Carnegie Mellon University
Software Engineering Institute

Cybersecurity Maturity Model Certification (CMMC)

THREATS TO NATIONAL SECURITY can come from any link in the Department of Defense supply chain. The risks to the Defense Industrial Base (DIB)—the network of the estimated 220,000, businesses and organizations that research, engineer, develop, acquire, deliver, sustain, and operate military systems—are especially alarming because of threats from cybercriminals and state-sponsored actors. To bolster the cybersecurity posture within the DIB supply chain, DoD turned to the CMU Software Engineering Institute to co-develop the Cybersecurity Maturity Model Certification (CMMC) with the Johns Hopkins University Applied Physics Lab.

A cyber attack within the DIB supply chain could result in devastating loss of intellectual property (IP) and controlled unclassified information (CUI), which increases risks to the warfighter. With its extensive history in modeling for cybersecurity risk and resilience and its deep research into supply-chain attacks, the SEI is ideally positioned to address the key objectives of the CMMC program:

- safeguarding sensitive information to enable and protect the warfighter
- enforcing DIB cybersecurity standards to meet evolving threats from adversaries, including state-sponsored actors intent on stealing IP and thwarting capability advancement
- ensuring compliance and accountability with DoD cybersecurity requirements

Since the inception of CMMC in 2019, the SEI has touched virtually every aspect of the program. The SEI helped to establish its structure based on proven cybersecurity practices, developed the certification and assessment standards, and created training for an estimated 160,000 contracting officers, program managers, and others in the defense acquisition workforce. The SEI engaged directly in numerous meetings and workshops with stakeholders throughout the DIB to develop a model that scaled appropriately to meet DoD needs while still being achievable by DIB contractors.

The DoD engaged with the SEI as co-developer of the CMMC because of the SEI's unique history of contributions to the DoD. The SEI

- is ideally positioned at the confluence of government, industry, and academia to have unique insights into the commercial defense ecosystem, government acquisition and compliance requirements, and technology research
- has the most extensive history in capability maturity modeling, beginning with the Capability Maturity Model (CMM), and continuing through the CERT Resilience Management Model (CERT-RMM) and CMMC and related supply chain risk assessment methodologies
- has supported extensive research in modernizing government software acquisition, Agile methods, DevSecOps, and other modern software development methods
- through its CERT Division is a national resource for research on cybersecurity, including vulnerabilities, secure coding, cyber risk and resilience, insider threat, cybersecurity monitoring and response, cyber workforce development, and AI incident response

Implementation of the CMMC Program will transform the DIB by better protecting sensitive DoD information from adversaries. It creates a baseline for DIB contractors to implement cybersecurity requirements according to a clear set of measures applicable across the federal space.

About the SEI

The Software Engineering Institute (SEI) advances software as a strategic advantage for national security. We serve the nation as a federally funded research and development center (FFRDC) sponsored by the U.S. Department of Defense (DoD).

Contact Us

sei.cmu.edu
412.268.5800 | 888.201.4479
info@sei.cmu.edu