

CMMC 2.0 Update

Forensic & Integrity Services
Government Contract Services
January 2022

On November 4, 2021, the Department of Defense (DoD) announced long-anticipated changes to the Cybersecurity Maturity Model Certification (CMMC) program as a result of the internal review that began in March 2021.



The updated model is being called CMMC 2.0. Summary of key changes include the following:

- ▶ Streamlined model to eliminate Levels 2 and 4, leaving:
 - ▶ Level 1 – Foundational (equivalent to previous Level 1)
 - ▶ Level 2 – Advanced (equivalent to previous Level 3)
 - ▶ Level 3 – Expert (equivalent to previous Level 5)
- ▶ CMMC-unique practices and all maturity processes are being eliminated
- ▶ Certain levels will have assessments conducted by Certified Third-Party Assessment Organizations (C3PAOs):
 - ▶ Level 1 contractors and a subset of Level 2 contractors will require annual self-assessments and submission of affirmations by senior company officials
 - ▶ Level 2 contractors managing information critical to national security will require an assessment by a C3PAO
 - ▶ Level 3 contractors will require triennial government-led assessments
- ▶ Certifications can be achieved with an active Plan of Action and Milestones (POA&M) in limited circumstances; however, POA&Ms cannot be for highest-weighted requirements
- ▶ CMMC waivers can be obtained in limited circumstances

DoD rulemaking to address the changes of CMMC 2.0 is expected to take 9 to 24 months and will require two distinct rulemaking processes:

- 1) Updates to Title 32 of the Code of Federal Regulations (CFR)
- 2) Updates to applicable Defense Federal Acquisition Regulation Supplement (DFARS) contracting clauses and Title 48 of the CFR

Although CMMC will not be included as a requirement in any solicitation until the final rules are issued, the DoD is considering incentivizing organizations who undergo and pass a CMMC assessment by a C3PAO in the meantime. Potential incentives that are currently being considered include additional profit margins and source selection evaluation criteria that factors network security of the organization.

The path forward for organizations contracting with the government

While organizations in the Defense Industrial Base wait for the rule finalizations, they should continue their journey of improving their cybersecurity posture. For organizations that already have contracts that include the DFARS 252.204-7012 clause and are targeting Level 2 of CMMC 2.0, it is primarily a continuation of that effort with the main difference being that they will need to undergo an assessment by a C3PAO.

If your organization is targeting Level 1, don't sigh in relief too early. Companies should be mindful of the annual assertions that are required and the potential risks, including False Claims Act (FCA) violations. Deputy Attorney General Lisa O. Monaco's **recent announcement** regarding the creation of the Department of Justice's Civil Cyber-Fraud Initiative indicates the government's focus on FCA as a tool to pursue any assertions.

Actions to take now




Organizations contracting with the government should take advantage of the extended rulemaking process by:

1. Confirming environment/system boundaries by understanding what is controlled unclassified information (CUI) and knowing where the CUI resides within the environment
2. Working with contracting officers to understand what types of CUI either by subcategory or specifically identified in contracts will fall under this umbrella of "critical national security information"
3. Performing assessments to ensure that they are compliant with the National Institute of Standards and Technology SP 800-171 requirements and identifying any POA&Ms for any requirements not met
4. Addressing POA&Ms to minimize the risk to the organization and advance the efforts of working through a resolution
5. Educating key stakeholders, not just IT personnel, on what CUI is and what their roles are in protecting it

Ernst & Young LLP continues to actively monitor the program and rulemaking developments. We are available to assist leaders in understanding and preparing for certification under the new model.

Ernst & Young LLP

Contact us

	<p>Sajeev D. Malaveetil Practice Group Leader Government Contract Services Forensic & Integrity Services</p> <p>+1 703 862 0543 sajeev.malaveetil@ey.com</p>		<p>Courtney Black Principal Government Contract Services Forensic & Integrity Services</p> <p>+1 214 969 9604 courtney.black@ey.com</p>
	<p>Mustafa Zuwawa Senior Manager Government Contract Services Forensic & Integrity Services</p> <p>+1 949 437 0703 mustafa.zuwawa@ey.com</p>		<p>Danielle Dalton Senior Manager Business Consulting</p> <p>+1 206 262 6418 danielle.dalton@ey.com</p>
	<p>Timothy Manning Senior Manager Government Contract Services Forensic & Integrity Services</p> <p>+1 617 375 8355 tim.manning@ey.com</p>		<p>Michael Hinckley Senior Manager Business Consulting</p> <p>+1 615 252 2124 michael.hinckley@ey.com</p>

EY | Building a better working world

EY exists to build a better working world, helping create long-term value for clients, people and society and build trust in the capital markets.

Enabled by data and technology, diverse EY teams in over 150 countries provide trust through assurance and help clients grow, transform and operate.

Working across assurance, consulting, law, strategy, tax and transactions, EY teams ask better questions to find new answers for the complex issues facing our world today.

EY refers to the global organization, and may refer to one or more, of the member firms of Ernst & Young Global Limited, each of which is a separate legal entity.

Ernst & Young Global Limited, a UK company limited by guarantee, does not provide services to clients. Information about how EY collects and uses personal data and a description of the rights individuals have under data protection legislation are available via ey.com/privacy. EY member firms do not practice law where prohibited by local laws. For more information about our organization, please visit ey.com.

About EY Forensic & Integrity Services

Embedding integrity into an organization's strategic vision and day-to-day operations is critical when managing complex issues of fraud, regulatory compliance, investigations and business disputes. Our international team of more than 4,000 forensic and technology professionals helps leaders balance business objectives and risks, build data-centric ethics and compliance programs, and ultimately develop a culture of integrity. We consider your distinct circumstances and needs to assemble the right multidisciplinary and culturally aligned team for you and your legal advisors. We strive to bring you the benefits of our leading technology, deep subject-matter knowledge and broad global sector experience.

Ernst & Young LLP is a client-serving member firm of Ernst & Young Global Limited operating in the US.

© 2022 Ernst & Young LLP.
All Rights Reserved.

US SCORE no: 14618-211US
2208-4084346
ED None

This material has been prepared for general informational purposes only and is not intended to be relied upon as accounting, tax, legal or other professional advice. Please refer to your advisors for specific advice.

ey.com/forensics/governmentcontractservices