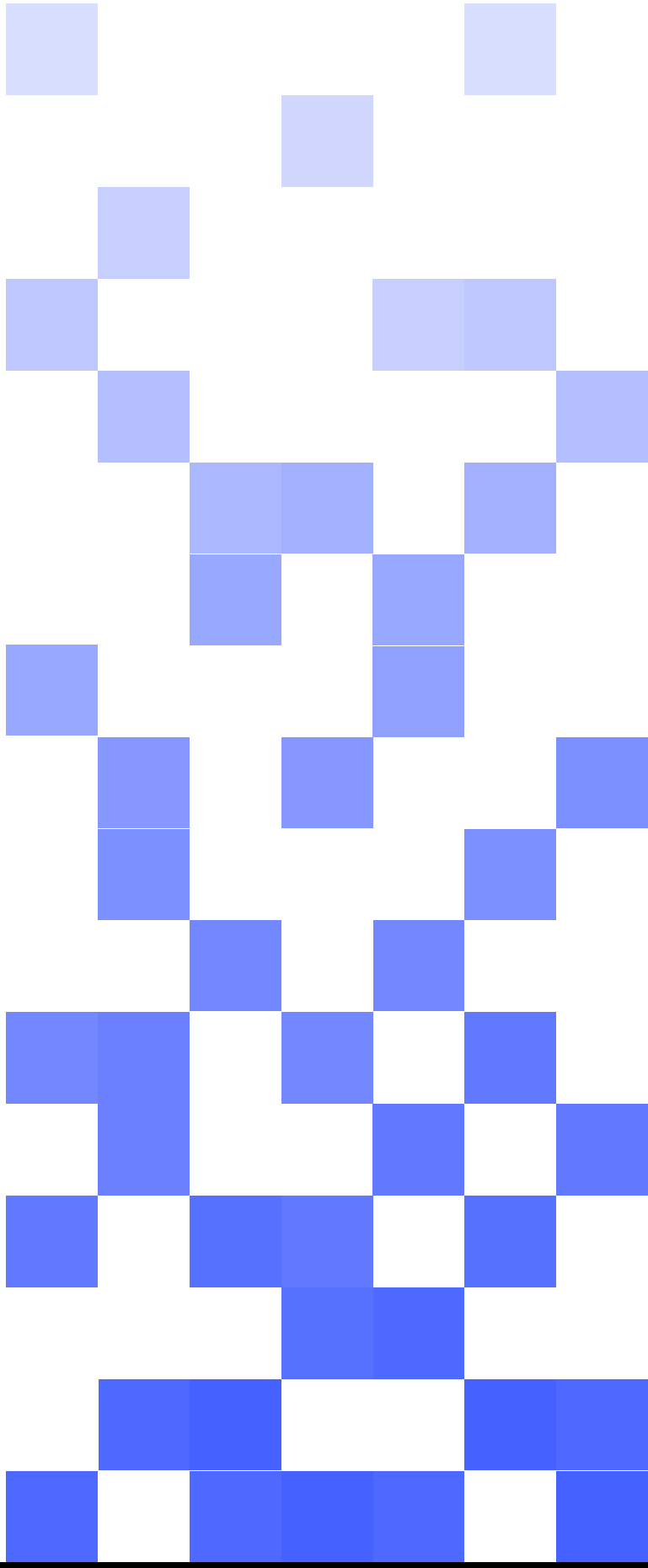
REPORT

The CMMC Readiness Gap: What the Assessors Saw Before Phase II Was Paused

www.sentinelblue.com

SENTINELBLUE

TABLE OF CONTENTS



INTRODUCTION

EXECUTIVE LETTER

We began writing this report right before a moment of significant change for the DIB, intending to talk about what CMMC readiness looked like as Phase II approached. Then the suspension announcement landed, sharpening our inquiry into a pressing question: where does the industry actually stand?

To find out, we sat down with five independent C3PAOs conducting CMMC Level 2 assessments and asked what they were actually seeing during their engagements with defense contractors over the last 18 months.

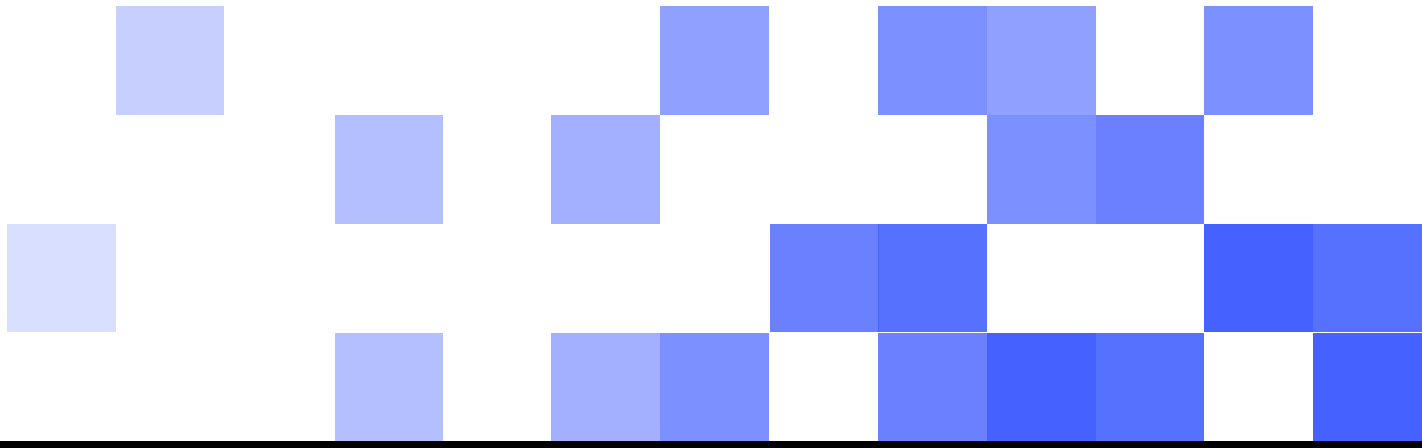
Most people will be unsurprised to hear that the DIB was largely not ready for Phase II. What we wanted to dig into was the "why": what the specific obstacles are, where OSCs get tripped up, and what's been separating the organizations that pass from the ones that don't.

It's no secret that CMMC is difficult. Good information about what's actually happening on the ground is hard to come by, and much of what circulates is either secondhand, anecdotal, or selling you something.

This report is one effort to close that gap. Our hope is that it will help both the federal contractors and the many service providers who support them as we navigate the changing CMMC landscape together.

Shields Up,

Andy Sauer, CEO, Sentinel Blue



ABOUT THIS REPORT

This report is based on semi-structured interviews with five independent C3PAO assessors, each drawing on direct experience conducting CMMC Level 2 assessments with defense contractors over the past 18 months. It is qualitative by design: rather than survey data or aggregate statistics, it captures what assessors are seeing firsthand, in their own words, across a range of organization sizes and industries within the DIB.

The report centers on common challenges for organizations seeking certification (OSCs) and the current state of CMMC preparedness among defense contractors. Findings are presented alongside relevant context on the regulatory landscape and the Phase II suspension, but the core of the report is the assessors' own observations.

Methodology

The interviews were conducted via Microsoft Teams in June and July 2026 with representatives from five C3PAOs: Cybersec Investments, Hive Systems, Kieri Solutions, Smithers, and Sentinel Blue (the publishers of this report). Collectively, these assessors work with organizations ranging from very small businesses with two employees to large primes with over 130,000 employees, though the majority of their engagements involve subcontractors and small-to-midsize suppliers. The organizations they assess span a wide range of verticals, including aerospace, manufacturing, software development, professional services, construction, and managed IT services. Gabrielle Hovendon, PhD, conducted the interviews and authored this report on behalf of Sentinel Blue.

A Note on Terminology

Throughout this report, we use "CMMC requirements" as shorthand for the more technically accurate "NIST SP 800-171 Rev. 2 requirements." In keeping with our mission to demystify CMMC compliance, we've favored the colloquial terms and abbreviations most familiar to our DIB audience.

SECTION ONE

SHIFTING SEAS & DIRE STRAITS FOR THE DIB

This report comes at a moment of significant change for the DIB. Last month, the Pentagon announced the immediate suspension of CMMC Phase II mandates, citing incompatibility between the need for third-party assessment and the need to rapidly expand the DIB. Now, as we wait for the task force report and feedback from a public RFI, it's unclear whether CMMC Level 2 C3PAO assessments will resume in their current form on an extended timeline or whether the third-party assessment mechanism will change altogether.

As justification for the suspension, DoD CIO Kirsten Davies cited assessor capacity, noting the 100,000+ DIB businesses needing a third-party assessment versus the roughly 100 available C3PAOs. Although it's true that many assessors are currently booked out past November, the reality is more nuanced.

The C3PAOs interviewed for this report all described turning down some OSCs seeking assessment, not because of a lack of capacity but because of the organization's lack of preparedness. It was a theme that came up again and again in our conversations, along with significant concern about the now-paused November timeline. While the fact that the DIB is unprepared won't come as a shock to anyone familiar with CMMC, the sheer size of the problem may be surprising.

> "On a scale of 1 to 10, where 1 means they can't spell CMMC and 10 means they're ready for Level 2 tomorrow morning, the average OSC is at a 3. They go in thinking it's a quick checklist, and they come out realizing they didn't understand the depth of CMMC controls."
>
> **– Robert McVay,** Senior Consultant for Information Security Services, Smithers

"We've been turning away about 20-30% of people that have a call with us because they're simply not ready for assessment," said Fernando Machado, Managing Principal and CISO of Cybersec Investments, which recently became the first fully accredited C3PAO. He noted that those percentages have held fairly steady over the last year as the overall level of readiness in the DIB remained low.

"They're not ready and they're panicking," agreed Kenny Watts, Lead Assessor at Sentinel Blue. "We've been seeing a huge number of clients that were pushing to do an assessment before November because a contract said they have to have it, but the overall preparedness is not improving across the board."

Robert McVay, Senior Consultant for Information Security Services at Smithers, had a similarly conservative take. "On a scale of 1 to 10, where 1 means they can't spell CMMC and 10 means they're ready for Level 2 tomorrow morning, the average OSC is at a 3," he said. "The average organization is also a minimum of six to nine months away from being ready to start an assessment. The ones that say before their pre-assessment that they'll be ready in one month, they almost unanimously ask for three to five more months to prepare once we've spoken. They go in thinking it's a quick checklist, and they come out realizing they didn't understand the depth of CMMC controls."

This lack of knowledge around CMMC requirements is central to understanding what's really happening in the DIB. It's not that organizations lack the resolve or dedication to meet the requirements, but rather that they don't know what they're walking into. These gaps in knowledge, along with the high cost of remedying them, are at the core of the unpreparedness epidemic. Resolving this widespread lack of knowledge will be key to improving CMMC for the future.

SECTION TWO

WHY IS NO ONE PREPARED?

We've known that CMMC third-party attestation was coming for a long time. Self-attestation of NIST SP 800-171 compliance has been required for defense contractors since 2017 under DFARS 252.204-7012, and third-party assessment has been on the horizon ever since CMMC was first introduced in 2019. In other words, November 2026 wasn't a surprise deadline sprung on the DIB overnight; Phase II came with plenty of warning.

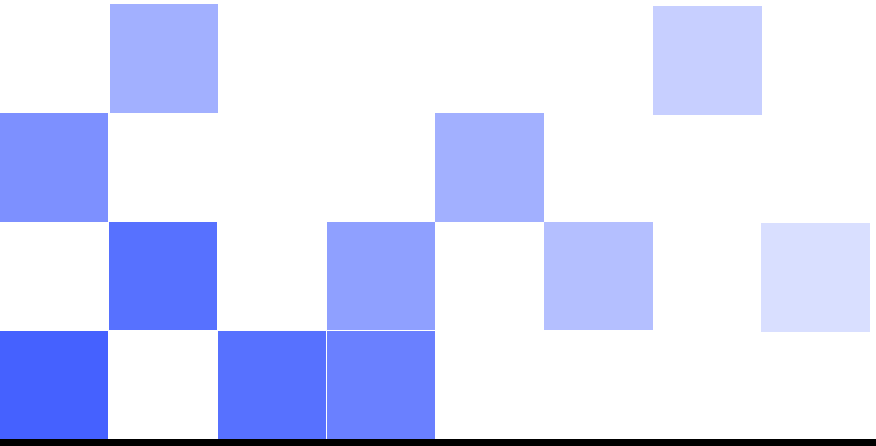
Still, many organizations have hesitated to begin the third-party assessment process. Our conversations revealed two key reasons: complexity and cost.

A Complex Framework

First, CMMC requirements are notoriously difficult to interpret without extensive experience in the space, and that complexity has led to foundational gaps in understanding. Without a strong sense of what's expected or where to start, organizations have consistently put off both their preparation and their third-party assessment.

"There are so many people in the defense contractor space who don't understand what assessment looks like," McVay said. "They don't understand the process, they don't know what C3PAOs look for, and they don't understand the CAP [the Cyber AB's procedural guide for assessments] because they haven't read it. There's still so much of the population that doesn't have any idea how the assessment is going to go."

For some companies, the lack of understanding has been paralyzing. For others, it's lent a false sense of confidence that CMMC would be just like any other audit: easily passed as long as general best practices are being followed. The reality, that CMMC requires extensive evidence and highly specific documentation, has been an unpleasant surprise for many organizations.



"People have assumed CMMC is a checkbox exercise and then found out it wasn't. Some have come from adjacent frameworks and have extensive experience in compliance, but the underlying CMMC requirements are unique in the fact that organizations have to both write down what they're doing and then show evidence. It's a challenging framework."

– Sam Heuchert, Lead Cybersecurity Assessor, Kieri Solutions

"People have assumed CMMC is a checkbox exercise and then found out it wasn't," said Sam Heuchert, Lead Cybersecurity Assessor at Kieri Solutions. "Some have come from adjacent frameworks and have extensive experience in compliance, but the underlying CMMC requirements are unique in the fact that organizations have to both write down what they're doing and then show evidence. It's a challenging framework."

This is compounded by the fact that some CMMC requirements spell out exactly what's expected while others are frustratingly vague, leaving organizations to interpret ambiguous language or figure out how a control applies to their specific environment without much guidance from the government. That inconsistency makes it difficult for organizations to develop reliable instincts for how to approach the framework.

In theory, the solution is straightforward: acquire deep subject matter expertise to help navigate the inconsistency and complexity of CMMC. In practice, this expertise has been difficult for many organizations to come by, and that's because of the second key reason organizations have delayed their third-party assessments: cost.

The High Price of Compliance

It's no secret that CMMC certification is expensive. The cost of certification is cited often, and for good reason: Assessment costs alone can range from $30,000 for a relatively small enclave to over $150,000 for a more complex environment with many users, and that's not accounting for the tens of thousands typically needed to implement the technical controls in the first place.

Part of the cost is structural. The government requires at least three CCAs to be involved in every Level 2 assessment, and that staffing requirement gets passed along in C3PAO costs. Assessment length adds to the cost as well: the larger the scope and the more complex the environment, the more assessment typically costs.

But it's also an investment to gain the knowledge needed to prepare for certification in the first place, particularly for SMBs with limited in-house IT capacity. It can cost well over $10,000 in certifications and schooling to gain the recommended CCP (Certified CMMC Professional) and CCA (Certified CMMC Assessor) credentials, including exam fees and background checks.

Unfortunately, this level of investment is often what it takes to understand the framework well enough to get through the assessment in one piece. Although CMMC's requirements are grounded in good cybersecurity practices, they do require qualified experts to implement and maintain them to the required level. For plenty of OSCs, that just isn't feasible.

"If an organization wants to do their CMMC preparation themselves, they're going to have to pay an exorbitant amount of money to get someone on staff certified," Watts said. "And if they don't have an experienced consultant to guide them, they'll be seriously struggling when it comes time for the assessment."

Compounding the entire problem is the fact that CMMC is as unforgiving as it's expensive. It includes very low tolerance for evidence gaps, very limited recourse to fix problems after an audit starts, many controls that can't be placed on a POA&M, and a strict pass/fail rubric. Failing an assessment means not just going back to fix the gaps but also paying tens of thousands of dollars for another full assessment.

Given the rigidity of the framework, the high cost of certification, and the difficulty of accessing knowledge, the contractors who *have* completed their Level 2 assessment are the exception rather than the norm: a testament to the resources and preparation it takes to clear the bar.

WHO STRUGGLES MOST WITH CMMC?

There's no one-size-fits-all profile for organizations that flounder or excel at CMMC preparation. Assessors recalled working with large defense contractors that were "spectacularly ready" as well as ones that were "spectacularly not ready"; with small mom-and-pop businesses that showed up highly prepared as well as ones that raised the question "what were you thinking?"

However, there were several traits that generally correlated with better CMMC Level 2 outcomes. First, organizations that have already gone through FedRAMP, NIST 800-53, ISO 9000, IATF 16949, or AS9100 assessments tend to do better because they're already familiar with working within strict compliance frameworks. Even when standards don't map directly to CMMC controls, the general practice of writing policies, documenting controls, and going through audits tends to help with CMMC preparedness.

Second, organizations whose core business involves an IT focus are often better prepared, likely because they already have the in-house knowledge to configure their IT environments correctly.

Where a construction firm might be discovering the difference between session lock and session termination for the first time, a tech company will already be familiar with technical controls and the configurations they require.

There are also common markers of organizations that are likely to struggle. While some small companies do show up to their Level 2 assessments well prepared, most tend to find CMMC challenging. The DoD has estimated costs for a small contractor to be at least $150K for an enclave-only approach in the first year alone, with assessment typically costing around $50K on average. For a company with only a few employees, this can be prohibitively expensive.

"The smaller companies tend to struggle more because they're coming from the perspective that money is tight," McVay explained. "The larger companies go out and hire an MSP and consultants; they throw money at the problem. The smaller companies can't afford to spend half a million on preparedness; they just don't have the budget."

Another profile with particular CMMC outcomes is manufacturers. Because they have specialized assets, legacy equipment, physical security concerns, and on-prem environments, manufacturers often find that upgrading their cybersecurity is a major operational shift.

Counterintuitively, though, these challenges sometimes translate to better preparedness. Because there is so much work to do across the entire organization, leadership often "understands that it's not just the IT team's problem" and invests in good communication and training, Heuchert said.

"They see they have these legacy processes and machines, and they see the need to train their internal staff because most outside consultants aren't going to have the 25 years of experience working with that one computer in the corner that's running Windows XP," he explained. "Those profiles of manufacturers seem to be doing extremely well in their preparedness."

The most challenging control families, according to the experts:

Access Control (AC): The largest family, with 70 assessment objectives spanning remote, mobile, and wireless access... and most can't be POA&M'd.

Identification and Authentication (IA): Common challenges include MFA implementation, session timeouts, and consistent enforcement.

Configuration Management (CM): Changes to systems routinely go undocumented, leaving no evidence trail.

Risk Assessment (RA): Common gaps include missing tabletop exercises, stale risk assessments, and registers not being updated after incidents.

System and Information Integrity (SI): Covers remediation, malicious code protection, and monitoring for alerts, but companies often misunderstand the reqs.

SECTION THREE

GRC TOOLS VS. HUMAN EXPERTISE

With limited budgets, some companies turn to GRC tools and platforms that promise to map controls, track evidence, and manage POA&Ms in one place. Whether they actually deliver on CMMC readiness is another question.

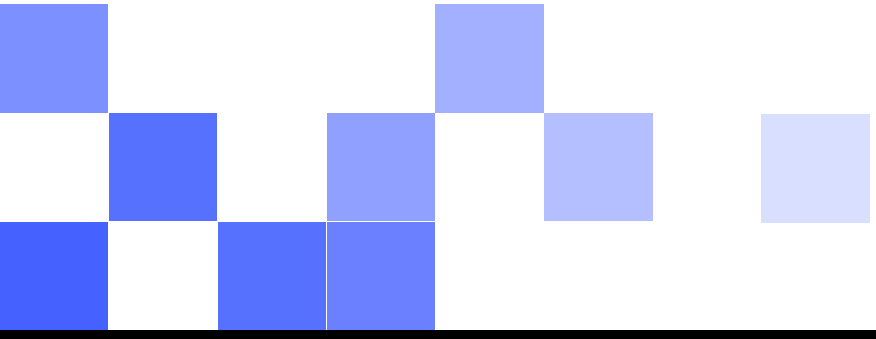
"The concern is around 'garbage in, garbage out,'" Machado said, explaining that around 30% of the OSCs he sees have invested in a dedicated compliance tool. "Whether it's helpful depends on whether the organization even understands the requirements. The tool is only as good as the quality of evidence being added to the portal."

In general, the assessors noted that GRC tools could be useful to keep evidence organized, particularly for larger companies juggling multiple frameworks. However, engaging a third-party platform mattered less than having a knowledgeable expert on the team. For many OSCs, that has meant bringing in an outside consultant, advisor, or managed service provider to guide CMMC preparation.

The one caveat? They have to be experienced in the space.

"There are certain service providers who don't understand the full scope of CMMC or are relying on marketing tactics instead of expertise, and unfortunately the customer ends up paying the price," said Katie Dodson, President of Hive Systems. "A good MSP will know the regulations, put their people through CCA and CCP classes so they know what assessors are looking for, and stay up to date with changes for their clients."

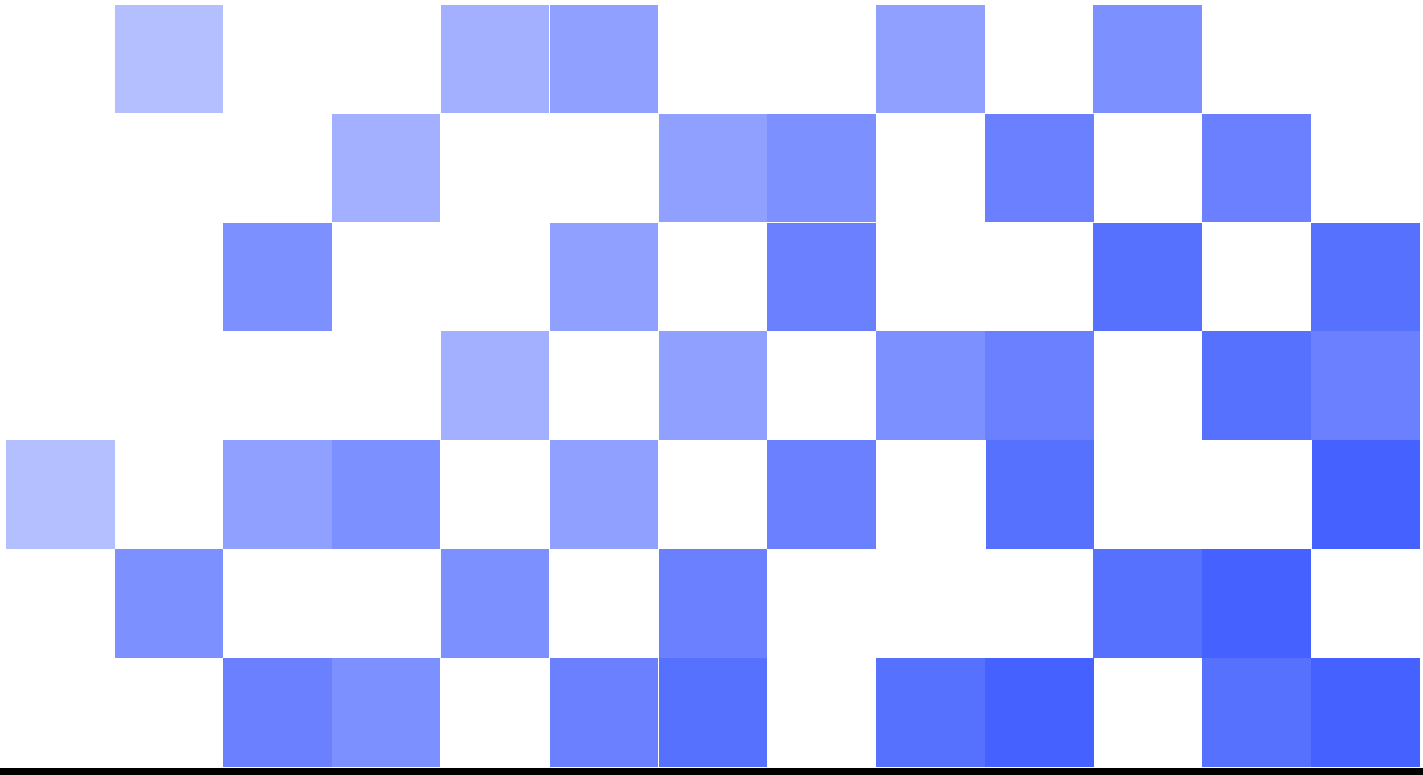
"It's highly dependent on the quality of the consultant or MSP," McVay agreed. "Above all, your expert needs to know the source material. As C3PAOS, we live by 32 CFR and DFARS, so you have to understand those."



> “The people who try to do it themselves are going to misinterpret the requirements and miss things. We tell people all the time that this is a multi-department initiative, not something that exists in a vacuum, and it’s worth the investment to get it right. You’re going to waste a lot of time and money if you do it wrong.”
>
> **– Katie Dodson,** President, Hive Systems

Of course, not every organization can afford that level of help, and the fallback options are thin. There are a few free or low-cost resources (e.g. NIST publications, the Cyber AB’s own guidance, and peer networks of other OSCs going through the same process), but none of them are real substitutes for hiring expertise.

“The people who try to do it themselves are going to misinterpret the requirements and miss things,” Dodson said. “We tell people all the time that this is a multi-department initiative, not something that exists in a vacuum, and it’s worth the investment to get it right. You’re going to waste a lot of time and money if you do it wrong.”



SECTION FOUR

DOCUMENTATION CHALLENGES

Surprisingly, what trips up organizations most during the assessment isn't the technical controls; it's the documentation. Assessors can often predict how an engagement will go within the first few hours based on an organization's documentation alone.

"When organizations come to us with a very short SSP, that's usually a red flag," Machado said. "If you're only giving us one-sentence answers, we're going to have to dig in, and it makes the assessment longer."

Dodson agreed. "If someone just gives me a bare-minimum SSP, it doesn't mean they're not compliant or they're not going to pass, but we have to dig a lot more to find what we need. It makes the assessment much more challenging," she said. "When I see an SSP where every objective is lined up and addressed individually and mapped to individual policies and procedures, it's fantastic. It's rare, but I love to see those."

Inconsistent documentation is one facet of the challenge. An SSP, a policy, and an evidence screenshot might each list a different value for the same control (for example, stating different times for the inactive session timeout under 3.1.11). Any of those values could be technically acceptable, but inconsistency between the artifacts creates doubt and concern for assessors, which in turn creates friction in the assessment.

Missing documentation, including organization-defined parameters (ODPs), poses a similar challenge.

The trickiest technical controls for OSCs:

3.1.10 (Session Lock) / 3.1.11 (Session Termination)
Frequently confused with each other. Both require re-authentication, but they trigger differently.

3.1.22 (Control CUI on Publicly Accessible Systems)
Often misinterpreted. Applies to public platforms like company websites and social media accounts.

3.13.11 (FIPS-Validated Cryptography)
Must be implemented, not just documented, and patching a FIPS-validated module can invalidate it.

3.3.3 (Review of Audit Logs)
Frequently conflated with capturing event logs and SIEM alerts.

3.5.3 (Multifactor Authentication)
Commonly rolled out in cloud environments but forgotten on local devices like firewalls and servers, leaving perimeter gaps.

"A lot of assessment teams have to ask, 'How did you define X?'" Heuchert said, noting that ODPs can trip up companies even when their technical controls are correct. "We can't assess something if you haven't defined it first. That structure throughout the entire assessment is challenging."

Below the surface, though, the problem is more complex than forgetting to write something down. CMMC's technical controls are challenging enough that they can easily dominate an IT team's focus, leading organizations to skimp on creating practical, well-documented administrative procedures. The result is a business that may have expended all their efforts on getting the technical requirements right, only to fumble at correctly defining and documenting their policies.

While C3PAOs have been criticized for being overly rigid about documentation, it's more often that the framework and regulations themselves are rigid. Even when assessors would like to suggest a quick fix for an incorrect policy, the CMMC guidelines are very strict: assessors must remain impartial and cannot act in a consultative way, not even to offer general advice or point out simple solutions to OSCs.

"It can feel punitive when they don't understand the requirements," Dodson said. "I hear organizations say, 'oh, that's what that meant? We could have fixed that in a minute if we'd known.' It's a huge challenge when the vast majority of controls are not POA&M-able."

"We can't say things like 'you're missing a signature on that policy, go get it and come back,'" Watts added. "It's why you really need an expert in your corner. If organizations have a consultant that's actively participating in the assessment with them, then the easy mistakes get addressed before it's too late. If they don't, even the highly technical people are struggling to catch everything and get the documentation right."

"You really need an expert in your corner. If organizations have a consultant that's actively participating in the assessment with them, then the easy mistakes get addressed before it's too late. If they don't, even the highly technical people are struggling to catch everything and get the documentation right."

– Kenny Watts, Lead Assessor, Sentinel Blue

SECTION FIVE

WHAT'S NEXT FOR THE DIB?

The suspension of CMMC Phase II will likely have major repercussions for defense contractors. Even if C3PAO assessments resume like usual after the 60-day review period, change is on the horizon. Rev 3 is about to be introduced, raising issues that don't have any consensus yet. For example, if an organization is partway through Level 2 when the standard shifts, do they finish under Rev 2 or restart under Rev 3? What happens to organizations that already certified under Rev 2 once Rev 3 becomes the baseline?

One thing is certain: Whether the November 2026 timeline resumes, is pushed down the road, or goes away altogether, the effects will ripple through the entire DIB. Contractors who paused or scaled back their compliance investments risk falling further behind if Phase II returns largely intact, and C3PAOs face their own uncertainty as their businesses now hinge on a review process whose future nobody can predict.

> "It's a lot like the five stages of grief. Plenty of organizations are still in denial about the requirements, but eventually they'll get around to acceptance."
>
> **– Fernando Machado,** Managing Principal and CISO, Cybersec Investments

In the meantime, DFARS 252.204-7012 is still firmly in place, and CMMC self-assessments and SPRS scores are still required. Companies still need robust security plans, technical controls that align with NIST SP 800-171, and clear evidence, just as they always have.

Until now, many contractors have been kicking the can down the road or otherwise ignoring the writing on the wall, but the underlying message has always been clear: Regardless of the government's enforcement mechanism, your organization should have strong, verifiable cybersecurity practices in place.

"It's a lot like the five stages of grief," Machado said. "Plenty of organizations are still in denial about the requirements, but eventually they'll get around to acceptance."

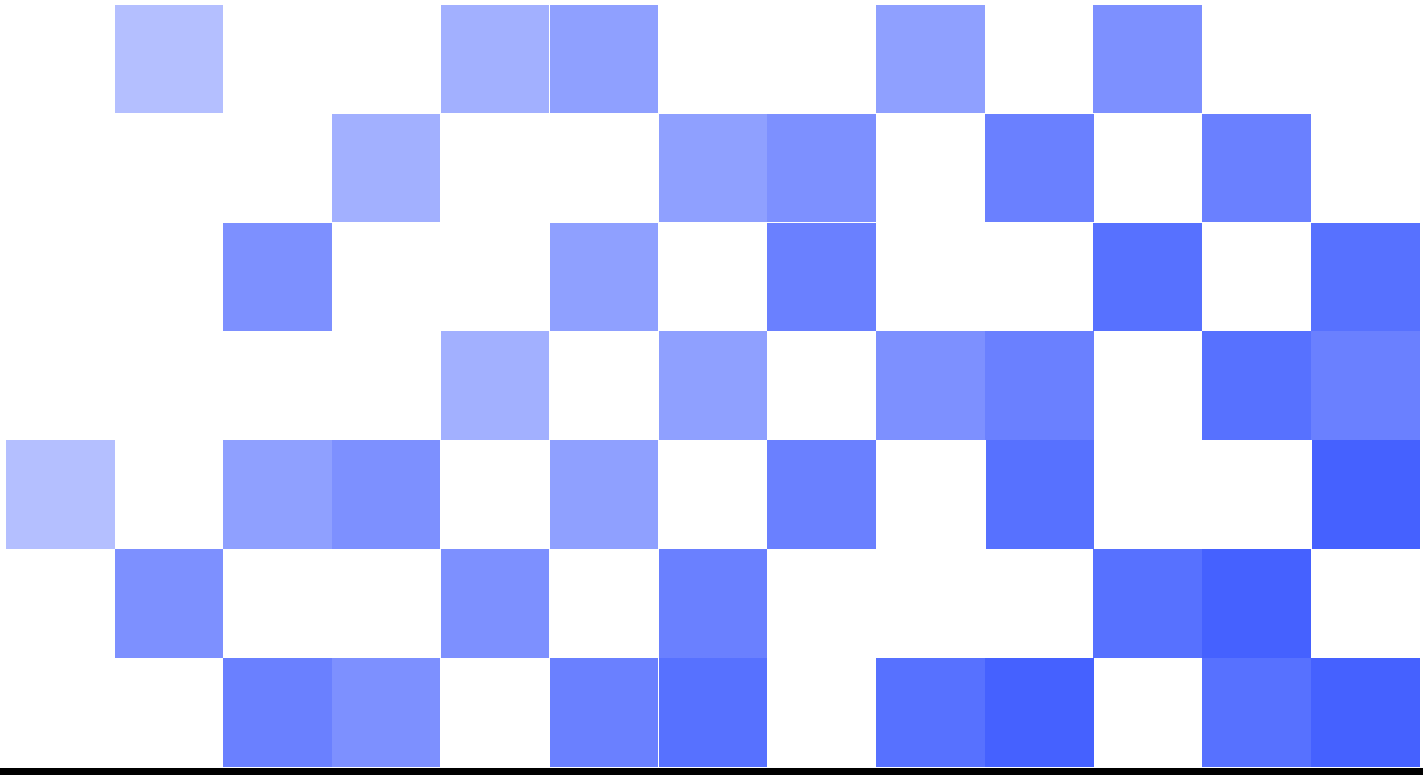
Final Recommendations: No Pause in Preparedness

Based on what we've heard from the assessors and what we're seeing across our own client base, here are our recommendations for organizations:

- **Stay on track with the NIST 800-171 requirements.** Your real risk has always been the actual cybersecurity threats that target your organization, and implementing these requirements will actively aid in your defense.
- **Don't delay moving your architecture to FedRAMP solutions.** The Phase II pause doesn't change your obligation under DFARS 7012 to use FedRAMP Moderate cloud services for handling CUI.
- **Identify a CMMC expertise strategy if you haven't already.** Will you develop the expertise in house? Will you work with a partner? No matter what, you need personnel who can understand, implement, and govern the DoD's cybersecurity requirements, regardless of what they end up being.

The case for independent assessment remains the same: An assessor confirms what a self-assessment can only assert. However, we do think it's reasonable to consider pausing your Level 2 assessment with your C3PAO while we wait for more clarity from the DoD.

The future of CMMC Phase II may be uncertain, but the DIB's mission isn't. The organizations that continue to invest in strong cybersecurity will be the ones best prepared for whatever comes next.



PARTICIPATING C3PAOS

Cybersec Investments is an Accredited Cybersecurity Maturity Model Certification (CMMC) 3rd Party Assessment Organization (C3PAO), Service-Disabled Veteran-Owned Small Business (SDVOSB), and Small Business Administration (SBA) 8(a) small business located in Melbourne, Florida. We are the first and only Accredited C3PAO on Florida's Space Coast. We have over 15 years of Department of War (DoW) cybersecurity experience. We specialize in assisting organizations in the Defense Industrial Base (DIB) meet CMMC, National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 and Defense Federal Acquisition Regulation Supplement (DFARS) compliance.

Hive Systems provides smarter cybersecurity services and assessments with their trusted experts while delivering leading cybersecurity products with Audora and Derive. Since 2018, Hive Systems has partnered with businesses to design tailored cybersecurity strategies that enhance existing investments and mitigate risks effectively. Through Hive Helps, the company extends pro bono services to qualified non-profit organizations and communities to ensure that limited resources don't stand in the way of social progress. Hive Systems is headquartered in Richmond, Virginia and serves clients and customers worldwide.

Kieri Solutions is an authorized C3PAO (CMMC Third-Party Assessment Organization), one of fewer than 100 organizations globally with the authority to conduct official CMMC Level 2 assessments and issue certifications recognized by the Department of War. The firm has been part of the CMMC ecosystem since before the program went live, supporting DIBCAC NIST 800-171 assessments and positioning itself as an early mover and recognized subject-matter authority in defense contractor compliance.

Sentinel Blue is a CMMC leader and managed security service provider bringing the power of enterprise cybersecurity tools to federal contractors of all sizes. Specializing in emerging technologies and digital transformation, Sentinel Blue offers comprehensive, scalable, end-to-end cybersecurity solutions for clients and partners within the Defense Industrial Base and other highly regulated industries. Guided by a belief that enduring security is built through thoughtful leadership, creative problem solving, and a commitment to doing the work the right way, Sentinel Blue partners with contractors and enterprises to protect sensitive information, meet regulatory requirements, and support national security missions.

Founded in 1925 and headquartered in Akron, Ohio, **Smithers** is a multinational provider of testing, consulting, information, and compliance services. With laboratories and operations in North America, Europe, and Asia, Smithers supports customers in the transportation, life science, packaging, materials, components, consumer, cannabis, dry commodities, defense, and energy industries. Smithers delivers accurate data, on time, with high touch, by integrating science, technology, and business expertise, so customers can innovate with confidence. The Quality Assessments Division of Smithers is an ANAB-accredited certification body and an authorized C3PAO. We provide services for large, medium, and small organizations in North America, Europe, and China in industrial enterprises, commercial services, and government business sectors.

WANT TO READ MORE?

Join our research mailing list to get future reports delivered to your inbox.