



The Cyber G.A.R.D.™ Framework

A practitioner's guide to assessment readiness under NIST SP 800-171 and CMMC, for Defense Industrial Base contractors and the broader federal contractor market.

DEFENSE INDUSTRIAL BASE

DFARS 252.204-7012 / 7019 / 7020 / 7021 ·
SPRS · CMMC Level 1 and Level 2

BROADER FEDERAL MARKET

FAR 52.204-21 · CUI · NIST SP 800-171 · prime
flow-downs · agency-specific clauses

Eddie White

CMMC Registered Practitioner · CCP (pending adjudication)
Lean Six Sigma Master Black Belt · ISO 9001 Lead Auditor
20-year U.S. Air Force veteran

September 2026

Globe-America Consulting, Inc. · SDVOSB
Fort Worth, Texas · globe-america.com

Abstract

A CMMC Level 2 assessment subjects a contractor to a structured evaluation across three methods, Examine, Interview, and Test, applied to the 110 NIST SP 800-171 requirements. The same three methods, drawn from NIST SP 800-171A, are what a civilian agency reviewer, a prime's due-diligence team, or a Department of War DIBCAC assessor applies when they look past the paperwork. The dominant vendor response to this challenge has been the compliance platform: software that automates gap analysis, generates documentation templates, and produces compliance reports. These tools provide real operational value. On their own, they leave the gap that matters most: the organizational capability to defend implementation claims under direct scrutiny.

This paper introduces the Cyber G.A.R.D.™ Framework, Globe-America Consulting's proprietary four-phase framework. Govern the Boundary, Align Evidence, Reinforce Implementation, Defend the Assessment: the phases follow the same logical sequence assessors follow in the CMMC Assessment Guide. The framework complements compliance platforms rather than replacing them, by building the organizational readiness that documentation alone cannot produce. This paper describes each phase, explains how a practitioner-led framework and platform investments work together, situates the framework in the CMMC landscape as it stands in September 2026, and extends it to contractors whose requirements arrive from a civilian agency or a prime rather than from a Department of War contract.

Introduction

There is a gap between compliance documentation and assessment readiness, and it is wider than most contractors realize. An organization can have a complete System Security Plan, a documented SPRS score, a library of policies, and a populated POA&M, and still face conditional findings that delay awards and require significant remediation.

The reason is structural. Assessors evaluate not just the existence of documentation but the verifiable accuracy of every implementation claim against the actual state of the organization's systems. They examine artifacts. They interview personnel. They test configurations. A compliance platform that generates documentation cannot make an IT administrator answer an assessor's question correctly. A framework, applied by a practitioner, can.

Cyber G.A.R.D.™ was designed to close that gap. It is a practitioner-developed framework built around the specific demands of the assessment process, sequenced to address the logical dependencies that determine whether an organization's compliance posture survives contact with an assessor or buckles under it.

§ 1 Where the Program Stands: September 2026

Any readiness paper written in 2026 has to say what the rules currently are, because they changed twice in ten months. The framework in this paper is designed to be stable across those changes; the obligations it is applied to are not.

Date	What happened	What it means for a contractor
November 10, 2025	CMMC Phase 1 took effect under 32 CFR Part 170 and DFARS 252.204-7021. Level 1 and Level 2 self-assessment requirements began appearing in Department of War solicitations.	If the clause is in the solicitation, the self-assessment and the SPRS affirmation are conditions of award today.
July 13, 2026	The Department of War suspended CMMC Phase 2 and stood up a Reform Task Force to review the program. The phased introduction of certification assessments paused.	The date an external assessor arrives moved. What has to be implemented did not: 32 CFR Part 170 is unchanged, Phase 1 remains in force, and primes have not withdrawn flow-downs.
Ongoing	DIBCAC Government Assessments continue under DFARS 252.204-7020, and the Department of Justice continues to pursue False Claims Act cases involving inaccurate cybersecurity attestations.	The Affirming Official's annual SPRS affirmation carries the same legal weight it did before the pause.
Civilian agencies	Outside the Department of War, FAR 52.204-21 sits in nearly every federal contract, CUI is governed by 32 CFR Part 2002, and agencies invoke NIST SP 800-171 for CUI directly or through prime flow-down. A government-wide FAR CUI rule has been proposed.	There is no SPRS score to post, but the same 110 requirements, the same boundary decisions, and the same evidence questions apply when a reviewer or a prime asks.

Table 1: The compliance landscape as of September 2026. Verify the Phase 2 status and the FAR CUI rule against current Department of War and FAR Council notices before relying on this table.

The practical reading

A pause in certification scheduling is not a pause in obligation. Contractors who use the Phase 2 suspension to defer implementation will arrive at the next scheduling milestone, whatever form it takes, with the same gaps and less time. Contractors who use it to close the gap between documentation and reality will arrive with nothing to remediate.

§ 2 Platforms and Frameworks: Where Each Earns Its Keep

The federal compliance market has grown significantly in response to CMMC enforcement and to primes flowing NIST SP 800-171 down their supply chains. The dominant commercial response has been platform development: software that automates compliance workflows, generates documentation from templates, and provides dashboards for tracking control status across all 110 requirements. These platforms serve a real purpose. They reduce the labor of documentation, provide structure for compliance programs, and give organizations visibility across their control landscape.

What a platform alone cannot do is make an organization assessment-ready. The distinction matters because an assessment is fundamentally an organizational evaluation, not a documentation review. Assessors evaluate three things: whether documentation accurately describes reality (Examine), whether personnel understand and execute the documented controls (Interview), and whether systems behave as documented (Test). Platforms address the first dimension partially, and the second and third only insofar as the data fed into them is accurate and current.

This is not an argument against platforms. The most successful programs use both: a platform to manage documentation, evidence inventory, and control tracking, and a practitioner-led framework to produce the organizational behavior the platform assumes is already in place. The Cyber G.A.R.D.™ Framework is that layer. It builds the readiness that platforms can then maintain.

How a platform and the framework divide the work

Readiness dimension	What a platform contributes	What Cyber G.A.R.D.™ contributes
Documentation generation and control tracking	Primary contributor. Templates, workflow automation, dashboards.	Reviews documentation for accuracy against the actual environment.
Evidence accessibility during assessment	Stores evidence references and links to artifacts.	Verifies every artifact can be retrieved on assessor request.
Personnel knowledge and interview readiness	Limited. Some platforms offer training modules.	Primary contributor. Pre-assessment interviews and walkthroughs.
Configuration accuracy under the Test method	Records claimed configurations. Cannot verify they match reality.	Primary contributor. Pre-assessment technical verification.
Boundary accuracy (CUI and FCI)	Scopes to inputs provided. Mirrors under-specification.	Primary contributor. Boundary definition and ESP mapping.
Currency across the lifecycle	Tracks artifact dates and review schedules.	Annual review cycles tied to affirmation and re-attestation obligations.

Table 2: Division of labor between a compliance platform and the Cyber G.A.R.D.™ Framework across the six readiness dimensions that determine assessment outcomes.

The four dimensions a platform alone misses

- **Personnel knowledge gaps.** Documentation describes a control. The assessor asks the IT administrator to demonstrate it. The administrator describes a different process than what is documented. The Interview finding contradicts the Examine narrative regardless of how complete the platform-generated SSP appears.
- **Configuration drift.** A platform records that MFA is implemented. The assessor tests it. A service account bypasses MFA enforcement. The Test finding contradicts the documented control and raises questions about every other implementation claim.
- **Evidence accessibility.** A platform references artifacts. The assessor requests them. They cannot be produced in current form. Evidence that exists in a platform record but cannot be retrieved during the assessment is treated as non-existent.
- **Boundary accuracy.** A platform scopes the assessment based on inputs provided during setup. If those inputs under-specified the CUI environment, the platform produces documentation that does not reflect the organization's actual scope.

The framework addresses all four. It teaches an organization how to govern its boundary accurately, align evidence to every claim, reinforce implementations through verification, and prepare personnel and documentation to defend under scrutiny.

§ 3 Cyber G.A.R.D.™ Framework Overview

The Cyber G.A.R.D.™ Framework is a four-phase compliance framework developed by Globe-America Consulting, Inc. Each phase addresses a distinct dimension of assessment readiness, and each phase is a logical prerequisite for the next.

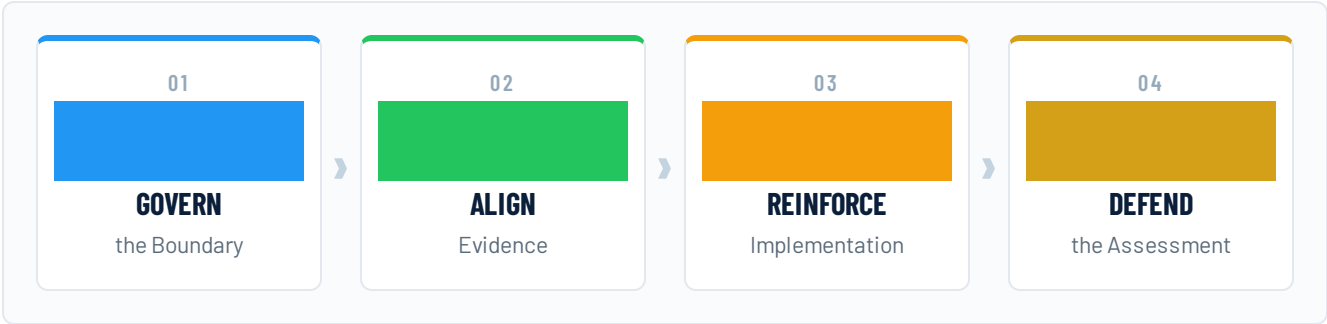


Figure 1: Cyber G.A.R.D.™ phase sequence. Each phase produces outputs that are prerequisites for the next.

Framework design principles

Principle	Description	Assessment impact
Sequential dependency	Each phase depends on outputs from the prior phase. Evidence cannot be aligned before the boundary is governed. Implementation cannot be reinforced before evidence is mapped.	Eliminates wasted effort on documentation that must be revised when boundary or scoping changes occur late.
Assessment-method alignment	Each phase maps directly to one or more of the three NIST SP 800-171A methods: Examine, Interview, and Test.	Every phase output serves a specific assessment function. No compliance activity is performed without a direct assessment benefit.
Lifecycle design	Structured for continuous application across the three-year assessment cycle and the annual affirmation, not as a one-time preparation exercise.	Maintains posture without full re-execution at each cycle.
Small-contractor scale	Designed for organizations with 5 to 200 employees operating without a dedicated compliance team, in either market.	Phase outputs are proportionate to the organization's size and the complexity of its protected-information environment.
Requirement-source neutral	The phases key to the assessment methods, not to the clause that imposed the requirement. A DFARS flow-down, an agency CUI supplement, and a prime's questionnaire all route through the same four phases.	One program satisfies a Department of War prime and a civilian agency without being rebuilt for each.

G Phase G · Govern the Boundary

The first and most consequential phase is Govern the Boundary. Every subsequent phase depends on the accuracy of the work performed here. The boundary governs the scope of the SSP, the applicability of each control, the extent of the evidence required, and ultimately the scope of the assessment itself. An inaccurate boundary at Phase G produces compounding errors in Phases A, R, and D.

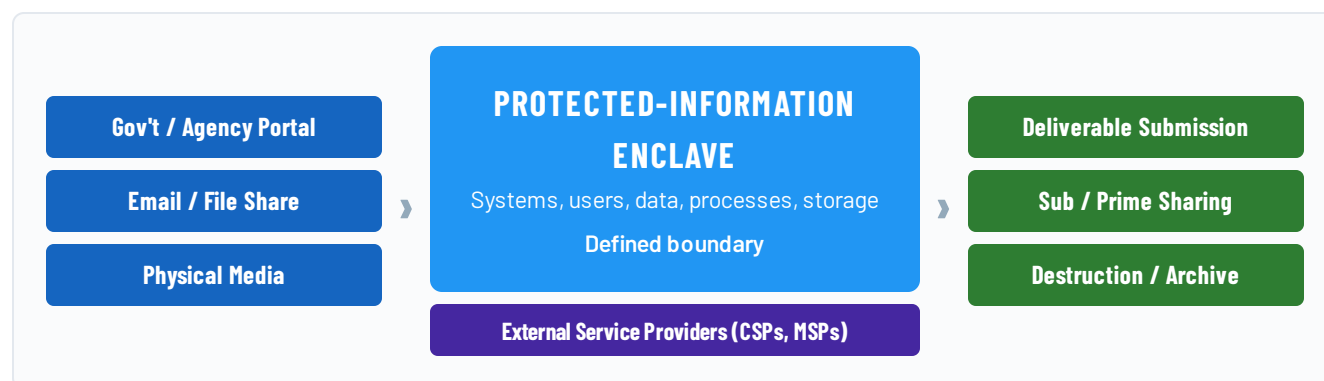


Figure 2: Environment components in Phase G. Every path CUI or FCI travels, in and out, must be mapped before any control is scored.

Starting with the clause, not the network

Phase G begins before any system is inventoried: with the contract. Which clauses are present determines which information is protected and which requirements apply. A Department of War contract carrying DFARS 252.204-7012 puts CUI and all 110 requirements in scope; one carrying only FAR 52.204-21 puts FCI and the 15 basic safeguarding requirements in scope. A civilian-agency contract may carry FAR 52.204-21, an agency CUI supplement, an agency-specific cybersecurity clause, or a prime's flow-down of NIST SP 800-171. Reading these together is the first Phase G deliverable. Scoping a network to protect information the contract does not actually put in the contractor's hands is as costly as missing information it does.

Defining the protected-information environment

The CUI environment is not synonymous with the organization's IT environment. It is the specific subset of systems, components, personnel, and processes that receive, generate, process, store, or transmit Controlled Unclassified Information (and, at Level 1 or under FAR 52.204-21 alone, Federal Contract Information). The boundary exercise must produce a specific, enumerated inventory that an assessor can use to independently scope the assessment:

- **Hardware inventory:** all workstations, servers, mobile devices, and network equipment within scope, identified by name, function, and operating system.
- **Software inventory:** all applications, cloud services, and platforms through which protected information flows, including versions and licensing status.
- **External Service Provider relationships:** all third-party services that process, store, or transmit protected information on the organization's behalf, including cloud infrastructure providers and managed service providers.

- **Data flows:** how information enters the environment (government or agency portals, email, physical media), where it is stored and processed, how it moves internally, how it is shared with subcontractors or primes, and how it is disposed of at contract close.

Ownership and accountability

Phase G must produce a clear accountability structure identifying the owner of every asset within the boundary, the Affirming Official responsible for the SPRS attestation or the agency attestation, the compliance Point of Contact, and the designated System Owner. These role assignments are referenced throughout the SSP and are direct targets of assessor interview activities. Personnel who do not know their role, or who describe it differently than it is documented, generate Interview findings.

Phase G key risk

The most common boundary error observed across Globe-America Consulting readiness engagements is under-specification of ESP relationships. Organizations routinely document their on-premises environment accurately and omit the cloud services, email platforms, and collaboration tools through which protected information actually flows. Phase G is complete only when every path that information travels has been mapped.



Phase A · Align Evidence

With the boundary established, Phase A maps every applicable NIST SP 800-171 requirement to the specific evidence artifacts that demonstrate its implementation. This phase directly addresses the Examine method, and it is the phase where the gap between documentation and assessment readiness most frequently manifests.

The evidence map

The evidence map is the operative output of Phase A: a structured reference that connects each SSP implementation narrative to specific, accessible artifacts that can be produced during Examine. A well-constructed evidence map enables the following during assessment:

- **Rapid evidence retrieval.** The assessor requests an artifact; the organization produces it within minutes.
- **Gap identification.** Any requirement with no evidence reference is immediately visible as an open item.
- **Currency monitoring.** Artifacts are tracked against review dates to prevent staleness.
- **SSP narrative validation.** Each implementation claim is cross-referenced against its supporting evidence.

Eliminating orphaned controls

An orphaned control is an SSP implementation narrative that makes a specific claim without a corresponding, accessible evidence artifact. Orphaned controls are among the most common sources of findings. They arise in three primary ways:

- **Template inheritance.** SSP language inherited from a vendor template that references controls not implemented in this organization's environment.
- **Evidence decay.** Artifacts that existed at the time of SSP development but have since been deleted, revised, or moved to inaccessible locations.
- **Aspirational documentation.** Narratives written to describe intended future-state implementations rather than the current verified state.

Phase A completion criterion

Phase A is complete when every implementation narrative in the SSP has at least one corresponding, accessible evidence artifact that can be produced on request. Until this condition is met, the organization has documentation, not assessment-ready documentation.

Phase R · Reinforce Implementation

Phase A produces documentation that accurately describes what should be implemented. Phase R verifies that it is. The critical insight driving Phase R is that documentation accuracy and system accuracy are not the same thing. An SSP can accurately describe the intended implementation of a control. The system can behave differently. When that gap exists, it is discovered during the Test method, not during documentation review.

Pre-assessment technical verification

Phase R consists of a systematic pre-assessment technical verification exercise: testing each claimed configuration against the SSP narrative before the formal assessment. Verification should cover every requirement subject to the Test method in the CMMC Assessment Guide, with priority weighting toward the requirements most frequently cited in conditional findings.

Verification area	Description	Priority
Multifactor authentication (IA.L2-3.5.3)	Verify MFA enforcement for all accounts, all entry points, and all privilege levels. Test specifically for service-account bypass paths, legacy protocol exceptions, and conditional access policy gaps.	HIGH
Audit logging (AU.L2-3.3.1 / 3.3.2)	Confirm that audit logs capture all required event types, that retention meets the 90-day minimum, and that logs are protected from modification.	HIGH
Access control (AC.L2-3.1.1 through 3.1.22)	Validate least-privilege account configurations, separation of duties for privileged accounts, and remote access controls against SSP claims.	HIGH
Configuration management (CM.L2-3.4.1 through 3.4.9)	Verify that system configurations match the documented baseline and that unauthorized software is actively blocked.	HIGH
Vulnerability scan coverage	Confirm that scanning covers the full boundary, including all hosts and ESP-managed assets.	MEDIUM

Incident response walkthrough	Test the documented incident response procedure with the IR team to confirm execution paths and reporting timelines (72 hours under DFARS 7012; agency-specific windows elsewhere) align with the SSP.	MEDIUM
Media protection / removable media	Verify enforcement of removable media restrictions and that any approved exceptions are documented and active.	MEDIUM
Security awareness	Confirm completion records and content currency of required training across all in-scope personnel.	LOWER

Table 3: Pre-assessment technical verification priorities. Tiers reflect the relative frequency with which the corresponding requirement families produce conditional findings in readiness work.

Ensuring personnel execution matches documentation

The Interview method evaluates whether personnel understand and correctly execute the controls documented in the SSP. Phase R addresses this through structured pre-assessment interviews with key personnel: the IT administrator, the compliance Point of Contact, the System Owner, and end users who handle protected information. The interview serves two purposes. It identifies gaps between the SSP narrative and actual operational practice that must be closed before the formal assessment, and it prepares personnel to articulate the organization's posture accurately and confidently in response to assessor questions.

D Phase D · Defend the Assessment

Phase D is the integration phase. Its function is to ensure that the work of Phases G, A, and R produces an organization that can survive the assessment across all three methods. The operative standard for Phase D completion is straightforward: minimize surprise findings on assessment day, whether the person across the table is a Third-Party Assessment team, a DIBCAC assessor, an agency reviewer, or a prime's due-diligence lead.

The mock assessment

The mock assessment is the central activity of Phase D: a structured simulation of the assessment, conducted by a qualified practitioner, that subjects the organization's posture to the same three-method evaluation it will face in the formal event. It produces a findings report that identifies contradictions, gaps, and vulnerabilities before an assessor does.

- **Examine simulation.** Document and evidence review against the assessment objectives in NIST SP 800-171A.
- **Interview simulation.** Personnel interviews against documented control implementations, rehearsed until the answers match the SSP because the practice matches the SSP.
- **Test simulation.** Technical verification of configurations against SSP claims.
- **Findings report.** Itemized list of contradictions, gaps, and readiness risks.
- **Remediation prioritization.** Ordered list of items requiring closure before the formal assessment.

Affirming Official preparation

The Affirming Official, typically the CEO, President, or COO, bears personal legal accountability for the accuracy of the SPRS submission under the False Claims Act, and comparable accountability for attestations made to a civilian agency or a prime. Phase D includes a structured Affirming Official briefing that ensures the person signing the attestation understands what they are certifying, has reviewed the pre-affirmation assessment record, and is prepared to describe the organization's compliance program accurately if asked by a contracting officer or an investigator.

Phase D Affirming Official standard

An Affirming Official who signs an attestation without a documented pre-affirmation review has no evidentiary basis for the accuracy of their legal certification. Phase D produces that basis.

§ 4 Cyber G.A.R.D.™ Across the Three-Year Lifecycle

A CMMC Level 2 certification, when the Phase 2 schedule resumes, is valid for three years. Within that period, and regardless of the certification schedule, organizations bear two ongoing obligations: the annual SPRS affirmation, which requires the Affirming Official to certify that the submitted score remains accurate, and preparation for re-verification at the end of the cycle. Civilian-agency contractors carry the equivalent in re-attestation at option exercise or recompetete. The framework is designed to support both.

Initial readiness	Year 1 maintenance	Year 2 maintenance	Year 3 re-verification prep
Full Cyber G.A.R.D.™ All four phases	G → A cycle Boundary review and evidence refresh	R phase Configuration re-verification	Full D phase Mock assessment and remediation

Table 4: Activity distribution across the three-year cycle. The framework is not a one-time checklist; annual affirmation obligations require continuous maintenance.

The annual affirmation

The annual SPRS affirmation is not a passive renewal. It is a legal certification that the organization's posture at the time of affirmation matches the submitted score. An organization whose environment has changed since the prior assessment, through technology migrations, personnel changes, or policy revisions, and which has not maintained its documentation accordingly, is submitting an inaccurate affirmation. The framework addresses this through a structured annual review: in Years 1 and 2, organizations cycle through Phases G and A, reviewing the boundary for accuracy, updating the evidence map for changes, and confirming that every implementation narrative remains true. This produces the documented pre-affirmation record that supports the Affirming Official's certification.

Re-verification preparation

In Year 3, organizations execute the full cycle. The Phase D mock assessment in Year 3 serves a specific purpose: identifying the implementation drift that has accumulated over the period and closing those gaps before the formal event. Organizations that have maintained the Phase G and Phase A cycles through Years 1 and 2 arrive at Year 3 with significantly less remediation than those who treat compliance as a point-in-time exercise.

§ 5 Beyond the Defense Industrial Base

The framework was developed in CMMC readiness work, and CMMC remains the most fully specified assessment regime a small contractor is likely to face. It is not, however, the only one. Civilian agencies handle CUI under 32 CFR Part 2002 and invoke NIST SP 800-171 in their contracts; primes on those contracts flow the requirement down; and several agencies add their own cybersecurity clauses with reporting windows and review rights. The control set is the same 110 requirements. The three assessment

methods are the same. What differs is who asks, what they call the review, and whether a score is posted anywhere.

Defense Industrial Base

Requirement source: DFARS 252.204-7012, 7019, 7020, 7021. Scoring: SPRS, affirmed annually. Verification: self-assessment, Third-Party Assessment, or DIBCAC Government Assessment. Phase D rehearses the assessor interview and the Affirming Official briefing.

Broader federal market

Requirement source: FAR 52.204-21, agency CUI supplements, agency-specific clauses, prime flow-downs. Scoring: none posted; the SSP and evidence are the case. Verification: agency review or prime due diligence. Phase D rehearses the reviewer's questions and the prime's questionnaire.

Because the framework keys to the assessment methods rather than to the clause, a contractor serving both markets runs one program. The Phase G clause review is where the two diverge, and it is the only place they need to.

§ 6 The NIST SP 800-171 Rev 2 to Rev 3 Transition

This paper is anchored on NIST SP 800-171 Rev 2, the control set on which CMMC Level 2 assessments are conducted under 32 CFR Part 170. NIST published Rev 3 in May 2024. As of September 2026 the Department of War continues to assess against Rev 2 for CMMC, while Rev 3 alignment work proceeds; civilian agencies may reference either revision in their contracts, which is one more reason the Phase G clause review comes first.

The framework is designed to remain stable across the revision change. Its phase logic is structured around the assessment process itself, the Examine, Interview, and Test dependencies, rather than around any specific list of control identifiers. The boundary work in Phase G applies whether the in-scope environment is measured against Rev 2 or Rev 3. The evidence alignment in Phase A and the technical verification in Phase R adapt to the active control set without changing the framework's structure.

Where Rev 3 introduces new requirements, particularly the consolidated organization-defined parameters (ODPs), the practical impact is contained within Phase A. Evidence maps that satisfied Rev 2 narratives will need to be reviewed against Rev 3 ODPs and supplemented where the new set requires additional evidence. The framework does not change. The artifact inventory expands. Organizations operating on a continuous lifecycle are positioned to absorb the transition during normal Year 1 and Year 2 maintenance rather than treating it as a separate event.

The recommendation for organizations approaching a first assessment in 2026 or 2027 is to align documentation and evidence to the revision named in the contract of record, while building Phase G and Phase A outputs in a structure that can be extended to Rev 3 ODPs as guidance issues. This is a content-layer recommendation, not a framework-layer change.

§ 7 Conclusion

The Cyber G.A.R.D.™ Framework is a practitioner-developed response to a specific and persistent failure mode in compliance practice: the gap between documentation and assessment survivability. Platforms generate documentation. A practitioner-led framework builds the organizational capability to defend it. The most successful programs use both.

The four phases, Govern the Boundary, Align Evidence, Reinforce Implementation, Defend the Assessment, follow the same logical sequence assessors follow in the CMMC Assessment Guide and in NIST SP 800-171A. They address each of the three assessment methods. They are designed for the operational reality of small and mid-size contractors, in the Defense Industrial Base and in the broader federal market. And they are structured for continuous application across the full lifecycle, through a Phase 2 pause and whatever follows it, not as a one-time exercise.

Contractors who build their programs on Cyber G.A.R.D.™ do not simply have documentation that says they are compliant. They have organizations that can demonstrate compliance under direct scrutiny. That distinction is the difference between conditional and unconditional findings, between a clean review and a costly remediation cycle, and between an affirmation an executive can sign and one they should not.

About the Author

Eddie White is the founder and Principal Consultant of Globe-America Consulting, Inc., a Service-Disabled Veteran-Owned Small Business based in Fort Worth, Texas. He is a Cyber AB Registered Practitioner, a Certified CMMC Professional candidate with adjudication pending, a Lean Six Sigma Master Black Belt, and an ISO 9001 Lead Auditor. His advisory practice serves small and mid-size contractors in the Defense Industrial Base and the broader federal contractor market, and every engagement is built on the Cyber G.A.R.D.™ Framework.

Prior to founding Globe-America, he served 20 years in the United States Air Force, including roles as an Information Security Manager and as a Contracting Officer's Representative with direct responsibility for government acquisitions and contractor oversight. Those assignments provided firsthand experience with the federal regulatory environment, contractor compliance expectations, and the acquisition structures that underpin federal contracting today.

He can be reached at eddie.white@globe-america.com, 682-284-2881, or globe-america.com.

References

Cyber AB. (2025). *CMMC Assessment Guide, Level 2*, current version. Retrieved from cyberab.org.

Department of War. (2024). CMMC Program Final Rule, 32 CFR Part 170. *Federal Register*, Vol. 89, No. 199.

Department of War. (2025). DFARS 252.204-7021, Cybersecurity Maturity Model Certification Requirements; effective November 10, 2025.

Department of War. (2026, July). Announcement of CMMC Phase 2 suspension and establishment of the CMMC Reform Task Force. [Cite the official notice.]

Defense Federal Acquisition Regulation Supplement. DFARS 252.204-7012, 252.204-7019, and 252.204-7020.

Federal Acquisition Regulation. FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems.

National Archives and Records Administration. 32 CFR Part 2002, Controlled Unclassified Information.

National Institute of Standards and Technology. (2020). *NIST SP 800-171 Revision 2: Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations*.

National Institute of Standards and Technology. (2024). *NIST SP 800-171 Revision 3*.

National Institute of Standards and Technology. (2021). *NIST SP 800-171A Revision 2: Assessing Security Requirements for Controlled Unclassified Information*.

Department of Justice. (2021). Civil Cyber-Fraud Initiative.

White, E. (2026). *CMMC Phase 1 Is Here: What Small Defense Contractors Need to Know Right Now*. Globe-America Consulting, Inc.

White, E. (2026). *The SSP as a Living Document: Structure, Evidence Alignment, and Assessment Survivability*. Globe-America Consulting, Inc.

The Cyber G.A.R.D.™ Framework is a proprietary compliance framework of Globe-America Consulting, Inc. Cyber G.A.R.D., G.A.R.D., the Cyber G.A.R.D. shield mark, and Govern · Align · Reinforce · Defend are trademarks of Globe-America Consulting, Inc. This paper represents the independent analysis and practitioner perspective of the author. It does not represent official Cyber AB, Department of War, or NIST guidance.