17 October,
2024

The DoD unveils the Cybersecurity Maturity Model Certification Program: A primer for defense contractors

By Perry Keating

Managing Director & President, Protiviti Government Services

As cybersecurity threats evolve, the U.S. Department of Defense (DoD) has introduced a long-awaited pivotal framework aimed at bolstering the security of its national defence supply chain: The Cybersecurity Maturity Model Certification (CMMC) Program. The new rule, published on 15 October, marks a significant step towards enhancing cybersecurity across the Defence Industrial Base (DIB).

The CMMC will be rolled out in four phases over three years, allowing time for organisations to adapt and comply without disrupting operations. Phase 1 implementation timelines have been extended by six months from the original proposal, providing more breathing room for contractors to prepare. Under certain conditions, Plans of Action & Milestones (POA&Ms) allow organisations additional time — up to 180 days — to achieve full compliance after obtaining conditional certification status.

The final rule aligns closely with existing National Institute of Standards and Technology (NIST) guidelines, specifically NIST SP 800-171 R2 and selected NIST SP 800-172 requirements.

Why it matters

The rule lays out requirements and standards designed to enforce protection of sensitive, unclassified information that is shared by DoD with its contractors and subcontractors. For defence contractors that do work with the DoD, CMMC compliance is imperative to understanding the key points of this comprehensive rule, including:

- **Streamlined levels for compliance**

The CMMC model has been condensed from five levels to three:
Level 1 focuses on basic safeguarding of Federal Contract Information (FCI).
Level 2 requires broader protection measures for Controlled Unclassified Information (CUI).
Level 3 includes additional requirements to protect against Advanced Persistent Threats (APTs).

- **Assessment requirements**

  The rule introduces a structured approach for assessments, which ensure contractors and subcontractors have implemented necessary cybersecurity standards: Self-assessments are allowed for Level 1 and parts of Level 2. Third-Party Assessment Organisations will conduct independent assessments for higher levels.

- **Clarification on subcontractor responsibilities**

  Clear guidelines have been established regarding subcontractors' roles in achieving CMMC compliance. Prime contractors must ensure that their subcontractors meet relevant cybersecurity requirements based on the sensitivity of information being handled.

- **Enhanced oversight and transparency**

  Increased oversight mechanisms ensure consistency in certification processes conducted by assessors. Measures for greater transparency aim to boost stakeholder confidence in certified entities' integrity.

What they say

Alexander W. Major, Partner, Co-Leader, Government Contracts, McCarter & English, LLP

"While the Final Rule doesn't include much in terms of surprises when describing the 'cookie jar' DoD insists the DIB possesses, it does highlight the challenges that continue to plague DoD in addressing the CUI 'cookies' DoD insists be placed in it. The Final Rule is a long-gestating example of DoD attacking the technology while leaving the root cause of cybersecurity incidents — human error — relatively unscathed."

What we say

The impact of the new rule on the defence industrial base will be significant. While initial compliance efforts may involve increased costs, these investments are crucial in mitigating risks associated with data breaches and intellectual property theft that could otherwise lead to far greater financial losses. By mandating uniform cybersecurity standards across all tiers of contractors and subcontractors, market dynamics within the DIB are expected to shift towards greater trustworthiness and reliability among participants handling sensitive information.

The bottom line

The phased implementation plan along with POA&M flexibility aims at reducing burdens, particularly on small businesses, while maintaining high-security standards essential for overall defence integrity. By

enforcing robust cybersecurity practices uniformly across all involved entities, this rule significantly strengthens supply chain resilience against sophisticated cyber threats targeting both large primes as well as smaller sub-tier suppliers within DIB ecosystems. The finalisation of the CMMC Program rule represents a critical milestone in protecting defence infrastructure from evolving cyber threats by establishing consistent cybersecurity practices across a vast supply chain landscape comprising hundreds of thousands of enterprises.

About Protiviti

Protiviti (www.protiviti.com) is a global consulting firm that delivers deep expertise, objective insights, a tailored approach, and unparalleled collaboration to help leaders confidently face the future. Protiviti and our independent and locally owned Member Firms provide clients with consulting and managed solutions in finance, technology, operations, data, analytics, digital, legal, HR, governance, risk, and internal audit through our network of more than 85 offices in over 25 countries.

Named to the 2024 Fortune 100 Best Companies to Work For® list, Protiviti has served more than 80 percent of Fortune 100 and nearly 80 percent of Fortune 500 companies. The firm also works with smaller, growing companies, including those looking to go public, and with government agencies. Protiviti is a wholly owned subsidiary of Robert Half (NYSE: RHI). Founded in 1948, Robert Half is a member of the S&P 500 index.

Protiviti is a CyberAB RPO organisation and has been supporting companies with CMMC services for seven years. For more information about Protiviti's cybersecurity practice and services, visit us or reach out via email at cmmc@protiviti.com.

About VISION by Protiviti

VISION by Protiviti is a global content resource exploring big, transformational topics that will alter business over the next decade and beyond. Written for the C-suite and boardroom executives worldwide, *VISION by Protiviti* examines the impacts of disruptive forces shaping the world today and in the future. Through a variety of voices and a diversity of thought, *VISION by Protiviti* provides perspectives on what business will look like in a decade and beyond.

© 2024 Protiviti Inc. An Equal Opportunity Employer M/F/Disability/Veterans.
Protiviti is not licensed or registered as a public accounting firm and does not issue opinions on financial statements or offer attestation services.

protiviti®