Trellix carahsoft.

Trellix

Trellix & CMMC 2.0

Simplified – and how we can help!

6000 Headquarters Drive
Plano, TX 75024

trellix.com

Trellix & CMMC 2.0

Simplified – and how we can help!

Thank you for downloading this Trellix whitepaper. Master Government Aggregator® and Distributor for Trellix's Cybersecurity solutions available via GSA, NASPO, CMAS, and other contract vehicles.

To learn how to take the next step toward acquiring Trellix's solutions, please check out the following resources and information:

For additional resources:
carah.io/TrellixResources

For upcoming events:
carah.io/TrellixEvents

For additional Trellix products:
carah.io/TrellixSolutions

For additional Cybersecurity solutions:
carah.io/Cybersecurity

To set up a meeting:
Trellix@carahsoft.com
855-462-2333

To purchase, check out the contract vehicles available for procurement:
carah.io/TrellixContracts

For more information, contact Carahsoft or our reseller partners:
Trellix@carahsoft.com | 855-462-2333

Trellix & CMMC 2.0

Simplified – and how we can help!

6000 Headquarters Drive
Plano, TX 75024

trellix.com

Summary

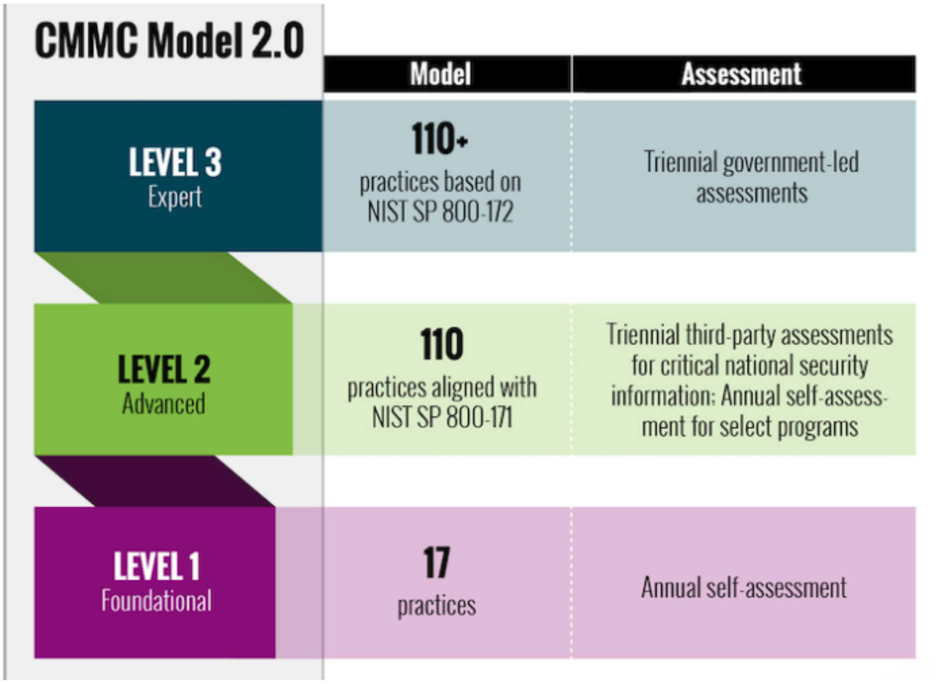
The Cybersecurity Maturity Model Certification (CMMC) is a unified standard for implementing cybersecurity across the defense industrial base (DIB). The base includes over 300,000 companies in the supply chain and the CMMC is the DoDs response to the many compromises of PII and sensitive information that we have seen over the past years. The CMMC 1.0 model was released by the US Department of Defense on January 31, 2020, and CMMC 2.0 released in November of 2021.

Is there any action I should take now?

Yes, since the CMMC release, certifications have now been included in requests for information (RFIs) and requests for proposal (RFPs), since mid 2020. This means you need to familiarize yourself with the process and the technical requirements – and this is not only for certification, but also working in your long-term cybersecurity agility.

The CMMC Framework

The CMMC model is broken out into three levels – and this is how it measures cyber-security maturity. See *Figure 1* below, highlighting Level 1, *Foundational,* through Level 3, *Expert* – showing the number of practices within each level.



CMMC Model 2.0	Model	Assessment
LEVEL 3 Expert	110+ practices based on NIST SP 800-172	Triennial government-led assessments
LEVEL 2 Advanced	110 practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assessment for select programs
LEVEL 1 Foundational	17 practices	Annual self-assessment

Figure 1.

Contractors can begin by identifying which level their organization falls under:

- **Level 1** (*Foundational*) – Nothing has really changed with this level in the newer model. If you handle FCI but not CUI, you fall into a Level 1. These organizations are expected to implement the Federal Acquisition Regulation's 17 most basic cybersecurity controls. ALL Federal contractors are required to implement these 17 basic safeguards, which focus for instance on physical protection and access control. Although this is the lowest level, implementing these controls is not an overnight process, so contractors should remain diligent when doing so.
- **Level 2** (*Advanced*) – Formerly Level 2/3. If your business is in the manufacturing sector, and/or provides parts and services for weapons, and it is very likely that your small business will fall under this category.
- **Level 3** (*Expert*) – Formerly Level 4/5. Large prime contractors and those of us that work on super critical national security programs that are significant targets of nation-state adversaries, and any Advanced Persistent Threat (APT) will have to focus on Level 3. These organizations handle CUI, but they also likely handle secret and, potentially, top-secret information.

Who must comply with CMMC?

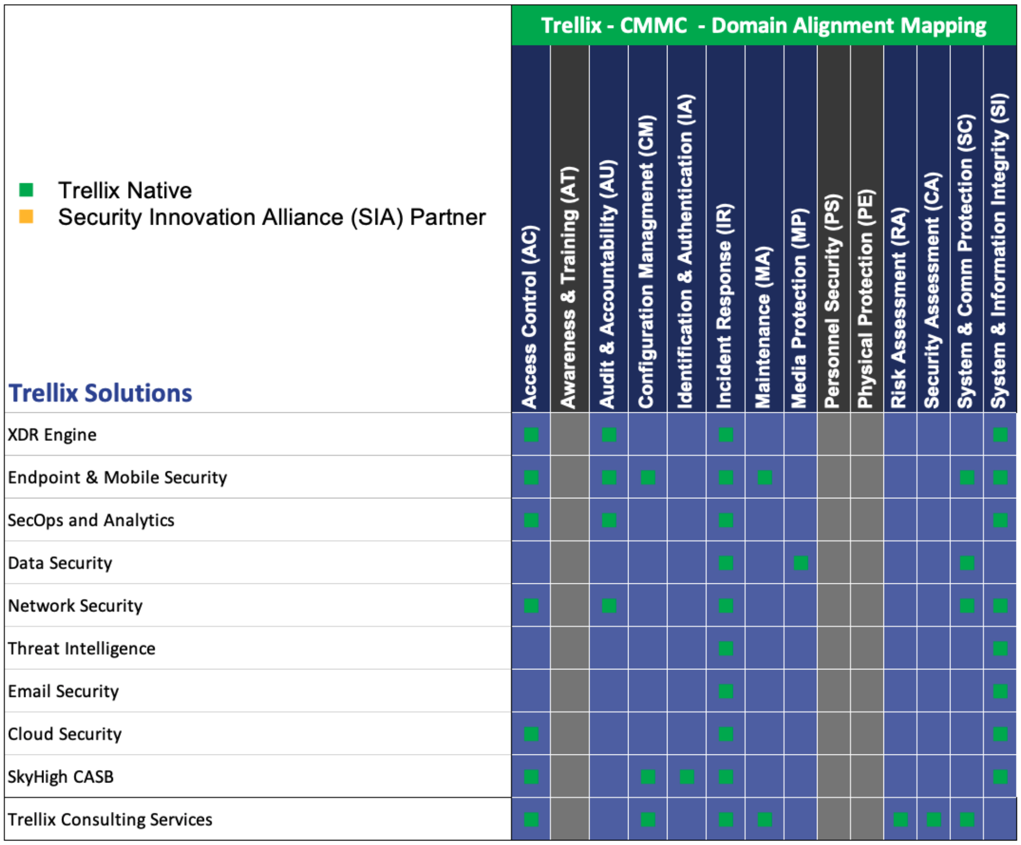
These contractors must all be CMMC-certified by September 30, 2025.

- All DoD contractors
- All DoD subcontractors
- All suppliers at all tiers along the supply chain
- DoD small businesses suppliers
- Commercial item suppliers who process, handle, or store controlled unclassified information
- Foreign suppliers
- All DoD contractor team members that handle Controlled Unclassified Information (CUI) such as IT Managed Service Providers

How can Trellix help?

Trellix is the world’s largest pure play cybersecurity organization, and we know the mission of the DoD is unique. Both data intelligence and threats are no longer confined to the walls of agencies or institutions—and neither should your security. By partnering together, we offer an open and integrated security system designed to mitigate risk, protect data and ensure visibility across all your devices, platforms and architectures.

Our technologies can help you meet your cybersecurity model maturity, and we have a number of integrated capabilities that can bring your organization to its end goal. Our staff understands the certification and validation requirements and Trellix has a dedicated group of individuals who solely support the Public Sector and the work you do. See *Figure 2* below mapping the CMMC domains to Trellix capabilities.



🟩 Trellix Native
🟧 Security Innovation Alliance (SIA) Partner

	Trellix - CMMC - Domain Alignment Mapping													
Trellix Solutions	Access Control (AC)	Awareness & Training (AT)	Audit & Accountability (AU)	Configuration Managmenet (CM)	Identification & Authentication (IA)	Incident Response (IR)	Maintenance (MA)	Media Protection (MP)	Personnel Security (PS)	Physical Protection (PE)	Risk Assessment (RA)	Security Assessment (CA)	System & Comm Protection (SC)	System & Information Integrity (SI)
XDR Engine	🟩		🟩			🟩								🟩
Endpoint & Mobile Security	🟩		🟩	🟩		🟩	🟩						🟩	🟩
SecOps and Analytics	🟩		🟩			🟩								🟩
Data Security						🟩		🟩					🟩	
Network Security	🟩		🟩			🟩							🟩	🟩
Threat Intelligence						🟩								🟩
Email Security						🟩								🟩
Cloud Security	🟩					🟩								🟩
SkyHigh CASB	🟩			🟩	🟩	🟩								🟩
Trellix Consulting Services	🟩			🟩		🟩	🟩				🟩	🟩	🟩	

Figure 2.

Conclusion

Trellix has a long history of helping our customers meet their cybersecurity needs and goals. CMMC is no different, in fact, this is just one more security framework that we are able to help our customers achieve. If your organization is navigating this security landscape, reach out to your local Trellix team – we know they can help!