Redspin
A Division of Clearwater

AWARE BUT NOT PREPARED

The State of Defense Industrial Base CMMC Readiness

INTRODUCTION

AWARE BUT NOT PREPARED

The State of Defense Industrial Base CMMC Readiness

The finalization of the Cybersecurity Maturity Model Certification (CMMC) rule marks a sea change in the way the Defense Industrial Base (DIB) will engage with the United States Department of Defense (DoD) from now forward. Requiring specific proof of necessary cybersecurity measures around Federal Contract Information (FCI), and Controlled Unclassified Information (CUI), CMMC's almost five-year scoping and rule-making process was completed and in effect as of December 16, 2024. Despite the long ramp-up, is the DIB ready for the significant change that CMMC represents?

At Redspin, we wanted to find out where the ecosystem stood as CMMC moved to final rulemaking. To that end, we undertook a study of the defense supply chain members known as organizations seeking certification (OSCs), including prime contractors, subcontractors, dual-role companies acting as both primes and subs, and including some External Service Providers (ESPs) to those organizations. The findings obtained through research conducted in the Fall of 2024 are presented in this report.

This data provides clear insights into what DIB members have experienced in their CMMC certification journeys so far, and reveals the widely differing levels of maturity in adoption of CMMC-aligned practices among the breadth of companies in this critical market. It also highlights challenges they are still facing even as rule-making was finalized in December 2024. This information will help DIB members benchmark their own readiness against peer organizations, offer insights into where their ongoing efforts need to focus, and provide the DOD with a better understanding of where its critical supply chain still needs to improve its security posture.

KEY FINDINGS

There is still a CMMC readiness gap

Over half of respondents only focused on attaining a self-assessment score against defined CMMC requirements. Yet the majority of respondents intend to achieve CMMC Level 2 certification, which requires third-party assessment of 110 practices. A combined 16.3% of respondents (10.5% reporting Slightly Prepared and 5.8% “Not at All Prepared) indicate minimal or no readiness for CMMC compliance. Fifty percent (50%), including dual-role companies that function as both primes and subs, report being only Moderately, Slightly or Not at All Prepared. Thirteen percent (13%) of respondents report having not taken any preparatory action at all.

Certification cost matters, but not just for subs

The costs of CMMC preparation and certification have been a chief concern among DIB members throughout CMMC’s evolution. While many have focused on cost primarily being a burden on small subcontractors, 52% of respondents who indicated cost as the top preparation challenge were prime or dual-role organizations, and only 20% were subcontractors. Even more interesting, 35% of respondents either don’t know what they have spent to date on preparing for CMMC, or say they have invested nothing or less than 1% of their budgets.

Scoping the ‘what’ of needed cyber defenses is progressing well...

Seventy-five percent (75%) of respondents have a CMMC-required System Security Plan (SSP) in place or in process. An SSP encapsulates ‘the what’ of their needed cyber defenses. However, only 47% respondents have finalized their SSP, even though it has been a DFARS 252.204-7012 requirement for contractors handling CUI dating back to the end of 2017. Interestingly, more respondents (54%) said they have and maintain a self-assessment Supplier Performance Risk System (SPRS) score only vs. the 47% that have finalized their SSP, since the SSP is a prerequisite to submitting an SPRS score to the DOD. This is another indication of why third-party validation of CMMC by a C3PAO will help improve DIB security.

...But progress in maintaining and updating practices is lagging

While many companies have initiated compliance measures, there is a clear delay in sustaining and updating these efforts. Of those with an SSP, two-thirds update it only annually, which risks leaving them vulnerable due to outdated plans. And, only 58% of respondents have a Plan of Action & Milestones (POA&M) and even fewer maintain or update that regularly, indicating significant gaps in tracking and addressing ongoing security risks.

The supply chain remains vulnerable

CMMC requirements must be flowed down to all subcontractors at every tier if those subs process, store or transmit FCI or CUI. In our survey, only 23.5% of respondents report already having a flow-down process that is actively monitored for compliance. Besides not meeting a CMMC requirement, this gap may also contribute to the ongoing supply chain vulnerabilities CMMC intends to prevent.

Service Provider value is recognized

With over 50% of respondents having worked with an ESP, it is clear that they see value in these partnerships / relationships. Once CMMC certification is achieved, 57% of respondents say they intend to continue their current way of operating when it comes to maintaining compliance, with 89% of those being OSCs that are already using an ESP. Combined with the 18% that indicate they intend to hire an ESP for the first time, there is clear evidence that the support of service provider organizations is seen as a valuable tool in maintaining CMMC certification.

Target Certification Levels

DoD contractors have a good understanding of what level of CMMC certification they need. Level 2 compliance is the brass ring; the majority of contractors need at LEAST a Level 2 certification because they store, transmit, and/or process CUI. Even while the great majority of our respondents are from small businesses, 90% are intending to become at least CMMC Level 2 compliant. Without it, these companies will have a limited role in the ecosystem.

Despite not having tens of thousands of employees, smaller companies are still quite capable of having the mature processes, business intelligence and strategic relationships with larger and/or other small contractors that enable them to take on the prime contractor role, in addition to acting as subs. Only 5% of our respondents want to achieve Level 3 compliance, with 75% of those operating as a prime or a sub.

It is important to note that the highest certification level does not necessarily equate to the most opportunities; the required CMMC Level is determined by the type of data a contractor handles. For example, Level 1 is designated for contractors that only handle FCI data.

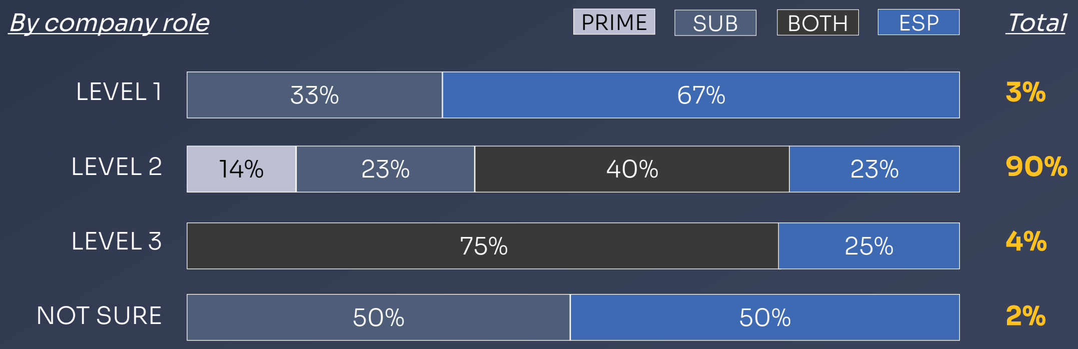
CMMC Awareness vs. Readiness

Respondents are quite aware of the DoD's emphasis on cybersecurity which is reflected through the Defense Federal Acquisition Regulations (DFARS) 252.204-7012 and codified in CMMC. Given CMMC's near five-year evolution, the great majority have had time to become familiar with it, with 81% reporting they are Very Familiar and another 17% being Somewhat Familiar.

However, familiarity does not necessarily equal preparation. Thirty percent (30%) claim they are Fully Prepared and 11.6% say they are Already Compliant – which, since CMMC rulemaking was not finalized at the time this survey was conducted, only means those few have completed the Joint Surveillance Voluntary Assessment Program (JSVAP) – a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) initiative that allows contractors with an active DoD contract to undergo a DIBCAC NIST 800-171 compliance assessment, which is required for Level 2 CMMC certification. They will now need to go through the final CMMC certification step.

FIGURE 1

What is your company's targeted level of compliance under CMMC?



KEY INSIGHT

58% of respondents are **not ready** for the CMMC rule which is now final.

The largest share (42%) of respondents feel Moderately Prepared, and 16% still have a long way to go by being Slightly Prepared or Not at All Prepared. This means that **58% of respondents are not ready for a rule that is now final and effective.**

It's also important to note that sentiment for CMMC compliance readiness does not always equate to a successful JSVAP or mock CMMC assessment. While it's encouraging to see many organizations reporting they are fully or moderately prepared, Redspin frequently encounters situations where companies believe they are ready but fall short in mock or actual certification assessments.

Preparatory Actions to Date

While just over half (55%) have worked with an ESP to start their preparations, an almost equal number (54%) have only focused on a self-assessment score. The Level 2 compliance that almost all aspire to requires certification beyond self-assessment, **creating a readiness gap.**

Among primes and dual-role companies, engagement with ESPs is higher (39%) than subs (31%), but 38% of primes and dual-role are only maintaining a self-attested Supplier Performance Risk System (SPRS) score, as are 63% of subs. This points to the potential scale of vulnerable DIB organizations as CMMC certification starts to validate the security maturity of these organizations at scale.

The 13% of respondents who have taken no action is a critical concern. At the very least, maintaining an SPRS self-assessment score has been mandatory since November 2020—meaning these companies are significantly behind and at risk of non-compliance and not properly safeguarding their CUI.

FIGURE 2

At this time, how prepared do you feel your company is to meet the requirements of your intended CMMC certification level?

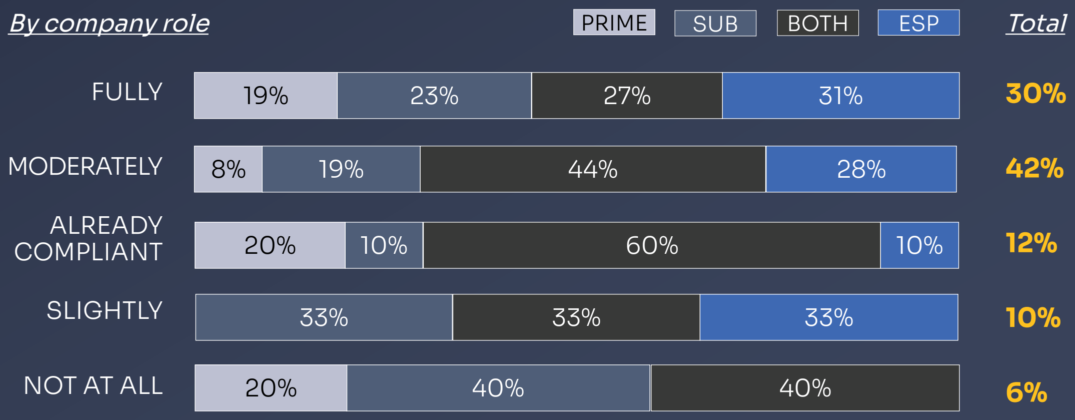


FIGURE 3

What actions has your company taken so far to prepare for CMMC certification?

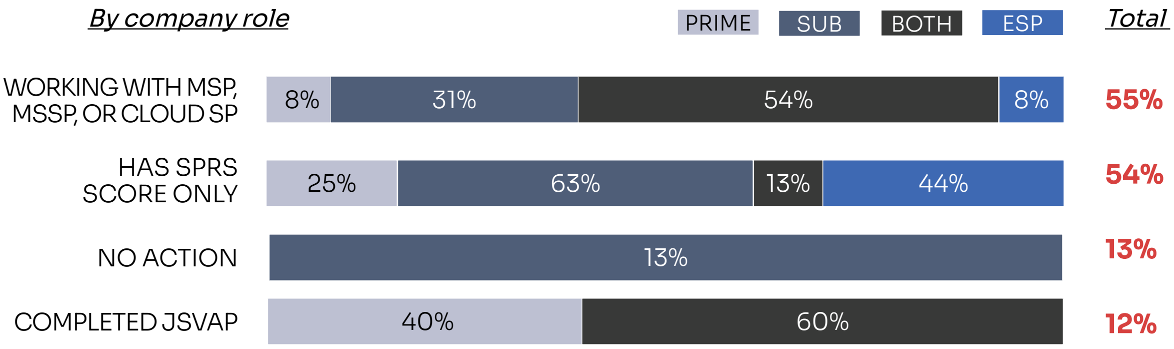
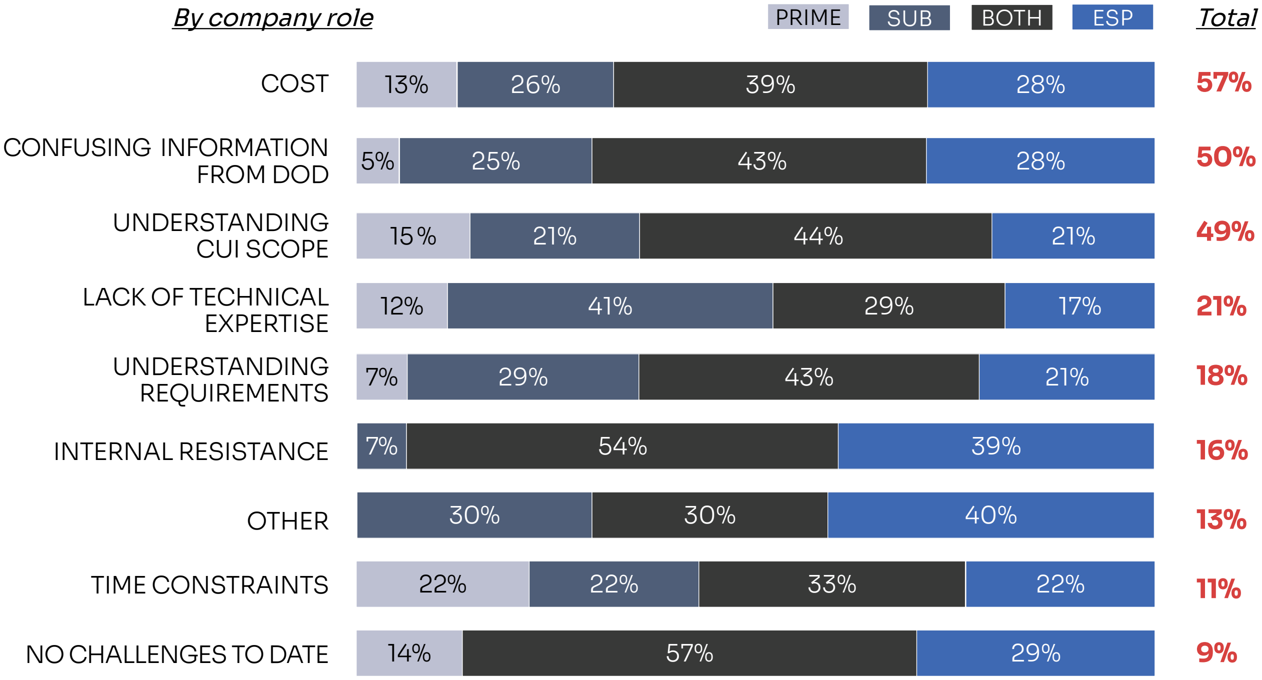


FIGURE 4

Has your company experienced challenges in preparing for CMMC?



Challenges in Preparing

There are several leading reasons why so many respondents are not yet CMMC ready. Preparation and certification costs top the list. Given CMMC's history and the accompanying uncertainty about if and when a final rule would become reality (lengthy stakeholder engagement and public comment periods, a change of presidential administrations and a global pandemic), it is understandable that half of respondents note confusion or inadequate information about CMMC. That also likely impacts the issue with understanding CUI scope boundaries.

Of those saying they have not experienced any challenges to date in their preparation, 54% act as dual-role companies, corresponding rather closely to those saying they are not fully prepared (Figure 2).

Fifty-two percent (52%) of those who indicated that costs of preparing and certifying as the top challenge

> “**CMMC certification** is required for our line of business, but doing so early gives us a **competitive advantage**.”
>
> *Matt King, Belcan, a Prime and Subcontractor*

> “**CMMC awareness doesn’t equate to readiness.** A lot of companies think they’ve got it covered, but when the assessment starts, they realize the depth and detail required exposes **gaps they didn’t see coming**. With 110 controls and 320 objectives to tackle, it’s easy to miss something important.”
>
> *Rob Teague, Director, CMMC Services, and CCA, Redspin*

were primes or dual-role organizations, and only 20% were subcontractors. While there has been ecosystem concern about hardships being imposed on smaller subcontractors, clearly the sentiment is broader.

Twenty-one percent (21%) indicated a concern about technical expertise; with 41% of respondents being subcontractors, it is clear many subs are lacking the technical expertise to handle the requirements. The percentage of others indicating a lack of technical expertise is much lower, with primes at 14% and dual-role companies at 29%.

What is even more alarming is that when asked about the challenge of internal resistance to instituting processes and procedures needed for CMMC compliance, 54% of prime and dual-role organizations had this concern, while only 7% of subcontractors found it so.

CMMC Business Value

Across all respondent types, reducing threat footprints and retaining existing contracts rank as the highest value reasons for achieving CMMC compliance, reflecting its core value. Both drivers being almost equal demonstrates that the fundamental need for CMMC is understood by the DIB community.

Among those rating “Helping us get more contracts” as Extremely or Very Important, only 25% are primes. This number rises to 76% for dual-role companies. It suggests that primes may not see this as a concern, possibly due to market confidence or viewing CMMC compliance as standard rather than a competitive edge. Similarly, for the value statement “help us win against our competitors,” 47.5% of respondents are subs, 71% are dual-role, and only 32% are primes.

Respondents don’t see compliance as very important for lowering cyber insurance premiums – indicating that insurance providers may not consider CMMC compliance in their underwriting analysis. Also, given the very high cost of cyber insurance policies, it is quite possible that smaller businesses are not even carrying this insurance.

FIGURE 5

Perceived business value of CMMC Compliance

*Ranked**

01. TO **REDUCE** OUR THREAT FOOTPRINT

02. TO HELP US **RETAIN** CONTRACTS

03. TO HELP US **GET MORE** CONTRACTS

04. TO HELP US **WIN** AGAINST COMPETITORS

05. TO HELP US **MAINTAIN/LOWER** CYBER INSURANCE PREMIUMS

* Issues rated as ‘extremely important’ by a majority of respondents

The Cost of Compliance

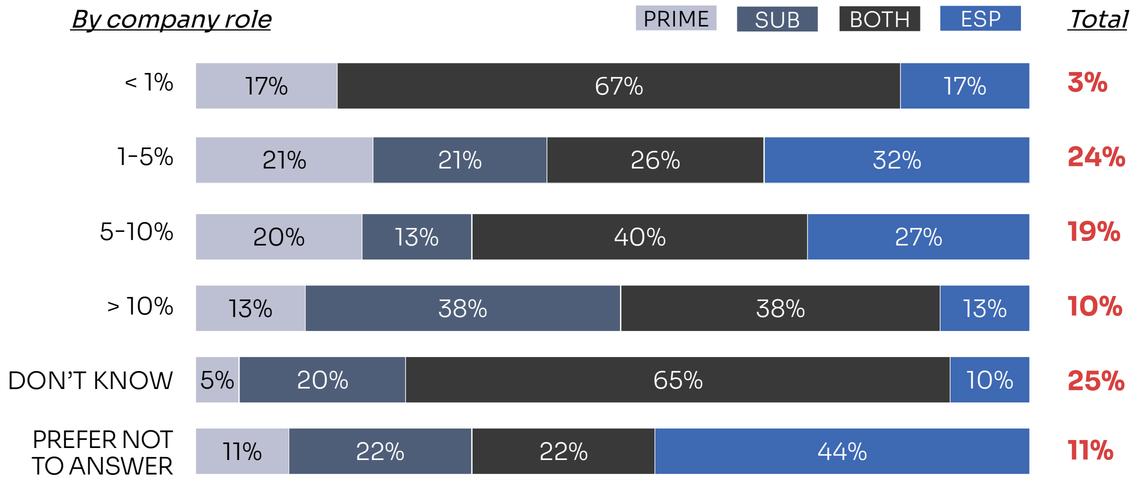
The associated cost of compliance has always been an issue for businesses preparing for CMMC. Twenty-nine percent (29%) of respondents report having invested over 5% of their budget towards this effort, however, respondents did not define whether this is from their operating budget, IR budget, or a different budget altogether.

A full 25% don't know how much they have spent, which could indicate that especially smaller businesses have a harder time tracking such costs, have not focused enough on it, or have been uncertain about exactly what to invest in, given the program's uncertain history. Sixty-five percent (65%) of those who don't know how much they've spent are dual-role companies.

In fairness, since a lot of the CMMC requirements can include modifying policies, procedures and documentation, costs can be difficult to estimate as added responsibilities would fall to existing staff at no additional expense. Still, lower investment likely ties to a lower level of preparedness. There is clearly a need for more market education and coaching on best practices for maximizing and measuring this investment.

FIGURE 6

What percent of your budget has your company invested in CMMC so far?



> "Being one of the few companies to achieve a perfect 110 in the JSVA Program, we see **a huge benefit** as being frontrunners for upcoming contract submissions due to our compliance with NIST 800-171 requirements."
>
> *Aaron Balistreri, MLT, a Prime Contractor*

Getting to Compliance

Seventy-eight percent (78%) of respondents have experience with compliance frameworks like ISO 27000, SOC 2, NIST, and HIPAA. This foundation helps them understand the compliance process and prepares them for meeting CMMC requirements.

Seventy-five percent (75%) of organizations either have a System Security Plan (SSP) in place or will soon. The SSP outlines the necessary cyber defenses and is a fundamental CMMC requirement. It details various aspects of the company's network, including maintenance, user identification, acceptable use by users, and other specifics that describe the entire network environment.

Fifty-five percent (55%) of subs have an SSP in place or in process, as do 82% of dual-role companies. It is interesting to note that only 47% respondents have finalized their SSP, as this has been a requirement for contractors handling CUI per the DFARS 252.204-7012, dating back to December 31, 2017. This is another indication of why third-party validation of CMMC by a C3PAO will help improve DIB security. Still, the good news is that 29% of respondents are actively working on getting an SSP in place, with the largest respondent group (40%) being subcontractors.

Far fewer respondents have gone as far as addressing deficiencies identified through a Plan of Action and

FIGURE 7

Has your company submitted a System Security Plan (SSP) to meet DFARS 252.204-171 requirements?

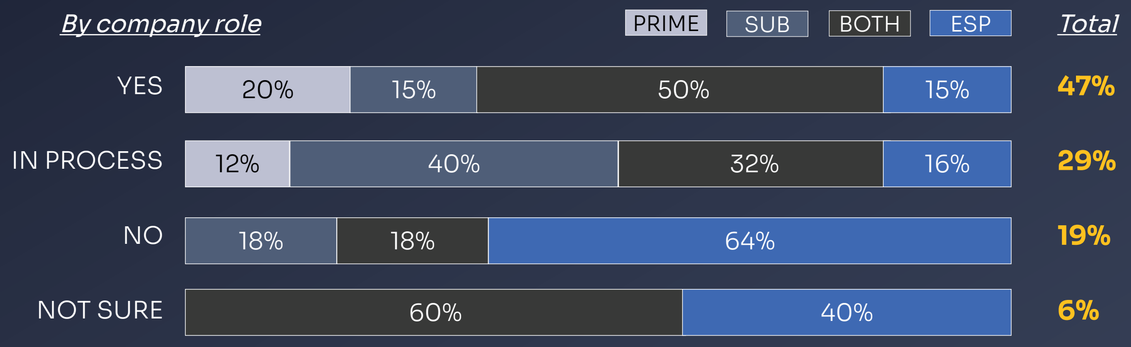
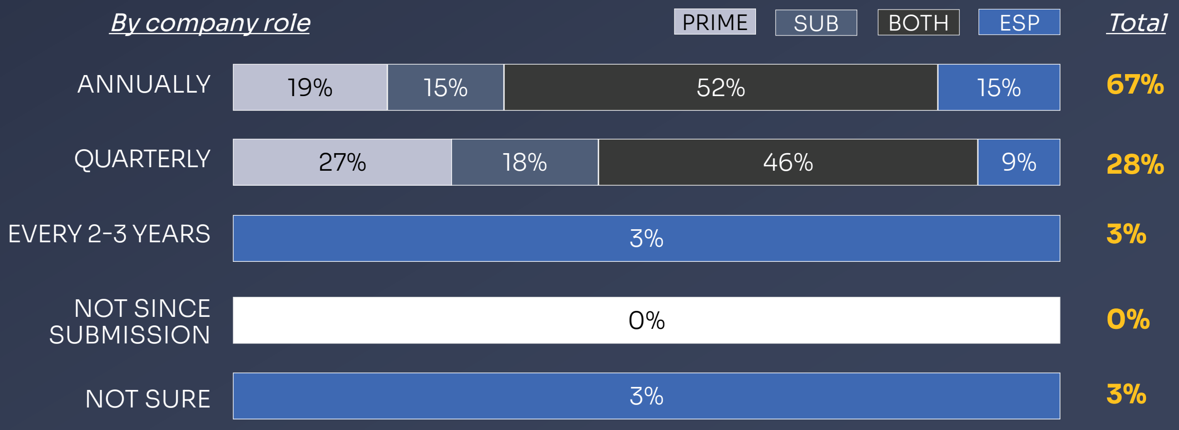


FIGURE 8

How often does your company review and update its SSP?



Milestones (POA&M), a critical step in demonstrating progress toward full compliance. A POA&M is issued when contractors fail to meet specific control requirements (under the final CMMC rule, POA&Ms can only be used for a limited number of controls), serving as a structured remediation plan that outlines steps to resolve identified gaps. Historically, the Defense Contract Management Agency (DCMA) has noted that many contractors fail to act on their POA&Ms to address identified issues. Most are off to a slow start: only 26% of respondents report having completed a POA&M, indicating they have the maturity in their security assessment, SPRS, and SSP to honestly identify what they need to address and the plan to remediate it. An additional 34% of respondents report they are working on it, reflecting the growth of an organization and their understanding of the cyclical process of managing cyber risk and remediation as the threat landscape evolves.

Still, as of now, more companies know “the what” of their cyber defenses than “the how” they will accomplish it, and many have a long way to go in addressing unimplemented security requirements and planned mitigations. Under CMMC, the use of POA&Ms is tightly controlled, requiring clear timelines and documented actions to achieve compliance, and underscoring the importance of continuous improvement and timely resolution to maintain readiness and meet contractual obligations.

Additionally, there may be some confusion about the required timing for review and update. That is because a previous DFARS requirement for a self-assessment designated the need for review and update at least once every three years. While CMMC changes this, there may well be an established contractor company belief or culture that defaults to the former requirement.

FIGURE 9

Has your company submitted a Plan of Action and Milestones (POA&M) to meet DFARS 252.204.171 requirements?

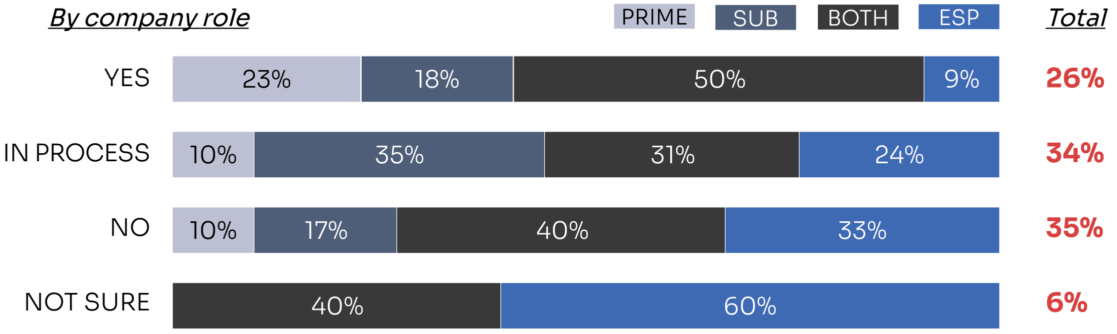


FIGURE 10

How often does your company review and update its POA&M?

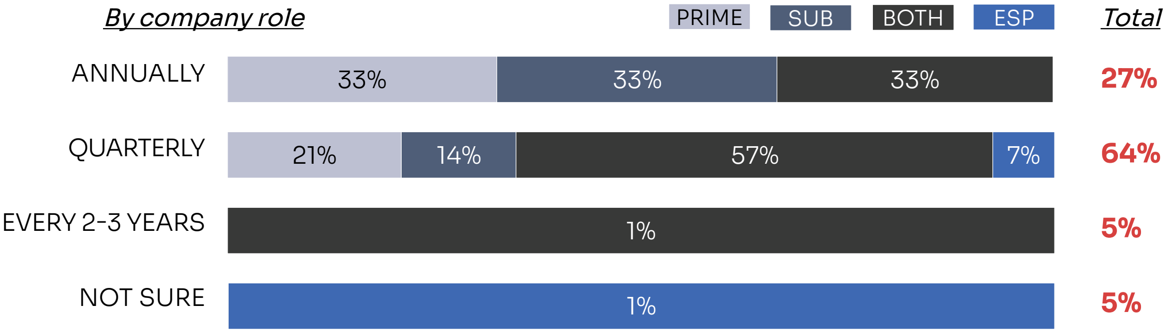
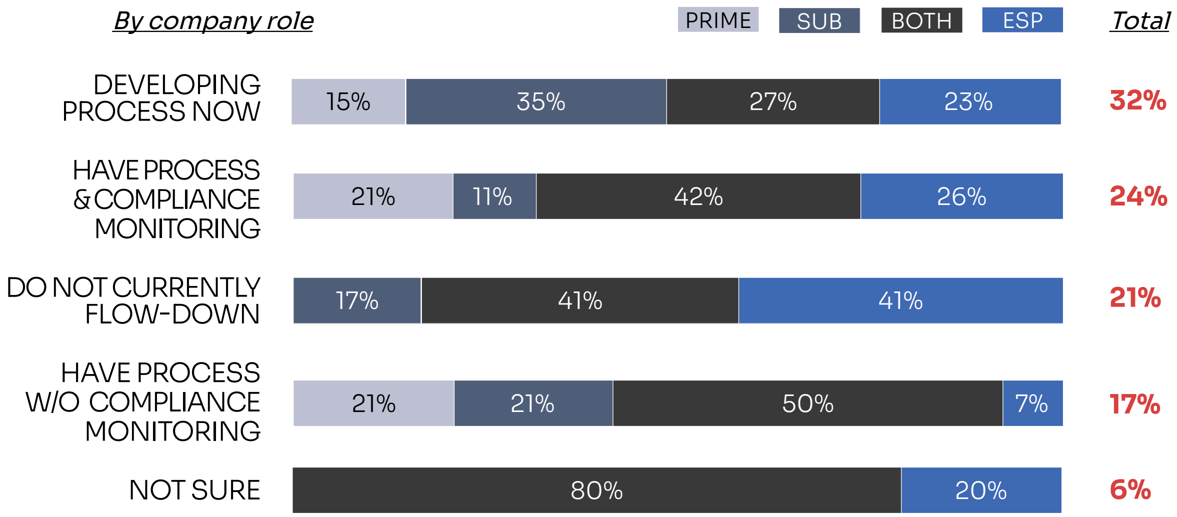


FIGURE 11

How does your company handle the flow-down of DFARS 252.204-7012 requirements?



Requirements Flow-down

Another important CMMC provision is the flow-down of cybersecurity requirements from prime contractors to their subcontractors and/or subcontractors to their own subs. All of the CMMC requirements must be flowed down to all subcontractors at every tier if those subs will be processing, storing or transmitting FCI or CUI.

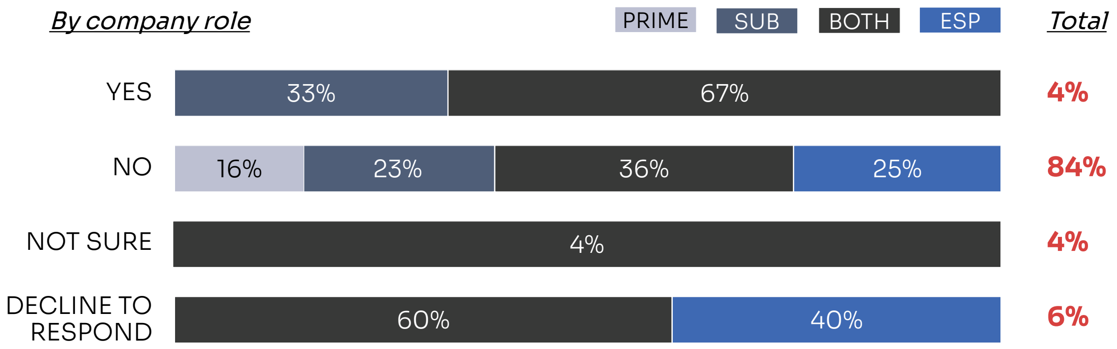
Only 23.5% of respondents in our survey have an actively monitored flow-down process. Besides lacking a mechanism to meet a CMMC requirement, this gap may also contribute to the ongoing supply chain vulnerabilities CMMC intends to prevent.

We also wanted insight into how many companies had experienced cyber incidents, given the pervasiveness of cyber threats and the known attractiveness of the defense supply chain to cyber-attackers. To this point, 86% of all respondents say they have not had a "reportable incident" as required under CMMC, 75% of which are OSCs. While it is highly unlikely that such a large percentage would not have had an incident, it could be that some companies have neglected to report what has been required under the DFARS 7012 regulation. Many organizations are reluctant to admit they have been victims of cyber-attacks unless required to do so.

> "Prime and subcontractors are now on the hook for making sure their subcontractors are not just aware of compliance requirements but are **actually meeting the appropriate CMMC levels**. These flow-down requirements mean contractors need to stay on top of their entire supply chain to avoid risks."
>
> *Dr. Thomas Graham, CISO, and CCA Redspin*

FIGURE 12

Has your company experienced any cybersecurity incidents involving CUI that required reporting under DFARS 252.204-7012?

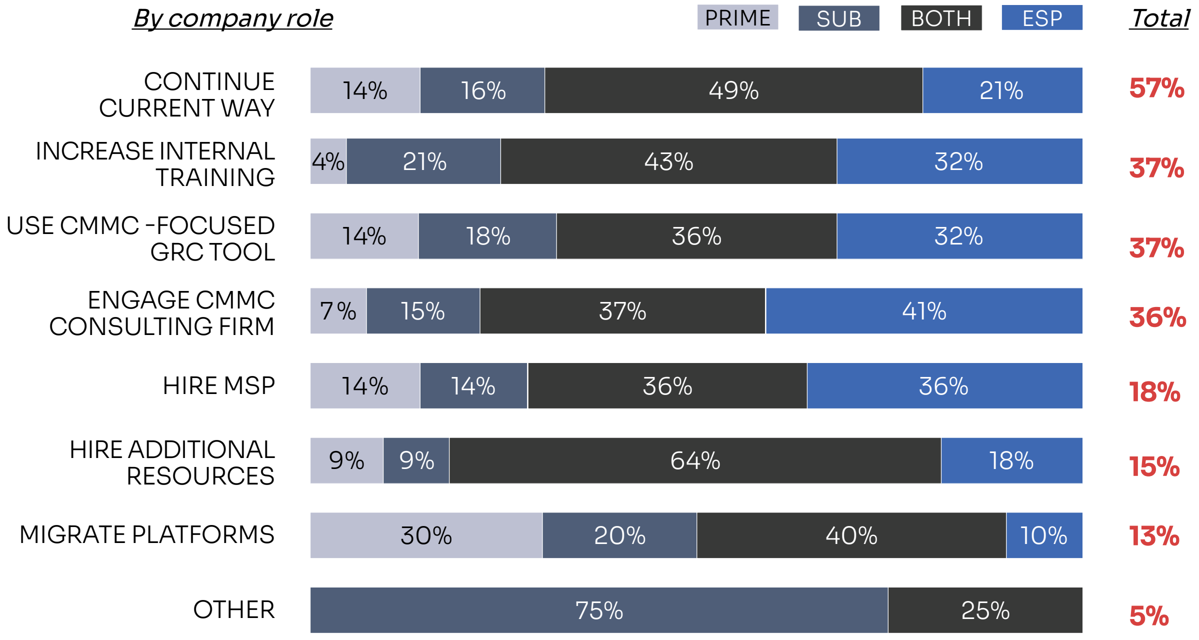


Compliance for the Long Term

Respondents plan to maintain their CMMC certification through a breadth of means. Fifty-seven percent (57%) intend to maintain the status quo among other steps, with 89% of those being OSCs that are already using an ESP. Combined with the 18% that indicate they intend to hire an ESP (not already working with one), there is clear evidence that the support of service provider organizations is seen as a valuable tool in maintaining CMMC certification.

FIGURE 13

Has your company experienced any cybersecurity incidents involving CUI that required reporting under DFARS 252.204-7012?



RECOMMENDATIONS

As CMMC moves from a requirement to a strategic necessity, the DIB must act quickly and decisively to bridge the existing readiness gaps. Below are steps organizations can take to improve their preparedness and ensure they meet CMMC requirements:

Acknowledge the Reality

Don't wait. Time is already short; you can't afford to make any mistakes that will result in rework and further delays. Failure to comply with CMMC/NIST SP 800-171 not only jeopardizes contracts but also the organization's reputation.

Leverage External Expertise

Don't navigate this journey alone. Partnering with specialists like a Certified Third-Party Assessor Organization (C3PAO) or a CMMC Registered Practitioner Organization (RPO) can significantly accelerate your compliance efforts.

Invest in Tools and Training

Designate a CMMC lead; send staff to Certified CMMC Professional (CCP) training; and ensure all employees receive cybersecurity best practices training to help avoid mistakes, increase efficiency in meeting compliance, and strengthen organizational security posture.

Start with a Gap Assessment

Begin with a comprehensive gap analysis to assess where your organization stands against CMMC requirements. Break down your findings into Fully Compliant Controls, Partially Implemented Controls, and Non-Existent Controls. Then develop a phased, structured approach to address the gaps.

Focus on Quick Wins

Start by addressing low-effort, high-impact tasks to build momentum. These quick wins will not only demonstrate progress to stakeholders but will also significantly enhance your cybersecurity posture.

Consider Migrating to an Azure GCC Cloud Environment

Microsoft's Azure Government Community Cloud (Microsoft GCC) provides a secure enclave tailored to meet CMMC and other federal compliance requirements. With Redspin as your partner, migrating to Microsoft's GCC can expedite compliance by offering pre-configured controls, streamlined data flow security, and built-in monitoring capabilities, reducing the burden on your internal IT team.

Develop a Sprint Roadmap

Take a phased, manageable approach to achieving compliance. Start by addressing urgent gaps, then proceed with tasks that require collaboration, and finally focus on creating long-term, sustainable processes for continuous compliance monitoring and improvement.

Commit to Ongoing Compliance

Establish regular internal audits, proactively update and close POA&Ms, and designate a dedicated team or role responsible for tracking updates to DoD regulations.

Recognize the Value of External Service Providers (ESPs)

These organizations offer valuable resources and can help mitigate risks associated with maintaining cybersecurity maturity. Many OSCs already using ESPs plan to continue doing so to maintain compliance. Those not using ESPs might consider hiring one to support compliance efforts.

Affirm Leadership Commitment and Organizational Support

This is critical for ensuring that CMMC compliance is prioritized and adequately resourced. Leadership must allocate sufficient budgets, clear timelines, and internal support to sustain compliance efforts across departments.

Don’t Treat the SSP as an Attestation Document

Your SSP is a living document. It should outline exactly how you address each objective. Redspin has found that those who actively work through each SSP objective tend to succeed in achieving and maintaining compliance.

For more how-tos on these and other steps that will streamline your journey to CMMC compliance, please contact Redspin.

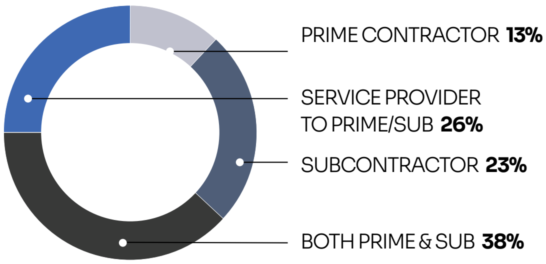
Summary

CMMC compliance is more than a regulatory necessity; it is a strategic imperative for organizations within the defense contracting ecosystem. By achieving certification, companies not only protect sensitive data and reduce cybersecurity risks but also secure their competitive standing and ensure the continuity of their business with the DoD. Organizations that proactively adopt and integrate CMMC requirements into their operations are better positioned to thrive in an increasingly security-conscious marketplace.

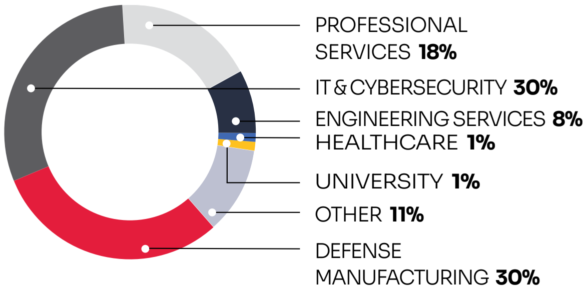
Methodology

This survey was conducted throughout September 2024. Respondents included cybersecurity and/or technical senior leaders in companies selling to the US Department of Defense. A total of 107 responses were received.

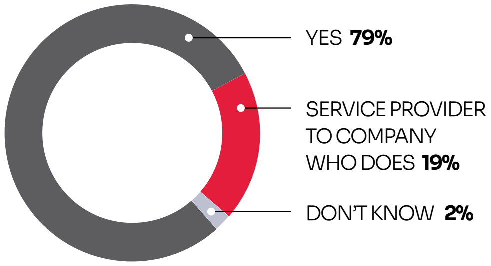
Respondents by company role



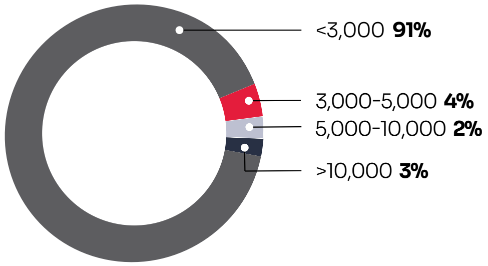
Respondents by DIB sector



Respondent companies handling CUI



Number of employees in respondent companies



About Redspin

As the first authorized CMMC Third-Party Assessment Organization (C3PAO), Redspin leads the industry in CMMC services. Our team of experts provides end-to-end support, from assessment preparation to training, to certification and beyond, ensuring Organizations are fully prepared to meet CMMC's requirements.

We understand that every organization is on its own CMMC journey, and there are business nuances, specific regulations and practices unique to different industries. Our approach is tailored to meet the needs of each unique DIB member, whatever stage of preparation and maintenance they are in.

With our DoD backgrounds and diverse experience supporting clients in highly regulated industries, we have the techniques and know-how to apply industry-specific or broad industry learnings to your environment. Our holistic managed services integrate advanced technologies and expert support to protect your organization.

Redspin is proud to be an expert coach and partner to assess, prepare, validate, and maintain your cyber defenses.

info@redspin.com | 888-907-3335 | redspin.com