cyberstar

DFARS PART 239 CLASS DEVIATION & DODM 8140.03

What the DoW CIO Memo Will Change

BOTTOM LINE UP FRONT

The Department of War CIO is expected to issue a DFARS Part 239 class deviation requiring contractors to **comply with DoDM 8140.03.**

This makes cyber workforce qualification a contractual requirement across the Defense Industrial Base.

Most organizations are focused on CMMC. This introduces a parallel requirement: your people must be trained, certified, and aligned to defined DCWF work roles — and you must be able to provide evidence that they meet 8140.03 qualification requirements.

CMMC secures your systems.

DoDM 8140.03 qualifies your people.

The dual compliance requirement

	CMMC	DoDM 8140.03
Requirement Focus	System & Network Security	Personnel Qualification
Outcome	Protects CUI/FCI Data	Ensure Workforce Readiness
Assessment Type	Third-Party Assessment (C3PAO)	Role-Based Qualification (Foundational, Residential)
Applicability	DIB Organizations with CUI	All DoW & DIB Cyber Personnel

Dual compliance

CMMC does not satisfy DoDM 8140.03.

Both are required.

Contract Risk

Unqualified personnel may impact contract eligibility and performance ratings.

Auditable Reporting

Real-time workforce readiness must be maintained and demonstrable.

HOW CYBERSTAR ADDRESSES DODM 8140.03

Purpose-built for 8140 readiness.

Already operational in DoW environments today.

Cyberstar is a COTS cyber talent management system that verifies personnel meet DCWF role requirements and provides auditable proof of 8140 readiness across the enterprise.
Available through Carahsoft.

How it works

Work role mapping

Automatically aligns personnel to DCWF work roles – replacing manual tracking and disconnected record systems.

Certification validation

Continuously verifies workforce against role requirements and identifies qualification gaps before they become audit findings.

Defensible 8140 reporting

A single authoritative source for real-time, audit-ready reporting with clear, defensible evidence for DoW review.

FedRAMP authorized

Available at IL2 and IL5, with P-ATO in process — meeting the security bar required for defense environments.

Recommended actions for CIOs and CISOs

1. Map cyber personnel to DCWF work roles
2. Conduct a gap analysis of current certifications and qualifications
3. Establish auditable tracking and reporting processes
4. Integrate DoDM 8140.03 as a distinct compliance track, independent of CMMC
5. Brief senior leadership on the dual compliance requirement

Understand your 8140 readiness before you have to prove it.

Schedule a brief conversation to understand how DoDM 8140.03 affects your contracts and what a compliant path forward looks like.

Explore Cyberstar

Learn more at carahsoft.com/cyberstar