Defense Industrial Base (DIB) Sector Coordinating Council (SCC) Supply Chain Cyber Training

Cyber/Cybersecurity Maturity Model Certification (CMMC) v2.0

CyberAssist

Agenda

- Module 1: Cybersecurity: Why it is Important?
- Module 2: Cybersecurity Maturity Model Certification
- Module 3: Assessment Process - Interim
- Module 4: Incident Reporting
- Module 5: Cybersecurity Best Practices
- Module 6: Risk Management
- Resource Guide: Glossary, Acronym Guide and Resources for Additional Information
- CMMC Domains
- Survey

Resource Guide

Glossary, Acronym Guide and Additional Resources for More Information

Disclaimer and Overview

Note: CMMC is still going through the rule-making process and certain aspects and requirements may change. Refer to the *Resources Guide* provided in this training for the most updated information.

- The intent of this training is to build awareness for Defense Industrial Base (DIB) suppliers of the likely requirements of the Cybersecurity Maturity Model Certification (CMMC) and their obligation to meet FAR 52.204-21 (basic cyber hygiene) and DFARS 252.204-7012 (specialized data handling and protection requirements).
- This training is self-paced and intended for a range of roles and responsibilities including, but not limited to, executives, project managers and technical staff from organizations seeking certification (OSC) and need to comply with CMMC. Currently, CMMC does not apply to any contractor.
- Note: Completion of this training DOES NOT certify your organization. This training is intended for the purposes of providing awareness of the subjects outlined above.
- The DIB Sector Coordinating Council (SCC) Supply Chain Task Force does not take responsibility for suppliers' certification by the CMMC 3rd Party Assessment Organization (C3PAO).
- This training focuses on U.S. regulations and industry best practices:
  - U.S. Department of Defense (DoD) Chief Information Officer (CIO) Cybersecurity Maturity Model Certification (CMMC) Information
  - National Institute of Standards & Technologies (NIST) publications
  - National Archives & Records Administration (NARA) definitions
  - DIB SCC Supply Chain Task Force – CyberAssist website

Glossary

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

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

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

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

Audit and Accountability (AU): Companies should create, protect, and retain system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate system activity and ensure that the actions of users can be uniquely traced to those users so they can be held accountable. Source*

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

Awareness and Training (AT): The purpose of information security awareness, training, and education is to enhance security by raising awareness of the need to protect system resources, developing skills and knowledge so system users can perform their jobs more securely, and building in-depth knowledge as needed to design, implement, or operate security programs for organizations and systems. Source*

Confidentiality: Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. Source: 44 U.S. Code Sec 3542

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

Controlled Unclassified Information (CUI): Information that requires safeguarding or dissemination controls pursuant to and consistent with law, 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 the Atomic Energy Act of 1954, as amended. Source: E.O. 13556 (adapted)

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

Contractor (Defense Contractor): Any individual, firm, corporation, partnership, association, or other legal non-Federal entity that enters into a contract directly with the DoD to furnish services, supplies, or construction. Source: 32 C.F.R. 158.3

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

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

Event: Any observable occurrence in a system and/or network. Events sometimes provide indication that an incident is occurring. Source: CNSSI 4009

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

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

Hacktivists: Can be similar in expertise to rogue actors, or can bring more expertise… but **Organized around a cause**

Identification and Authentication (IA): Identification and authentication is a technical measure that prevents unauthorized individuals or processes from entering a system. Identification and authentication is a critical building block of information security since it is the basis for most types of access control and for establishing user accountability. Source*

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 Response (IR): 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

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

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

Information System: 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

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)

Maintenance: Any act that either prevents the failure or malfunction of equipment or restores its operating capability. Source: NIST SP 800-82 Rev 2

Maintenance (MA): Companies should perform periodic and timely maintenance on company systems and provide effective controls on the tools, techniques, mechanisms, and personnel used to conduct system maintenance. Source*

Media Protection (MP): Media protection is a requirement that addresses the defense of system media, which can be described as both digital and nondigital. Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed. Source*

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

Personnel Security (PS): Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets through the malicious use or exploitation of their legitimate access to the company's resources. Companies should be vigilant when recruiting and hiring new employees, as well as when an employee transfers or is terminated. Source*

Phishing emails: Broad-based messages sent indiscriminately to very large numbers of recipients with the expectation that at least a small percentage will respond.

Physical Protection (PE): The term physical (and environmental) security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment. Source*

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

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). Source: NIST SP 800-37 Rev 1

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

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 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

Rogue actors: Anyone who developed hacking skills.

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

Security Assessment (CA): A security requirement assessment is the testing and/or evaluation of the management, operational, and technical security requirements on a system to determine the extent to which the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system. Source*

Social engineering: The practice of psychologically manipulating people into performing actions or divulging information that could compromise security.

Spear phishing emails: A method by which attackers (organized perpetrators out for financial gain, trade secrets or national security information) target specific individuals or organizations seeking unauthorized access to data.

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

System and Communication Protection (SC): System and communications protection requirements provide an array of safeguards for the system, including the confidentiality information at rest and in transit. System and communications protection also establishes boundaries that restrict access to publicly accessible information within a system. Using boundary protections, a company can monitor and control communications at external boundaries as well as key internal boundaries within the system. Source*

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Glossary (cont'd)

System and Information Integrity (SI): System and information integrity provides assurance that the information being accessed has not been meddled with or damaged by an error in the system.

System Security Plan: 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

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

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

*https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/DoD-Guidance-for-Reviewing-System-Security-Plans-and-the-NIST-SP-800-11-6-2018.pdf

Source: CMMC Glossary, https://dodcio.defense.gov/Portals/0/Documents/CMMC/Glossary_MasterV2.0_FINAL_202111217_508.pdf

Acronym Guide

AC: Access Control

AU: Audit and Accountability

AT: Awareness and Training

C3PAO: CMMC Third-Party Assessment Organization

CA: Security Assessment

CCP: Certified CMMC Professional

CFR: Code of Federal Regulations

CM: Configuration Management

CMMC: Cybersecurity Maturity Model Certification

CDI: Covered Defense Information

CUI: Controlled Unclassified Information

DCMA: Defense Contract Management Agency

DIB: Defense Industrial Base

DIBCAC: Defense Industrial Base Cyber Assessment Center

DFARS: Defense Federal Acquisition Regulation Supplement

DoD: Department of Defense

DoD CUI: Department of Defense Controlled Unclassified Information

FAR: Federal Acquisition Regulation

FCI: Federal Contract Information

IA: Identification and Authentication

IR: Incident Response

IT: Information Technology

MA: Maintenance

MP: Media Protection

OSC: Organizations Seeking Certification

PS: Personnel Security

PE: Physical Protection

POAM: Plan of Action and Milestones

RA: Risk Assessment

RP: Registered Practitioner

RPO: Registered Provider Organization

SC: System and Communications Protection

SPRS: Supplier Performance Risk System

SI: System and Information Integrity

SSP: System Security Plan

Resources Available for More Information

The following resources provides additional information and the latest news related to CMMC and cybersecurity. We recommend you reference these resources for the latest information and guidance on CMMC and cybersecurity.

- DoD CMMC page: https://dodcio.defense.gov/CMMC/
- DIB SCC Cyber Assist site: https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/
- CMMC Level 1: https://ndisac.org/dibscc/cyberassist/cybersecurity-maturity-model-certification/level-1/
- CMMC AB Town Halls: https://cmmcab.org/#townhall
- SEI CMMC Website: https://www.sei.cmu.edu/go/cmmc
- Supplier Performance Risk System: https://www.sprs.csd.disa.mil/
- CMMC Self-Assessment Guide (Level 1): https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level1_V2.0_FinalDraft_20211210_508.pdf
- CMMC Self-Assessment Guide (Level 2): https://dodcio.defense.gov/Portals/0/Documents/CMMC/AG_Level2_MasterV2.0_FINAL_202112016_508.pdf
- NIST Risk Management Framework Training: https://csrc.nist.gov/Projects/risk-management/rmf-training
- National Archives (NARA) CUI Information: https://www.archives.gov/cui
- CUI Program Blog: https://isoo.blogs.archives.gov/
- Federal Register: https://www.federalregister.gov/

Resources Available for More Information (cont'd.)

- Capability Maturity Model Integration (CMMI): https://cmmiinstitute.com
- CERT Resilience Management Model (CERT-RMM): https://cert.org/resilience
- National Defense Information Sharing and Analysis Center (NDISAC): https://ndisac.org/
- NIST News Feb. 2021: https://www.nist.gov/news-events/news/2021/02/nist-offers-tools-help-defend-against-state-sponsored-hackers
- National Institutes of Standards and Technology (NIST) - Cybersecurity: https://www.nist.gov/cybersecurity
- Center for Internet Security (CIS): https://www.cisecurity.org/
- Federal Trade Commission, Cybersecurity for Small Business: https://www.ftc.gov/system/files/attachments/cybersecurity-small-business/cybersecuirty_sb_factsheets_all.pdf
- Department of Homeland Security (DHS): https://www.dhs.gov/
- Cybersecurity & Infrastructure Security Agency (CISA): https://www.cisa.gov/
- U.S. Computer Emergency Readiness Team: https://us-cert.cisa.gov/
- Small Business Administration: https://www.sba.gov/
- Cloud Computing FAQs: https://ndisac.org/dibscc/cyberassist/awareness/cloud-computing-faqs/
- National Cyber Security Centre (Information for Small and medium sized organisations): Small & medium sized organisations - NCSC.GOV.UK
- Protecting Your Small Business: Ransomware
- Protecting Your Small Business: Phishing
- Protecting Your Small Business: Multi-Factor Authentication