Trustwave®

Cybersecurity Maturity Model Certification

Department of Defense (DoD) has always required contractors/suppliers to meet certain cybersecurity standards and has now instituted the updated Cybersecurity Maturity Model Certification (CMMC) 2.0 as a standardized framework.

CMMC and DoD

CMMC creates a process to enable companies to satisfy the security requirements set forth in the Defense Federal Acquisition Regulation Supplement and is overseen by the Office of the Under Secretary of Defense for Acquisitions and Sustainment (DFARS). The National Institute of Standards and Technology (NIST) Special Publications (SP) 800-171 and 800-172 serve as the basis for these measures.

The DoD requires proof of CMMC compliance to ensure protection of federal contract information (FCI) and controlled unclassified information (CUI) from nation-state and nefarious actors, while keeping the supply chain running safely. The DoD announced the release of CMMC 2.0, aimed to simplify implementation and working with an advisory partner is still the best method to guarantee quick, trouble-free preparation to meet the necessary Level for handling DoD data.

The CMMC Accreditation Body (CMMC-AB) has authorized Trustwave Government Solutions (TGS) as a Registered Provider Organization (RPO) and many of its team as Registered Practitioners (RP). Before the CMMC's implementation, our team successfully assisted DoD contractors with NIST and DFARS compliance, and we have been assisting DoD customers with meeting these compliance requirements and specifically CMMC since the rollout started.

The new framework now has three levels:

- **Level 1 Foundational:** Applies to companies that focus on the protection of FCI. It will be based on the 17 controls found in FAR 52.204-21, Basic Safeguarding of Covered Contractor.
- **Level 2 Advanced:** Builds upon Level 1 requirements and introduces additional practices to enhance cybersecurity maturity based on the 110 controls from NIST SP 800-171. This Level has additional requirements to ensure the protection of the two types of CUI data – prioritized and non-prioritized.
- **Level 3 Expert:** Adopts an additional subset of the 35 enhanced controls from NIST SP 800-172 to protect CUI from advanced persistent threats (APT).

Two key question you need to answer in meeting the new compliance requirements are:

- Is your cybersecurity maturity at the desired level to participate in the US government contract bidding process?
- How can you implement and stay compliant with these new best practices for managing cybersecurity?

Trustwave, a proven leader in employing and managing cybersecurity, can help you meet these new compliance requirements, especially with the US Defense Industrial Base (DIB) sector. Let Trustwave help you customize made-to-order compliant cybersecurity solutions to propel you on your security maturity journey to meet CMMC standards.

Our trusted experts can help by reviewing your current security posture/maturity, against CMMC standards, and preparing artifactsfor examination by the Certified Third-Party Assessor Organizations' (C3PAO) findings. Trustwave will meet you where you stand to proactively protect your IT investments and advise you on CMMC prerequisites. Trustwave offers a CMMC readiness assessment to assist clients preparing for auditing and reviewing security roadmaps.

Depending on certification goal, Trustwave can provide guidance, remediation plans, and proven security testing results with consulting, testing and managed services, plus a large array of security products and tools to help protect your organization's security posture. These services and tools will help you to:

- Validate compliance with existing DFARS and Supplier Performance Risk System (SPRS) requirements
- Acquire greater visibility into the data assets you are responsible for securing
- Test and identify vulnerabilities with next step solutions and compliance
- Review system security plans and help prepare for a visit from the assessors
- Rapidly mitigate the impact of a security incident with a comprehensive incident response plan
- Customize and scale flexible visibility into situational awareness for your cybersecurity assets all in one place to suit your unique needs

Assessment Approach

1. **Understanding the Requirements:** The first step in the assessment process is to gain a thorough understanding of the CMMC requirements for the applicable Level 1/2/3. This includes working with the client in reviewing the CMMC documentation, guidelines, and control families to identify the specific cybersecurity practices and processes that need to be in place.
2. **Gap Analysis:** Trustwave consultants will conduct a comprehensive gap analysis to identify any gaps or deficiencies in the client's current cybersecurity posture in relation to the CMMC requirements. This will involve reviewing the client's existing system security plan (SSP), policies, procedures, and technical controls to identify areas that need improvement.
3. **Risk Assessment:** Trustwave consultants will conduct a risk assessment to identify potential vulnerabilities and threats that can impact the client's sensitive data. This will involve evaluating the client's systems, networks, applications, and processes to identify potential risks and their potential impact on the confidentiality, integrity, and availability of the data.
4. **Remediation Plan:** Based on the findings from the gap analysis and risk assessment, Trustwave consultants will work with the client to develop a remediation plan tailored to the client's specific needs. This will include recommendations for addressing identified gaps and deficiencies and implementing appropriate cybersecurity controls and practices to meet the requirements for the applicable Level 1/2/3.
5. **Implementation Support:** Trustwave will provide ongoing support to the client during the implementation phase. This will involve assisting the client in implementing the recommended cybersecurity controls and practices, providing guidance on best practices, and conducting periodic reviews to ensure that the client is on track to meet the requirements.
6. **Documentation, Reporting, and Pre-certification Assessment:** Finally, Trustwave will help the client in documenting their cybersecurity processes and practices in alignment with the requirements. This will involve preparing detailed reports and documentation to demonstrate compliance with the CMMC requirements to the DoD or other relevant parties, as needed. Before undergoing an official CMMC assessment, Trustwave will conduct a pre-certification assessment to ensure that the client's cybersecurity program meets the chosen CMMC level requirements. This will involve a comprehensive review of all cybersecurity practices and controls to ensure they are in place and functioning effectively.

CMMC LEVEL	DESCRIPTION	CONTROLS	TRUSTWAVE CAPABILITY
#1 Foundation	Organizations at this level are expected to implement basic cybersecurity practices to safeguard Federal Contract Information (FCI)	• Access Control (AC) - 4 • Identification and Authentication (IA) - 2 • Media Protection (MP) - 1 • Physical Protection (PE) - 4 • System and Communications Protection (SC) - 2 • System and Information Integrity (SI) - 4	• Conduct initial cybersecurity assessments to identify gaps and vulnerabilities • Develop and implement cybersecurity policies and procedures • Provide employee training and awareness programs • Assist with developing and implementing basic access controls, such as password policies and user account management
#2 Advanced	Organizations at this level are required to implement intermediate cybersecurity practices to protect Controlled Unclassified Information (CUI).	• Access Control (AC) - 18 • Awareness and Training (AT) - 3 • Audit and Accountability (AU) - 9 • Configuration Management (CM) - 9 • Identification and Authentication (IA) - 9 • Incident Response (IR) - 3 • Maintenance (MA) - 6 • Media Protection (MP) - 8 • Personnel Security (PS) - 2 • Physical Protection (PE) - 2 • Risk Assessment (RA) - 3 • Security Assessment (CA) - 4 • System and Communications Protection (SC) - 14 • System and Information Integrity (SI) - 3	• Conduct comprehensive cybersecurity risk assessments and develop risk mitigation strategies • Assist with implementing and managing security controls, such as firewalls, antivirus, and intrusion detection systems. • Develop incident response plans and provide guidance on responding to cybersecurity incidents • Assist with third-party risk management and supply chain cybersecurity
#3 Expert	Organizations at this level must implement advanced cybersecurity practices from NIST 800-172 to protect CUI and reduce the risk of advanced persistent threats (APTs). The actual controls from the 35 enhanced requirements have not been defined.	• Access Control (AC) - 3e • Awareness and Training (AT) - 2e • Configuration Management (CM) - 3e • Identification and Authentication (IA) - 3e • Incident Response (IR) - 2e • Personnel Security (PS) - 2e • Risk Assessment (RA) - 7e • Security Assessment (CA) - 1e • System and Communications Protection (SC) - 5e • System and Information Integrity (SI) - 7e (Note: AU, MA, MP, and PE do not have enhanced controls and have been omitted.)	• Conduct in-depth cybersecurity assessments to identify potential vulnerabilities and weaknesses • Develop and implement advanced security controls, such as multifactor authentication, encryption, and security information and event management (SIEM) systems • Provide guidance on security architecture and network segmentation • Develop and implement advanced threat hunting and monitoring techniques • Assist with continuous monitoring and assessment of cybersecurity posture

Trustwave is a leading cybersecurity and managed security services provider focused on comprehensive threat detection, response, investigation, and eradication. Offering a comprehensive portfolio of managed security services, consulting and professional services, and enterprise cloud & data protection technology, Trustwave helps businesses embrace digital transformation securely with customers in 96 countries.

Trustwave®

www.trustwave.com

CMMC_0523