSSI 4009

Unauthorized Access

Any access that violates the stated security policy.

Source: CNSSI 4009

User

Individual, or (system) process acting on behalf of an individual, authorized to access a system.

Source: NIST SP 800-53 Rev 5

Virus

A computer program that can copy itself and infect a computer without permission or knowledge of the user. A virus might corrupt or delete data on a computer, use e-mail programs to spread itself to other computers, or even erase everything on a hard disk.

See Glossary: *Malicious Code*

Source: CNSSI 4009

Vulnerability

Weakness in an information system, system security procedures, internal controls, or implementation that could be exploited by a threat source.

Source: NIST SP 800-30 Rev 1

Vulnerability Assessment

Systematic examination of an information system or product to determine the adequacy of security measures, identify security deficiencies, provide data from which to predict the effectiveness of proposed security measures, and confirm the adequacy of such measures after implementation.

Source: CNSSI 4009

Vulnerability Management

An Information Security Continuous Monitoring (ISCM) capability that identifies vulnerabilities [Common Vulnerabilities and Exposures (CVEs)] on devices that are likely to be used by attackers to compromise a device and use it as a platform from which to extend compromise to the network.

Source: NISTIR 8011 Vol. 1

Web Proxy

See Glossary: *Proxy*

Whitelist

An approved list or register of entities that are provided a particular privilege, service, mobility, access or recognition.

An implementation of a default deny-all or allow-by-exception policy across an enterprise environment, and a clear, concise, timely process for adding exceptions when required for mission accomplishments.

Source: CNSSI 1011

Acronyms and Abbreviations

The following is a list of acronyms and abbreviations used in the Cybersecurity Maturity Model Certification (CMMC) documentation.

AA	Audit and Accountability
ABAC	Attribute-Based Access Control
AC	Access Control
ACSC	Australian Cyber Security Centre
AES	Advanced Encryption Standard
AIA	Aerospace Industries Association
AM	Asset Management
API	Application Programming Interface
APT	Advanced Persistent Threat
AT	Awareness and Training
AU	Audit and Accountability
BYOD	Bring Your Own Device
C2M2	Cybersecurity Capability Maturity Model
C3PAO	CMMC Third-Party Assessment Organization
CA	Security Assessment
CD-ROM	Compact Disc Read-Only Memory
CDI	Covered Defense Information
CDI	Covered Defense Information
CEA	Council of Economic Advisers
CERT	Computer Emergency Response Team
CERT RMM	CERT® Resilience Management Model
CFR	Code of Federal Regulations
CI	Configuration Item
CIO	Chief Information Officer
CIS	Computer Information System
CIS	Center for Internet Security
CISA	Cybersecurity and Infrastructure Security Agency
CM	Configuration Management
CMMC	Cybersecurity Maturity Model Certification
CNSSD	Committee on National Security Systems Directive
CNSSI	Committee on National Security Systems Instructions

COMSEC	Communications Security
CPI	Critical Program Information
CSF	Cybersecurity Framework
CSIS	Center for Strategic and International Studies
CSP	Credential Service Provider
CTI	Controlled Technical Information
CUI	Controlled Unclassified Information
CVE	Common Vulnerabilities and Exposures
CVMP	Cryptographic Module Validation Program
CWE	Common Weakness Enumeration
D/A	Department/Agency
DCISE	DIB Collaborative Information Sharing Environment
DCS	Distributed Control System
DD	Represents any two-character CMMC Domain acronym
DFARS	Defense Federal Acquisition Regulation Supplement
DHC	Device Health Check
DIB	Defense Industrial Base
DKIM	Domain Key Identified Mail
DMARC	Domain-based Message Authentication, Reporting, and Conformance
DMZ	Demilitarized Zone
DNS	Domain Name System
DNSSEC	Domain Name System Security
DoD	Department of Defense
DoDI	Department of Defense Instruction
DPCI	Derived PIV Credential Issuers
DVD	Digital Versatile Disc
E.O.	Executive Order
eSATA	External Serial Advanced Technology Attachment
ESP	External Service Provider
FAQ	Frequently Asked Question
FAR	Federal Acquisition Regulation
FBI	Federal Bureau of Investigation
FCI	Federal Contract Information
FDDI	Fiber Distributed Data Interface
FDE	Full Disk Encryption
FedRAMP	Federal Risk and Authorization Management Program

FFRDC	Federally Funded Research and Development Center
FIPS	Federal Information Processing Standard
FTP	File Transfer Protocol
GDPR	General Data Protection Regulation
HIPAA	Health Insurance Portability and Accountability Act
HSPD	Homeland Security Presidential Directive
HTTP	Hypertext Transfer Protocol
HTTPS	Hypertext Transfer Protocol Secure
HVA	High-Value Asset
IA	Information Assurance
IA	Identification and Authentication
IBAC	Identity-Based Access Control
IC3	Internet Crime Complaint Center
ICAM	Identity, Credential, and Access Management
ICS	Industrial Control System
ID	Identification
IDA	Identification and Authentication
IDPS	Intrusion Detection and Prevention Systems
IEC	International Electrotechnical Commission
IETF	Internet Engineering Task Force
IIoT	Industrial Internet of Things
IoT	Internet of Things
IP	Internet Protocol
IPSec	Internet Protocol Security
IR	Incident Response
IS	Information System
ISAC	Information Sharing and Analysis Center
ISAO	Information Sharing and Analysis Organization
ISCM	Information Security Continuous Monitoring
ISDN	Integrated Services Digital Network
ISO	International Organization for Standardization
IT	Information Technology
ITIL	Information Technology Infrastructure Library
L#	Level Number
LAN	Local Area Network
LSI	Large-Scale Integration

MA	Maintenance
MAC	Media Access Control
MC	Maturity Capability
MC##	Maturity Capability Number
MDM	Mobile Device Management
MEP	Manufacturing Extension Partnership
MFA	Multifactor Authentication
ML	Maturity Level
ML#	Maturity Level Number
MMC	Multimedia Card
MP	Media Protection
N/A	Not Applicable (NA)
NARA	National Archives and Records Administration
NAS	Networked Attached Storage
NAS	National Aerospace Standard
NCSC	National Cyber Security Centre
NIST	National Institute of Standards and Technology
NISTIR	NIST Interagency (or Internal) Report
NPE	Non-Person Entity
NSA	National Security Agency
NSA/CSS	NSA Central Security Service
NSPD	National Security Presidential Directive
NSTISSD	National Security Telecommunications and Information Systems Security Directive
NTP	Network Time Protocol
NYSSCPA	New York State Society of CPAs
OMB	Office of Management and Budget
OS	Operating System
OSC	Organization Seeking Certification
OT	Operational Technology
OUSD A&S	Office of the Under Secretary of Defense for Acquisition and Sustainment
PCI	Personal Identity Verification Card Issuers
PDA	Personal Digital Assistant
PE	Physical Protection
PGP	Pretty Good Privacy
PII	Personally Identifiable Information
PIV	Personal Identify Verification

PKI	Public Key Infrastructure
PLC	Programmable Logic Controller
POC	Point of Contact
POTS	Plain Old Telephone Service
PP	Physical Protection
PPD	Presidential Policy Directive
PS	Personnel Security
PUB	Publication
RADIUS	Remote Authentication Dial-in User Service
RE	Recovery
Rev	Revision
RF	Radio Frequency
RFC	Request for Comments
RM	Risk Management
RMM	Resilience Management Model
RMM	Risk Management Model
RPO	Recovery Point Objectives
RTO	Recovery Time Objectives
SA	Situational Awareness
SaaS	Software as a Service
SAS	Security Assessment
SC	System and Communications Protection
SCADA	Supervisory Control and Data Acquisition
SCRM	Supply Chain Risk Management
SHA	Security Hash Algorithm
SI	System and Information Integrity
SIEM	Security Integration and Event Management
SMS	Short Message Service
SOC	Security Operations Center
SP	Special Publication
SPF	Sender Policy Framework
SSC	Secure Socket Layer
SSD	Solid-State Disk
SSP	System Security Plan
SSP	Sector Specific Plan
TLS	Transport Layer Security

TTP	Tactics, Techniques, and Procedures
U.S.	United States
UARC	University Affiliated Research Center
UK	United Kingdom
UMD	Universal Media Disc
URL	Uniform Resource Locator
USB	Universal Serial Bus
UTC	Coordinated Universal Time
UUENCODE	Unix-to-Unix Encode
VLAN	Virtual Local Area Network
VoIP	Voice over Internet Protocol
Vol.	Volume
VPN	Virtual Private Network
WAP	Wireless Access Point
WPA2-PSK	WiFi Protected Access-Pre-shared Key
xD	Extreme Digital (flash memory card device)


OFFICE OF THE UNDER SECRETARY OF DEFENSE
ACQUISITION AND SUSTAINMENT
CYBERSECURITY MATURITY MODEL
CERTIFICATION