MINERVA CYBER TECHNOLOGIES

FORT MEADE ALLIANCE
An Independent Community Organization

Captiva Solutions

CMMC: What to Do Now

30 July 2026

Kim Irving • Eberechi Ugwu-Amole

SMARTERCYBER℠

Eberechi (Ebbie) Ugwu-Amole

President & CEO, Captiva Solutions | CMMC LCCA| CCI | CCA | CCP | CISSP | CISA | CISM | CGEIT | CRISC | CDPSE | CoBIT | PMP

- 25+ years of cybersecurity and GRC leadership supporting organizations across CMMC, FedRAMP, FISMA, NERC CIP, and enterprise risk programs.
- CMMC ecosystem leader since the framework's inception with hands-on experience spanning readiness, assessor training, official content development, and assessment operations.
- Lead CMMC Certified Assessor and Certified Instructor with deep experience translating CMMC requirements into practical implementation guidance.
- Creator of Captiva's Real-Skills-for-Real-Jobs® methodology focused on bridging theory, compliance expectations, and job-ready execution.
- Builder of cybersecurity talent pipelines for over 20+ years through professional training, workforce development, mentoring, and certification pathways across the DIB.

Practical CMMC readiness, assessor perspective, training excellence, and implementation lessons for the Defense Industrial Base.

CMMC ecosystem leadership rooted in assessment, training, and governance leadership.

President & CEO, Captiva Solutions

MINERVA
CYBER TECHNOLOGIES

Captiva Solutions

Captiva Solutions: CMMC, Cybersecurity & Training Services

A cybersecurity consulting and training firm helping organizations translate compliance obligations into defensible, operational security practices.

CMMC Ecosystem Roles – Full Spectrum Support

APP Develop official CMMC training content

ATP Train CMMC professionals and assessors

Former RPO Support readiness and gap closure

Candidate C3PAO Support assessment capability and discipline

Training & Consulting Strengths – Decades of Impact Across IT, Cybersecurity, Training & Consulting

IT & Cybersecurity Excellence

Hands-on practice across CMMC, FedRAMP, FISMA, and NERC CIP — helping hundreds of professionals and organizations achieve measurable cybersecurity compliance.

Cybersecurity Training Leadership

20 years of structured training delivery through the proprietary Real-Skills-for-Real-Jobs® (RS4RJ®) methodology that turns frameworks into actionable, on-the-job skills.

Consulting & Advisory Authority

End-to-end GRC advisory — readiness gap assessments, remediation, and C3PAO-candidate assessment support across the Defense Industrial Base.

Active roles within the CMMC Ecosystem give Captiva a uniquely full-spectrum voice on the CMMC framework.
We are positioned to help organizations move from CMMC uncertainty to clear, practical execution.

Kim Irving

Co-Founder & CEO, Minerva Cyber Technologies | CMMC Registered Practitioner (CMMC-RP) | Mission Critical Fellow | AUSCF Board Member | FMA Micro Business Cohort Alumni

- Senior cyber executive and growth leader with more than 25 years of experience delivering advanced technology solutions to federal agencies, including 17 years directly supporting the warfighter and national security mission.
- Leads Minerva's full-lifecycle CMMC practice, including strategy, scoping, gap assessment, remediation planning, evidence development, and assessment preparation for Level 1 and Level 2 environments.
- Known for translating complex CMMC and NIST 800-171 requirements into practical, sustainable execution for both business and technical stakeholders.
- Brings deep experience in cybersecurity, DevSecOps, AI/ML, cloud, modernization, and federal growth strategy, with a track record of building resilient, mission-critical environments and driving measurable business results.

MINERVA
CYBER TECHNOLOGIES

Captiva Solutions

About Minerva

- Minerva Cyber Technologies is a Woman-Owned Small Business (WOSB) providing cybersecurity services and solutions for government customers and regulated organizations.
- We support federal agencies, defense contractors, and other mission-critical organizations with services spanning cybersecurity compliance, cyber operations, resilience strategy, operational technology security, and advisory support for frameworks including CMMC, NIST-based compliance, FISMA, and related requirements.
- Our approach is practical: scope it correctly, prioritize what moves the needle, and build an evidence trail that holds up under assessment. See our list of complete offerings at https://minervacybertech.com

CAMI CYBER AWARDS 2023
Best of Anne Arundel County
CYBERSECURITY ASSOCIATION OF MARYLAND, INC.

9TH ANNUAL
CYBERSECURITY AWARDS FINALIST
Cybersecurity Association

Technical.ly
RealLIST STARTUPS
Minerva Cyber Technologies
2026 MARYLAND HONOREE
Recognized as one of the region's most promising early-stage companies

carahsoft
Microsoft
WIZ
NVIDIA
DRAGOS
FORESCOUT
SKOPENOW
SAS
CDW

What you will learn today

We will focus on four main topics:

1. What Changed
   - Separate the Phase 2 headlines from the obligations that still remain in force.
2. Level 1 Credibility
   - Define scope, safeguards, and the minimum evidence needed for self-attestation.
3. Next 30 Days
   - Reduce compliance friction and cyber risk with practical near-term actions.
4. Protect Your Prior Investment
   - Translate prior Level 2 and 800-171 work into current value and future readiness.

This session intentionally does not…

- Interpret specific contracts or provide legal advice.
- Debate products or tools by brand.
- Assume every company needs enterprise-wide scope.

Poll #1: Who is in the room?

Which best describes your role?

- Executive / Owner
- Contracts / Procurement
- IT
- Security
- Compliance / Quality
- Operations / Program Mgmt

What you need to know about current events.

60-day Review

Industry comments are being solicited during the review period, with responses due by August 14.

Assessments Continue

The news file reports that certifications, eMASS uploads, and many assessments are still proceeding.

Primes Still Care

Prime contractors are still flowing requirements and asking subcontractors for proof of cyber maturity.

Self-Attestation Risk

Unsupported affirmations can increase False Claims Act and whistleblower exposure.

Small Business Burden

Officials cited compliance overhead and ecosystem capacity as reasons for slowing the rollout.

Business as Usual

The most consistent message in the materials is simple: keep improving, keep documenting, and do not rip up the roadmap.

What actually changed.

Headline

On July 13, 2026, the Department of War announced a suspension of CMMC Phase 2, along with Phase 3 and Phase 4, and launched a 60-day review of the full program.

What did not change

Phase 1 remains active, self-assessments remain relevant, and contractors still have to safeguard federal information and continue required NIST SP 800-171 work where applicable.

HOT TOPIC

False Claims Act

Raytheon/Nightwing — $8.4M (May 2025)

- DOJ alleged Raytheon failed to implement required cybersecurity controls on an internal development system used for unclassified DoD contract work.
- Settlement resolved allegations that claims were submitted while cybersecurity requirements in DoD contracts or subcontracts were not met.
- Whistleblower share: $1.512M; case cited as U.S. ex rel. Doe v. Raytheon Co. et al., No. 21-cv-2343 (D.D.C.).
- **CMMC takeaway:** internal systems supporting contract performance matter; evidence must match actual implementation.

MORSECORP — $4.6M (March 2025)

- DOJ alleged MORSE billed on Army and Air Force contracts while knowing it had not fully implemented required NIST SP 800-171 controls.
- Allegations included use of a third-party email host without required protections and failure to maintain a consolidated written system security plan.
- Whistleblower share: $851,000; case cited as U.S. ex rel. Berich v. MORSECORP Inc. et al., No. 23-cv-10130 (D. Mass.).
- **CMMC takeaway:** gaps in SSPs, external service arrangements, and inherited controls can become FCA issues when certifications overstate readiness.

L1 BASICS

Credible Level 1 self-assessment.

What Credibility Requires

- Clear boundary definition for the systems and users that handle federal contract information.
- Basic safeguards actually configured and operating.
- Minimum evidence collected before anyone signs an attestation.
- A management narrative that matches operational reality.

What Credibility Does Not Mean

- Buying every tool marketed as a CMMC shortcut.
- Writing enterprise-scale policy binders no one follows.
- Treating Level 1 like a paperwork-only exercise.
- Assuming a future rule change will fix weak operations.

HIGH VALUE PRIORITIES

What really falls in scope.

Contracts

Identify the awards, subcontracts, and task orders that actually drive the obligation.

People

Map the workforce, admins, and partners that touch in-scope information or systems.

Systems

List devices, shared drives, cloud apps, email, backups, and management tools tied to delivery.

Data Flow

Follow how information is created, stored, transmitted, and archived from intake through closeout.

Access Paths

Include remote access, admin privileges, and third-party connections that can affect the boundary.

Assumptions

Write down what is included, excluded, inherited, and still unresolved so scope can be defended later.

WHY THIS MATTERS

Level 1 is simple, but not casual.

Protect FCI

Level 1 is about protecting Federal Contract Information on systems that store, process, or transmit it.

All 15 must be MET

A Final Level 1 (Self) result requires a MET result for every requirement; no POA&Ms are allowed.

Every Year

The organization must complete the self-assessment annually, submit the results in SPRS, and provide annual affirmation.

SCOPE

Scope in plain English.

In scope

- Systems that process, store, or transmit FCI
- People using those systems to perform contract work
- Devices, shared services, and locations that can expose that FCI

Usually out of scope

- Public information and simple payment/transaction data
- Standalone systems with no FCI connection
- People and equipment that never touch FCI workflows

Plain-English test: if the asset, user, app, share, email box, endpoint, or room could expose nonpublic contract information, treat it as part of your Level 1 story.

FCI

What counts as Federal Contract Information?

Think everyday contract work

Statements of work, technical directions, deliverables in progress, tasking emails, engineering files, staffing plans, and internal work products generated for the Government can all be FCI.

Think not public

If it is provided by or generated for the Government under contract and is not intended for public release, it fits the FCI definition unless it is public information or simple transactional information.

Practical rule: if you would hesitate to post it publicly because it reveals contract performance details, assume it is FCI until proven otherwise.

5 BUCKETS

The 15 requirements in five buckets.

Access

Who can get in and what they can do

Identity

Know the user, device, or process is real

Media & physical

Protect devices, spaces, and disposed media

Boundary defense

Control connections, segmentation, and traffic

Hygiene

Fix flaws and stop malicious code

These buckets are a teaching device, not a regulatory rewrite. They map the FAR 52.204-21 controls into operational themes people can assess and maintain.

MINERVA
CYBER TECHNOLOGIES

Captiva Solutions

BUCKET MAP

How the buckets line up to the FAR controls

Bucket	Controls	Theme	Operator Cue
Access	1, 2, 4	Use limits	Only the right people, doing the right things, in the right places
Identity	5, 6	Identification + authentication	No anonymous access to FCI systems
Media & physical	7, 8, 9	Protect devices and places	Clean disposal, controlled rooms, logged visitors
Boundary defense	3, 10, 11	Connection and segmentation	Control external systems and network edges
Hygiene	12, 13, 14, 15	Fix and scan	Patching, AV, updates, and scans are routine

MINERVA
CYBER TECHNOLOGIES

Captiva Solutions

BUCKET 1-2

Access and identity requirements.

1

Authorized access only

Limit system access to authorized users, authorized processes, and authorized devices.

2

Allowed functions only

Limit users to the transactions and functions they are permitted to execute.

4

Public posting control

Control information posted or processed on publicly accessible systems.

5

Identify users/devices/processes

Know who or what is requesting access to the system.

6

Authenticate before access

Verify identities as a prerequisite to system access.

MET idea

Accounts, roles, MFA or strong sign-in, disabled shared access to FCI, and public-site review controls should all tell the same story.

BUCKET 3-4

Media, physical, and boundary defense.

7

Sanitize or destroy media

Dispose of or reuse media containing FCI only after proper sanitization or destruction.

8

Limit physical access

Restrict access to systems, equipment, and operating environments to authorized individuals.

9

Escort and log visitors

Escort visitors, monitor activity, maintain physical access logs, and manage access devices.

3

Control external connections

Verify and limit connections to and use of external systems.

10-11

Protect boundaries and separate public systems

Monitor communications at boundaries and separate public-facing components from internal networks.

MET idea

Network diagrams, firewall rules, visitor logs, badge procedures, and media disposal records should connect to actual FCI handling.

BUCKET 5

System hygiene requirements.

12

Fix flaws quickly

Identify, report, and correct information and system flaws in a timely manner.

13

Protect from malicious code

Provide anti-malware protection at appropriate locations in organizational systems.

14

Keep protection current

Update malicious code protection mechanisms when new releases are available.

15

Scan periodically and on download

Perform periodic scans and real-time scans of files from external sources.

Operational pattern

Patch cadence, vulnerability or defect tickets, EDR status, AV update evidence, and scan settings should be current and recurring.

MET idea

Policies say “timely,” but evidence shows no cadence, no owner, and no proof the fixes reached the actual in-scope devices.

CREDIBLE MET

What makes “MET” credible?

Documented

Policy, procedure, diagrams, inventories, and role assignments describe the control as implemented today.

Observable

Screenshots, configurations, admin settings, logs, and physical walkthroughs show the control operating on in-scope assets.

Repeatable

Recurring tickets, review records, training, approvals, and timestamps prove the practice is sustained, not staged for assessment day.

Fast test: if one screenshot is the only proof, it is usually weak; if the story shows who, what, where, and when, MET is much more believable.

EVIDENCE EXAMPLES

Evidence that stands up under scrutiny.

Access & identity

User list with roles, joiner/mover/leaver workflow, MFA settings, sample access approval, disabled stale accounts, and a walkthrough of least-privilege permissions.

Media & physical

Asset inventory, device disposal record, shredding or destruction receipts, office access rules, visitor log, and badge or key issuance process.

Boundary defense

Network diagram, firewall or secure gateway settings, segmentation for public services, remote access rules, and approved external system list.

System hygiene

Patch reports, vulnerability remediation tickets, EDR/AV health dashboards, signature update status, and scan policies for downloaded files.

ANNUAL CYCLE

Annual self-assessment workflow.

1

Confirm scope

Identify the systems, people, and locations touching FCI.

2

Test all 15

Score each requirement MET or not MET based on current evidence.

3

Fix before filing

Because no POA&Ms are allowed at Level 1, close gaps before claiming compliance.

4

Package evidence

Retain the evidence set that supports the annual result and affirmation.

Mindset: assess like someone else will review your logic later, even though Level 1 is a self-assessment.

Poll #2: What is your biggest blocker to CMMC?

- Scope clarity
- Evidence collection
- MFA/access control
- MSP responsibility
- Asset inventory
- Leadership time/budget

MINERVA
CYBER TECHNOLOGIES

Captiva Solutions

30 DAYS

Next 30 days for Phase 1 posture.

Weeks 1-2

- Confirm contract drivers and scope assumptions.
- Inventory systems, users, and admin paths.
- Validate basic safeguards already in place.
- Stand up one evidence repository with naming discipline.

Weeks 3-4

- Close the most visible evidence and operating gaps.
- Draft a concise self-assessment narrative for leadership.
- Document residual risks and funded next steps.
- Prepare talking points for primes, customers, and auditors.

ROI

Keep Level 2 work from going to waste.

Policies

Reuse as governance baseline and trim to current scope.

Tooling

Retain for security value even if the certification timeline slips.

Consulting Work

Convert prior gap analysis and roadmaps into today's operating plan.

Platform Work

Keep SSP, POA&M, and evidence structures active to avoid sunk-cost thinking.

Prior Level 2 work is not wasted if it still improves protection, reduces rework, and shortens the path back to higher assurance when the program settles.

CMMC STORY

The CMMC story you should be able to tell.

Core Message

We understand our current scope, have completed a credible Level 1 self-assessment approach, and are continuing practical cybersecurity improvements that preserve future readiness.

Proof Points

- Defined boundary and ownership.
- Visible evidence set and repository.
- Documented roadmap for next 30, 60, and 90 days.
- Prior Level 2 work mapped to current business value.

Questions and next steps.

Do the work that still matters:

1. Protect Data
2. Support Self-Attestation
3. Preserve Future Readiness

Questions?