How the DIBCAC Assessment Works

Selection, Notification, and Execution of the Government's CMMC and NIST SP 800-171 Assessments

David W. Koran

CyberAB Registered Practitioner Advanced

September 2026

Summary

In plain terms: the Department of War operates its own team of cybersecurity assessors, separate from the commercial CMMC ecosystem. That team, the Defense Industrial Base Cybersecurity Assessment Center, selects contractors for review, notifies them through official correspondence, collects their security documentation, and verifies whether the protections reported to the government actually exist. Its staffing and assessment capacity are growing. This paper explains how the process works, from selection through the score recorded in the government's supplier database.

The Defense Contract Management Agency's FY2027 budget request funds 167 civilian positions for its cyber assessment mission, up from 141 in FY2025. The FY2026 increase of six positions established one additional functional assessment team expected to perform approximately 20 additional assessments annually. The FY2027 request adds 20 positions and three more teams expected to perform 65 additional assessments annually. The budget justification describes this as a phased hiring plan to meet the demand specified in the CMMC compliance rule. At full FY2027 funding, annual assessment capacity would exceed the FY2025 level by roughly 85 assessments.

Those teams belong to the Defense Industrial Base Cybersecurity Assessment Center, known as DIBCAC, the government organization that conducts Medium and High NIST SP 800-171 assessments of defense contractors, assesses every candidate CMMC Third Party Assessment Organization, and performs the government-led assessments within the CMMC program. Set against a Defense Industrial Base the CMMC Program rule sizes at approximately 220,000 entities, that capacity makes raw selection odds low and concentration the operative variable. This paper examines a DIBCAC assessment from the contractor's side in three phases: how the center determines who is assessed, how it informs the selected organization, and how it completes the assessment and records the result.

The Center and Its Capacity

DIBCAC operates within the Defense Contract Management Agency. When DCMA established the center in 2019, it opened with 42 employees and announced an intent to grow the assessment workforce substantially. In an August 2024 briefing, DCMA described a center of approximately 135 personnel, including assessors, team chiefs, group chiefs, business operations divisions, and training teams. The FY2027 budget documentation shows the trajectory continuing.

Fiscal Year	Civilian FTEs	Capacity Change
FY2025	141	Baseline
FY2026	147 (+6)	One additional functional team, approximately 20 additional assessments annually
FY2027 (request)	167 (+20)	Three additional functional teams, 65 additional assessments annually

The center's workload is broader than contractor assessments alone. The agency's budget justifications assign DIBCAC all CMMC Level 3 assessments of contractors supporting the Department's critical programs and technologies, the assessment of every candidate C3PAO's unclassified network before that organization may conduct CMMC Level 2 assessments, and continued post-award monitoring under DFARS 252.204-7012. The additional assessments funded in FY2026 and FY2027 are therefore distributed across contractor reviews, assessments of the assessors, and program support rather than representing contractor visits alone.

Two dates are worth holding side by side. The FY2027 budget request was published in April 2026, and the Department suspended the CMMC Phase II contract requirements in July 2026. The two actions sit on different tracks. The suspension addressed the schedule for requiring third-party certifications in contracts, while the budget line funds the government's own assessment workforce, which operates under DFARS clauses that remain in contracts today. Nothing in the budget documentation conditions the hiring plan on the Phase II schedule.

How DIBCAC Determines Who Is Assessed

Exposure to a DIBCAC assessment begins with the contract rather than with any selection algorithm. DFARS 252.204-7012 obligates a contractor handling covered defense information to implement NIST SP 800-171. DFARS 252.204-7019 requires a current Basic Assessment score in the Supplier Performance Risk System (SPRS) as a condition of award. DFARS 252.204-7020 then supplies the mechanism this paper concerns: the contractor shall provide access to its facilities, systems, and personnel necessary for the government to conduct a Medium or High NIST SP 800-171 DoD Assessment. Any contractor holding the clause can lawfully be selected, and consent isn't part of the process.

The assessment methodology defines three confidence levels. A Basic Assessment is the contractor's self-assessment and carries a confidence level of Low because the score is self-generated. A Medium Assessment is conducted by government personnel through a review of the Basic Assessment, a thorough document review, and discussions with the contractor. A High Assessment adds verification, examination, and demonstration of the system security plan (SSP) to validate that the requirements have been implemented as described.

The government doesn't publish a selection roster or the weighting behind it. What the record supports is narrower and still useful. The budget language ties assessment capacity to demand under the CMMC rule. The Level 3 mandate concentrates DIBCAC attention on contractors supporting critical programs and technologies. DCMA describes the center's mission as verifying the protection of contractor systems that store, process, or transmit CUI. From that record and from observed assessment activity, selection concentrates where program criticality, CUI volume, and supply chain position intersect. Aerospace manufacturers routinely sit at that intersection: they hold technical data packages and engineering specifications, they receive CUI from primes and pass it to lower-tier machine shops, and they frequently support propulsion, airframe, missile, and space programs. A strong self-reported SPRS score offers no insulation from selection. Verifying whether a reported score reflects an implemented reality is a substantial part of what Medium and High assessments exist to do.

Probability and Concentration

The raw probability of selection is low, and stating it precisely frames everything else in this paper. The CMMC Program final rule describes a Defense Industrial Base of approximately 220,000 entities, of which the Department estimates roughly 80,000 handle CUI and will require CMMC Level 2. DIBCAC's volume runs in the low hundreds of assessments per year. DCMA stated in early 2020 that the center was capable of conducting more than 100 DFARS 252.204-7012 assessments annually, and the funded FY2026 and FY2027 additions total approximately 85 more assessments per year, distributed across contractor reviews, C3PAO assessments, and program support. Even under the deliberately generous assumption that every assessment DIBCAC performs in a year were directed at a CUI-handling contractor, a few hundred assessments against roughly 80,000 companies puts the undifferentiated annual base rate below one percent. That figure is a ceiling for the population rather than a probability for any particular company, because selection isn't random and the Department doesn't publish its weights.

That arithmetic is the reason the risk factors in the preceding section matter more than the base rate. A capacity measured in hundreds can't be spent

randomly across a population measured in tens of thousands and still produce useful oversight, so selection concentrates. The factors already described, meaning program criticality, CUI volume, supply chain position, and a reported score that invites verification, do more than adjust a contractor's odds at the margin. They divide the population into a large group whose practical annual exposure approaches zero and a much smaller group for which selection is a foreseeable event within a contract's period of performance.

One concentration mechanism deserves separate treatment because it operates through no action of the affected company. When DIBCAC assesses a prime or mid-tier contractor, the assessment examines how CUI enters and leaves the environment. The SSP, the data flow diagrams, and the contractor's subcontract records identify by name the downstream companies that receive CUI from the assessed environment. Every one of those subcontractors already holds the access clause through mandatory flowdown, and the clause obligates the prime to confirm its subcontractors' assessment posture before award. A subcontractor of an assessed contractor is therefore visible to the assessment team, contractually exposed, and attached to the same program that drew the government's attention in the first place. No official policy states that assessing a prime triggers assessments of its subcontractors, and this paper doesn't claim one exists. The observation is narrower: an assessment of a prime converts its subcontractors from anonymous entries in a population of tens of thousands into named CUI recipients on a program the Department has already prioritized, and selection concentrates on exactly that kind of visibility.

How DIBCAC Informs the Contractor

No official template of a DIBCAC notification letter is published. The agency treats the notification as official correspondence issued to a specific contractor. The pattern described here therefore reflects the accounts of assessed contractors and the practitioners who supported them rather than a government publication, and individual notifications vary.

The notification generally arrives as official DCMA correspondence, commonly by email from a dcma.mil address to an executive or point of contact associated with the company in the System for Award Management, though no published template establishes a single delivery route. It identifies the assessment type and its contractual basis in DFARS 252.204-7012 and NIST SP 800-171, directs the contractor to acknowledge receipt and designate a technical point of contact within a few business days, and requests documentation: the current SSP, the plan of action and milestones, and network architecture diagrams, with related policies and procedures following as the review develops. For Medium Assessments, reported production timelines are short; assessed contractors have described

document requests due within roughly one to two business weeks. For High Assessments, reported notice generally runs about 30 days and includes a proposed schedule for the document review and for onsite or virtual interview sessions.

The operative point is that the notification starts a clock the contractor doesn't control. Because the access requirement in 252.204-7020 is a contract term, the assessment itself isn't negotiable. The variables available to the contractor are scheduling details and the quality of what it produces.

The Evidence DIBCAC Requests

The evidence demand arrives in two tranches. The notification requests the documents that define the environment: the SSP, the plan of action and milestones, and network architecture diagrams, with policies and procedures following as the review develops. The assessment itself then consumes a much wider evidence set, because NIST SP 800-171A defines three assessment methods, examine, interview, and test, and each method consumes its own kind of proof. Documents satisfy the examine method, personnel satisfy the interview method, and live demonstrations satisfy the test method. Medium Assessments stop at examination and discussion, while High Assessments use all three.

The categories below reflect the clause definitions, DCMA's published assessment materials, and the accounts of assessed contractors. No single assessment requests every artifact listed, and the team's requests narrow as the review develops, but each category has appeared in reported assessments and each maps to requirement families the methodology scores.

Category	Representative Artifacts
Core assessment documents	System security plan; plan of action and milestones; substantiation of the reported SPRS score; results of prior assessments
Environment and scope	Network architecture diagrams; CUI data flow diagrams; hardware and software inventories; asset lists defining the assessed boundary
Governance	Policies and procedures mapped to the 110 requirements; a documentation traceability matrix where one is maintained
Access and identity	Account inventories and access control lists; privileged account records; multifactor authentication configuration; remote access and session settings

Category	Representative Artifacts
System configuration	Baseline configurations; hardening settings; screenshots of security settings; change control records
Monitoring and audit	Audit log samples for specified periods; log review and alerting records; vulnerability scan results and remediation records; evidence that logs are retained for the period the SSP defines
Personnel and training	Security awareness and role-based training records; personnel screening records
Incident response	Incident response plan; test and exercise records; procedures for 72-hour cyber incident reporting to the Department under DFARS 252.204-7012
Physical security	Facility access and visitor records; media handling, marking, and sanitization records
External providers	Customer responsibility matrix from cloud and managed service providers; FedRAMP Moderate or equivalency documentation for cloud services storing CUI; agreements showing DFARS 252.204-7012 flowdown
Cryptography	FIPS 140 validation certificates, with CMVP certificate numbers, for the modules protecting CUI in transit and at rest

Log retention deserves a precise statement because a fixed number of years is often asserted and none exists in the governing documents. NIST SP 800-171 requirement 3.3.1 directs contractors to create and retain audit logs to the extent needed to support monitoring, analysis, investigation, and reporting, and the assessment objectives in NIST SP 800-171A test whether the contractor defined a retention period and whether records are retained consistent with that policy. The assessor therefore scores retention against the contractor’s own documented number, and a contractor with a defined one-year retention its logs substantiate outscores one with no defined period at all. The one hard figure in the regime sits elsewhere: after submitting a cyber incident report, DFARS 252.204-7012 requires preservation of affected system images and relevant monitoring and packet capture data for at least 90 days. Six-year figures circulating in industry guidance trace to the False Claims Act limitations period, which can reach ten years, and describe how long a compliance representation can be challenged rather than how long a log must be kept. A one-year retention with the most recent 90 days readily searchable is a common benchmark in practice, but it’s a design choice the SSP must state, not a regulatory floor.

Two characteristics of the evidence demand deserve emphasis. First, the evidence must agree with the SSP rather than merely exist. The methodology verifies the plan against the environment, so a policy describing a control the configuration doesn't show, or a configuration the plan doesn't describe, reads as a discrepancy rather than as partial credit. Second, evidence must be producible on the assessment's schedule. During a High Assessment week, the team asks named personnel to demonstrate controls live: producing an audit log for a specified period, presenting a multifactor authentication challenge, displaying encryption settings, or walking through an account provisioning request. A control that works but can't be substantiated during the assessment may be scored as not implemented, subject to the follow-up evidence and rebuttal process described later in this paper, because the methodology credits verified evidence rather than verbal assurance.

How DIBCAC Completes the Assessment

The clause definitions establish what each assessment level involves, and reported practice fills in the format.

Element	Medium Assessment	High Assessment
Method	Review of the Basic Assessment, a thorough document review, and discussions with the contractor as needed	All Medium elements plus verification, examination, and demonstration of the system security plan against NIST SP 800-171A
Format	Documentation based, conducted virtually in reported practice	Onsite or virtual, with scheduled interviews and live demonstrations
Confidence level	Medium	High
Reported notice	Short; document production described in roughly one to two business weeks	Approximately 30 days, with a proposed schedule for review and interviews

Contractor CMMC Level 3 assessments sit in the same building but under a different rule. Where Medium and High Assessments verify NIST SP 800-171 under the DFARS clauses, a Level 3 assessment is conducted by DIBCAC under the CMMC Program rule at 32 CFR part 170 for contractors supporting the Department's most critical programs, presupposes a CMMC Level 2 certification, and adds 24 selected requirements from NIST SP 800-172. The population subject to Level 3 is small, and the Phase II suspension left its contract-requirement schedule unsettled, so this paper concentrates on the

Medium and High Assessments that make up the bulk of DIBCAC's contractor-facing work.

DCMA has published its working cadence for the assessments it performs on candidate C3PAOs, and participant accounts describe contractor High Assessments following the same general arc. Documentation is delivered roughly two weeks before the assessment. The team conducts an internal readiness review ending in a go or no-go decision, finalizes the assessment plan and the interview and demonstration schedule the week prior, executes during a defined assessment week, and delivers an out-brief. In the published C3PAO cadence, the final memorandum and report follow within ten business days of the out-brief.

Scoring follows the NIST SP 800-171 DoD Assessment Methodology. Each of the 110 requirements carries a weight of five, three, or one point, deducted from a perfect score of 110 when a requirement is not implemented, with a floor of negative 203. The assessment verifies the SSP against the assessment objectives in NIST SP 800-171A. A requirement is credited when the implementation matches what the plan describes and the evidence supports it.

The clause also governs how the result is recorded. The Department posts Medium and High summary level scores to SPRS, including the standard assessed, the assessing organization, every CAGE code covered by the SSP, a brief description of the plan architecture where more than one plan exists, the date and level of the assessment, the summary score, and the projected date for reaching 110. Before posting, the Department provides the score to the contractor and offers rebuttal and adjudication, and the contractor has 14 business days after the assessment to provide additional information demonstrating requirements the team did not observe or to rebut questioned findings. Documentation generated in a High Assessment beyond the score is retained by the Department as CUI and protected from release, including under Exemption 4 of the Freedom of Information Act.

The recorded score has consequences beyond the assessed company. A government-conducted score sits in SPRS beside the self-reported Basic score, visible to Department components making award decisions, and the government's number is the one those readers weigh. The clause also flows down: a prime may not award a subcontract subject to NIST SP 800-171 unless the subcontractor has at least a current Basic Assessment posted in SPRS.

What the Mechanics Mean for a Contractor

Three observations follow from the mechanics themselves rather than from any prediction about enforcement.

First, the timeline is the constraint. The documentation a notification requests is produced within days or weeks of receipt. An SSP, a plan of action and milestones, and architecture diagrams that must be written after the notification arrives will be written under the worst possible conditions and reviewed by a team whose method is to compare them against observed reality.

Second, the SSP is the assessed artifact. Rather than measuring security in the abstract, the assessment measures whether the environment matches the plan and whether the assessment objectives are satisfied. A strong self-reported score that the plan and evidence cannot substantiate resolves into a low government-recorded score, and that recorded score is what contracting officials see.

Third, capacity growth changes the probability of assessment rather than the process. The clause dates to 2020 and the methodology has been stable since version 1.2.1 was issued that June. What the FY2026 and FY2027 budget actions change is how many times each year the process runs. For a contractor whose documentation is current, evidence-backed, and consistent with its reported score, more assessments change little, while a contractor whose reported score outruns its evidence sees its annual selection odds rise with every added team.

A Test Any Executive Can Run

The fastest way for an executive to learn where the company stands is to run a small version of the notification internally. Ask the IT lead or managed service provider for four items within one business day: the current SSP, the plan of action and milestones, the network and CUI data flow diagrams, and audit logs covering a recent 30-day window of your choosing. The request should arrive without advance warning, because a DIBCAC notification arrives the same way, and the one-day window is deliberately tighter than the one to two weeks a Medium Assessment allows. The compressed timeline separates documentation that exists from documentation that would need to be written in response to the request.

The results sort into three readings. Documents delivered within the day and consistent with the score reported in SPRS indicate a company that would meet a real notification on its own terms. If the documents arrive but disagree

with each other or with the reported score, the company has the discrepancy problem this paper describes, and closing it is a smaller project now than it would be during an assessment. And documents that can't be produced at all indicate that the reported score rests on implementation the company can't currently evidence, which is precisely the condition a Medium or High Assessment converts into a recorded government score.

The one-day test is a snapshot, and the durable version of it is a schedule. Conducting genuine self-audits at a regular interval, whether performed internally or by a qualified third party, keeps the SSP, the reported score, and the evidence aligned as the environment changes, because that alignment is what decays between reviews. A company that audits itself against the NIST SP 800-171A objectives finds its own discrepancies while they're inexpensive to close, and it also changes the character of a DIBCAC assessment if one arrives: the team receives organized, previously tested evidence, the interviews cover controls personnel have already demonstrated, and the assessment proceeds on the contractor's documentation rather than on gaps discovered in real time. The distinction that matters is between a genuine audit that tests evidence against the assessment objectives and a checkbox review that reaffirms last year's answers, because DIBCAC's method reproduces the former.

The planning conclusion follows directly: the documentation set a DIBCAC notification requests should exist, current and evidence-backed, before the notification arrives, and one business day of internal notice is enough to find out whether it does.

About the Author

David W. Koran is a CyberAB Registered Practitioner Advanced (RPA) and the founder of a consulting practice serving Defense Industrial Base contractors and their legal counsel, focused on CMMC readiness, enablement, and implementation. He is an Associate Member of the American Bar Association Section of Public Contract Law and the author of The CMMC Decision. His viewpoint article on the CMMC appeared in National Defense Magazine in July 2026, and his analysis of CMMC assessment capacity was featured in Forbes in September 2026. He can be reached at dkoran@davidkoran.com or (802) 335-2662.

References

Department of War, Fiscal Year 2027 Budget Estimates, Operation and Maintenance, Defense-Wide, Volume 2 (DCMA Cyber exhibits). https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2027/

budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_2/Volume_2.pdf

Department of War, Fiscal Year 2027 Budget Estimates, PB-31Q Personnel Summary (DCMA Cyber). https://comptroller.war.gov/Portals/45/Documents/defbudget/FY2027/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_2/PB-31Q.pdf

Fiscal Year 2024 Budget Estimates, Defense Contract Management Agency Cyber OP-5 (DIBCAC mission description). https://comptroller.war.gov/Portals/45/Documents/defbudget/fy2024/budget_justification/pdfs/01_Operation_and_Maintenance/O_M_VOL_1_PART_1/DCMA_Cyber_OP-5.pdf

DFARS 252.204-7020, NIST SP 800-171 DoD Assessment Requirements, eCFR. https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7020

DFARS 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, eCFR. https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7012

31 U.S.C. 3731, False Claims Act procedure (limitations periods). https://www.law.cornell.edu/uscode/text/31/3731

DFARS 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements, eCFR. https://www.ecfr.gov/current/title-48/chapter-2/subchapter-H/part-252/subpart-252.2/section-252.204-7019

NIST SP 800-171 DoD Assessment Methodology, Version 1.2.1 (June 2020). https://www.acq.osd.mil/asda/dpc/cp/cyber/docs/safeguarding/NIST-SP-800-171-Assessment-Methodology-Version-1.2.1-6.24.2020.pdf

NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information. https://csrc.nist.gov/pubs/sp/800/171/a/final

DCMA, Building a Cybersecurity Assessment Capability (2019). https://www.dcma.mil/News/Article-View/Article/1885182/building-a-cybersecurity-assessment-capability/

DCMA DIBCAC, Leveraging DCMA Capabilities, briefing to the Defense Acquisition University (August 2024). https://www.waru.edu/sites/default/files/2024-08/Leveraging_DCMA_Capabilities_DIBCAC_DAU%20Presentation_8_13_24.pdf

DCMA DIBCAC, CMMC Assessment Team Candidate C3PAO Assessment Process briefing (2021, approved for public release). https://insidecybersecurity.com/sites/insidecybersecurity.com/files/documents/2021/apr/cs2021_0075.pdf

Cybersecurity Maturity Model Certification (CMMC) Program, Final Rule, 89 FR 83092 (October 15, 2024). https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

32 CFR part 170, Cybersecurity Maturity Model Certification (CMMC) Program, eCFR. https://www.ecfr.gov/current/title-32/subtitle-A/chapter-I/subchapter-M/part-170

DCMA, DCMA's Contributions to Cybersecurity through DIBCAC (assessment capacity statement). https://www.manufacturingtechnologyinsights.com/cxoinsights/dcma-s-contributions-to-cybersecurity-through-dibcac-nwid-2229.html

Department of War Chief Information Officer, About CMMC. https://dodcio.defense.gov/cmmc/About/