

Cybersecurity is not paperwork.

CMMC should strengthen the DIB’s ability to protect defense information, recover from attack, and keep delivering for the mission.

VISION BRIEF / AUGUST 2026

THE THESIS

Secure the industrial base as a system. The DIB is a living network of manufacturers, engineers, managed providers, cloud services, primes, assessors, and Government programs. Attackers use the seams between them. CMMC must make those handoffs stronger without letting responsibility disappear across them.

FIVE PRINCIPLES

01 Automation over documentation Collect security facts where the work happens. Stop making every supplier and reviewer rewrite them.	02 Continuous over point-in-time Recheck affected claims when accounts, systems, providers, or boundaries change.
03 Assessment-ready over dashboard-green Prepare evidence another person can trace, test, challenge, and disagree with.	04 Accessible over enterprise-only Make strong cybersecurity achievable for the small suppliers the mission depends on.
05 Ecosystem-wide over contractor-only Give every party a clear part without letting anyone pass responsibility downstream.	

PUT SCARCE EFFORT WHERE IT IMPROVES SECURITY.

Protect Fund and operate MFA, backups, logging, patching, recovery, and the people who make them work.	Know Keep a current record of what is protected, who owns it, what supports the claim, and what changed.	Challenge Use qualified people to test the implementation, resolve conflicts, and reach accountable findings.
--	--	---

HOW THE WORK RUNS	Scope → Protect → Record → Check → Decide → Update Software can collect facts and run repeatable checks. Qualified people handle context, conflicts, findings, and consequential decisions.
--------------------------	---

ONE SYSTEM, DISTINCT RESPONSIBILITIES

Providers Prove what the shared service performs and what remains with the customer.	Contractors Own scope, safeguards, gaps, evidence, and the organizational affirmation.	Assessors Examine the implementation and record independent findings.	Government Sets the rules, tests new methods, and retains its decision authority.
--	--	---	---

POLICY CHOICES CHANGE THE RESULT

Reopen unchanged 97% current assurance · 36% suppliers lost · 33k peak backlog	Add assessment capacity 97% current assurance · 18% lost · 27k peak backlog	Graduated verification 90% current assurance · 3% lost · 12k peak backlog	Coordinated reform 91% current assurance · 1% lost · 7.4k peak backlog
--	---	---	--

Median modeled outcomes through 2049, not forecasts. Assumptions and sensitivity cases are published at cmmc20x.com/analysis/methodology.

THE IDEA CAN BE TESTED NOW

CMMC 20X compares seven CMMC policy options with public assumptions and limitations. Deep Fathom has also represented all T10 Level 2 requirements and 320 assessment objectives in software, enough to test whether better records reduce repeated work without transferring findings or official decisions to software.

READ AND TEST THE WORK

- [Read the declaration](#)
- [Read the five principles](#)
- [Read the Blueprint](#)
- [See the complete ecosystem](#)
- [Compare the seven CMMC policy options](#)

Source and status: Deep Fathom publication, reviewed August 13, 2026. Working-implementation detail: cmmc20x.com/product. Analysis method and limitations: cmmc20x.com/analysis/methodology. Contact: cmmc20x@deepfathom.ai.