CyberSagacity

COMPLIANCE BRIEF

Application Security Testing for CMMC 2.0 compliance.

CMMC 2.0 is the DoD's unified cybersecurity standard for the Defense Industrial Base. Many of its NIST SP 800-171 controls quietly require application-level security testing — and that's where most programs fall short.

PUBLISHED
2025

AUDIENCE
DIB Contractors · C3PAOs · Compliance

FORMAT
Compliance Brief

CYBERSAGACITY.COM

WHAT IS CMMC 2.0?

The DoD's unified standard for protecting FCI and CUI.

Cybersecurity Maturity Model Certification 2.0 applies to all contractors and subcontractors handling Federal Contract Information (FCI) or Controlled Unclassified Information (CUI). It has three levels.

LEVEL 1

Foundational

For FCI

15 basic cyber-hygiene practices. Verified by annual self-assessment.

LEVEL 2

Advanced

For CUI

110 practices from NIST SP 800-171. Triennial third-party assessment by a C3PAO.

LEVEL 3

Expert

Highly sensitive CUI

Built on NIST SP 800-172. Triennial government-led assessment.

Non-compliance risks contract loss, reputational harm, and costly remediation.

ORGANIZATIONS REQUIRED TO MEET CMMC 2.0

CMMC reaches across the entire DoD supply chain.

Any entity handling FCI or CUI is in scope — a broad and growing market:

- **Software developers** — mission planning, weapons, logistics, custom defense apps.
- **Hardware manufacturers** — electronics, sensors, avionics, military parts.
- **Cybersecurity providers** — monitoring, IR, and compliance services.
- **IT service providers & integrators** — secure DoD IT infrastructure.
- **Cloud & managed service providers** — storing or processing FCI/CUI.
- **Engineering & R&D firms** — defense research and prototyping with CUI.
- **Logistics, maintenance & construction** — DoD operations with CUI access.
- **Academic & research institutions** — federally funded defense research.

TIMELINE

The final rule (32 CFR Part 170) took effect **December 16, 2024**. Requirements began appearing in contracts in 2025, with full implementation expected by **2028**.

When mandated, failure to meet CMMC disqualifies an organization from DoD contracts.

APPLICATION SECURITY TESTING REQUIREMENTS IN CMMC

Four control families quietly demand AppSec testing.

SYSTEM & INFORMATION INTEGRITY

SI

SI.1.210 SI.2.216 SI.3.219 SI.3.220

Identify and correct flaws; track CVEs and patch frameworks; use SAST/DAST to verify secure code; protect against malicious code and vulnerable dependencies (SCA).

CONFIGURATION MANAGEMENT

CM

CM.2.063 CM.2.064

Provide only essential capabilities; review apps for unnecessary, risky features; apply and document secure configuration of app platforms, web servers, and APIs.

ACCESS CONTROL

AC

AC.2.009 AC.2.016

Limit unsuccessful logons; control the flow of CUI per authorizations — implemented as secure authentication and access controls inside applications.

RISK ASSESSMENT

RA

RA.3.144 RA.3.145

Conduct vulnerability scans of web apps and APIs and remediate findings; analyze security trends — using application security testing data to drive decisions.

CMMC mandates no specific tools — but 800-171 repeatedly requires application-level security measures.

RECOMMENDED APPLICATION SECURITY TESTING PRACTICES

To align with Level 2 or higher, test the application layer.

Testing method	Purpose	Supports controls
SAST	Detects vulnerabilities in source code during development.	SI.1.210 · SI.3.219
DAST	Tests running applications for runtime flaws.	SI.1.210 · RA.3.144
SCA	Identifies vulnerable open-source dependencies.	SI.1.210 · SI.3.220
Penetration testing	Simulates attacks to find deeper issues.	RA.3.144 · AC.2.016
Secure code reviews	Manual or automated reviews of source code.	SI.1.210 · SI.3.219

Best practice for Level 2+: code & dependency scanning (SAST, DAST, SCA, CSPM, API, PenTest), vulnerability scanning of web apps, and secure SDLC processes.

THE OPPORTUNITY & HOW CYBERSAGACITY HELPS

A mandatory market — and a precision compliance partner.

$4B
DoD-estimated contractor investment in CMMC implementation over **20 years**.

2028
Full implementation — compliance becomes **mandatory** for DoD contracts.

110
NIST SP 800-171 practices at Level 2 — many requiring **application security testing**.

Costs range from a few thousand dollars for Level 1 self-assessments to millions for Level 3 — driving urgent demand for effective assessment and remediation tooling.

CyberSagacity streamlines compliance where programs struggle most — **application security testing** — validating, prioritizing, and quantifying defects against NIST SP 800-171 controls, with the evidence and auditability assessors expect.

THE BOTTOM LINE

Turn application security testing from a compliance gap into defensible, audit-ready evidence.