Advanced Technical Solutions

CMMC Acronym Cheat Sheet

Acronym	Definition
CMMC	The **Cybersecurity Maturity Model Certification** covers three maturity levels ranging from "Basic Cybersecurity Hygiene" to "Advanced/Progressive." In time, you will need to demonstrate CMMC compliance to do business – as a prime or subcontractor – with the U.S. Department of Defense.
CMMC-AB	The **CMMC Accreditation Body** oversees a community of qualified, trained, and trustworthy assessors who can assess your performance against the controls and best practices outlined in CMMC.
CUI	**Controlled Unclassified Information** is information that requires safeguarding or dissemination controls pursuant to and consistent with applicable law, regulations, and government-wide policies but is not classified under Executive Order 13526 or the Atomic Energy Act, as amended.
DIB	The **Defense Industrial Base** is the collection of organizations that support the mission of the Department of Defense. DIB includes some of the nation's largest aerospace and defense corporations, as well as thousands of smaller businesses that contribute to the successful execution of DOD missions.
EDR	**Endpoint Detection and Response**, also known as endpoint threat detection and response (ETDR), is an integrated endpoint security solution that combines real-time continuous monitoring and collection of endpoint data with rules-based automated response and analysis capabilities.

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.
FedRAMP	The **Federal Risk and Authorization Management Program** provides a standardized approach to security authorizations for Cloud Service Offerings. FedRAMP is a government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services.
FIPS	**Federal Information Processing Standards** is a set of standards that describe document processing, encryption algorithms and other information technology processes for use within non-military federal government agencies and by government contractors and vendors who work with these agencies.
POAM	As part of any NIST 800-171/CMMC assessment, you should create **Plans of Action & Milestones** to map out next steps for remediation.
SIEM	A **Security Incident & Event Management system** combines Security Event Management (SEM), which analyzes event and log data in real-time to provide event correlation, threat monitoring, and incident response, with Security Information Management (SIM), which gathers and analyzes log data and generates a report.
SPRS	**Supply Performance Risk System** is DOD's single, authorized application to retrieve information about a supplier's performance. This web-enabled enterprise application gathers, processes, and displays data about supplier performance – including compliance with NIST 800-171.
SSP	A **System Security Plan** is a "living" document that articulates an organization's security policies and posture.
OSC	**Organization Seeking Certification** within the DIB seeking CMMC certification for Maturity Levels 1-3.
RPO	**Registered Provider Organizations** that provide advice, consulting, and recommendations to OSCs but do not conduct certified assessments. CMMC-AB authorizes RPOs to represent the organization as familiar with the basic constructs of the CMMC standard. They have agreed to the CMMC-AB Code of Professional Conduct.
RP	**Registered Practitioners** are authorized by CMMC-AB to provide non-certified advisory services, informed by basic training on the CMMC standard. RPs do not conduct certified CMMC assessments. RP's must be associated with an RPO.

C3PAO	**CMMC Third-Party Assessor Organizations** are authorized by the CMMC-AB to manage the Organizations Seeking Certification (OSCs) assessment process. Defense contractors and subcontractors may only obtain certification through a C3PAO.
GCC High	Microsoft maintains several clouds, including Microsoft Office 365 (Commercial) and **Office 365 GCC (Government Community)**. Additionally, Microsoft created a cloud specifically for DOD, with authorization for impact Level 3 in Azure Government.
MFA	**Multi-factor Authentication** is a security feature offered by many websites, applications and devices that dramatically improves account security. Sometimes MFA is also referred to as Two-Factor Authentication or 2FA. Technically, MFA could refer to a system where there are more than two forms of authentication.
NIST 800-171	The **National Institute of Standards and Technology** promotes and maintains measurement standards and guidelines to help protect federal agencies' information and IT systems. NIST 800-171, Protecting Controlled Unclassified Information In Nonfederal Information Systems and Organizations, was first published in June 2015 but has since been updated in response to evolving cyberthreats. It offers guidelines on how to securely access, transmit, and store CUI in nonfederal information systems and organizations.
FAR	The **Federal Acquisition Regulation** is the primary regulation for use by all executive agencies to acquire supplies and services with appropriated funds. FAR is jointly issued by The Department of Defense (DoD), the U.S. General Services Administration (GSA), and the National Aeronautics and Space Administration (NASA).
DFARS	**Defense Federal Acquisition Regulation Supplement** (DFARS) is a set of cybersecurity regulations administered by the Department of Defense (DoD) for external contractors and suppliers. The DFARS implements and supplements the FAR and provides detailed information about applying the regulation for DoD contractors, minimum requirements, and options to meet compliance standards.
ATS	**Advanced Technical Solutions (ATS)** is a leading Information Technology (IT) and Information Systems (IS) service provider headquartered in Rochester, NY, serving small, medium, and large organizations across New York State for more than 18 years. ATS is a Registered Provider Organization (RPO) with the CMMC Accreditation Body (CMMC AB).