2025

CYBERSECURITY, DFARS, AND CMMC READINESS

SMALL DIB CONTRACTORS SURVEY REPORT

Alluvionic®
PROJECT ASSURANCE®

Executive Summary

The key findings of this report are based upon a targeted survey of small defense industrial base (DIB) contractors which revealed critical trends related to cybersecurity maturity, DFARS compliance, and CMMC readiness.

Despite growing pressure from the Department of Defense (DoD) to secure Federal Contract Information (FCI) and Controlled Unclassified Information (CUI), many organizations remain unclear on their obligations and underprepared for compliance.

This report presents key findings from the survey and offers insight into the current posture of small contractors facing the evolving cybersecurity landscape mandated by the Cybersecurity Maturity Model Certification (CMMC) 2.0 framework.

Key Finding Areas

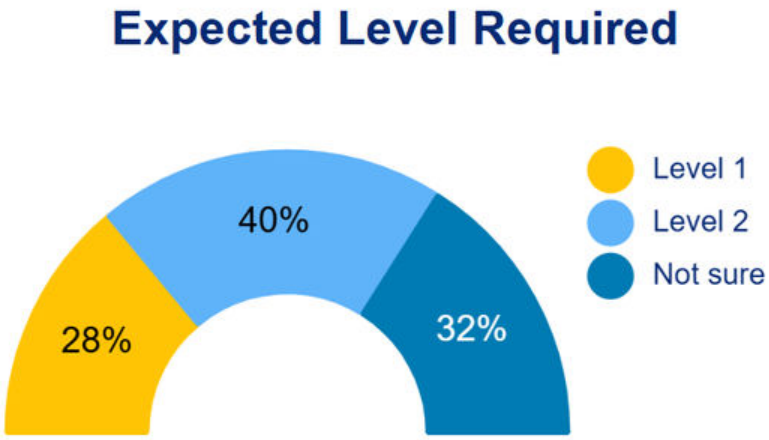
The survey identified key findings in the following areas.

Awareness | Readiness | Financial Investments | Timeline Considerations

Awareness

CMMC Confusion Remains Widespread.
Nearly one-third of surveyed contractors reported that they do not know which CMMC level applies to their business.

This uncertainty is important because the level decides if a company can do a self-assessment or needs a third-party certification, and it affects both the technical steps and policies required by the CMMC program.



56% haven't done a gap analysis against CMMC or NIST 800-171

70% haven't deployed compliant technical tools

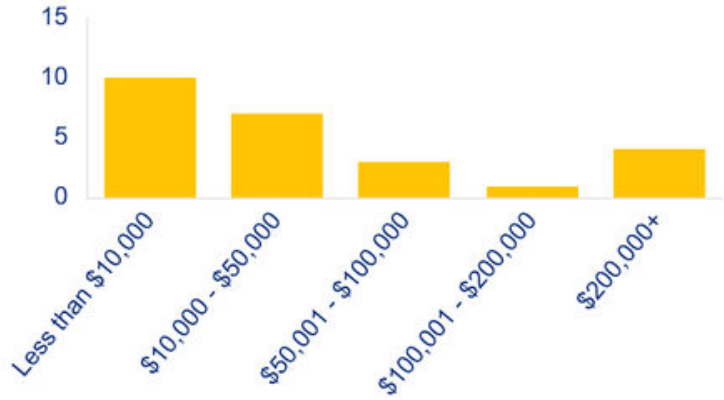
50% haven't documented key cybersecurity policies

Readiness

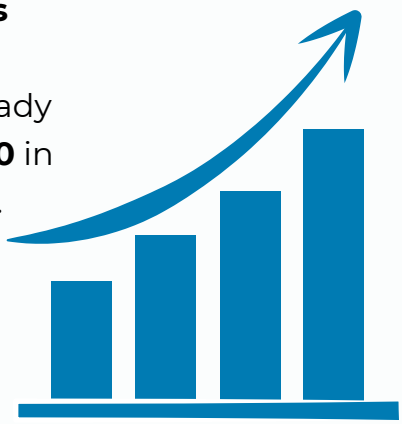
Organizations have not taken sufficient readiness steps.
While some organizations have taken early steps, most have not formally begun the compliance journey.

Financial Investments

Compliance is Expensive — And Ongoing.
These figures highlight the financial commitment required for robust cybersecurity readiness, especially at Level 2, which aligns with the 110 controls from NIST SP 800-171.



40% of contractors pursuing level 2 certification have already invested over **$100,000** in compliance efforts.



The average estimated cost to sustain level 2 compliance is over **$120,000 annually**.

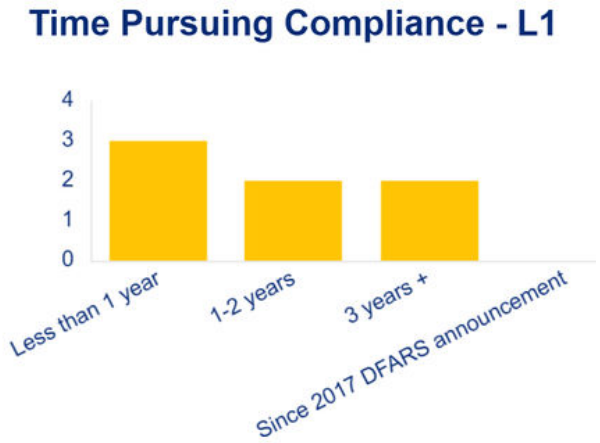
15% Reported that they've already **lost business opportunities** due to not meeting the required cybersecurity standards.

Timeline Considerations

About a third of contractors have spent over 3 years pursuing compliance. Many underestimated how staffing, resources, and planning impact timelines. With CMMC enforcement underway, delays may lead to lost contract opportunities.

Time Pursuing Compliance By Level

Level 1 is simpler, but many contractors still spend years on it.



Have spent more than 1 year preparing for CMMC and still aren't done.

While cybersecurity frameworks are often underestimated for their rigorousness, there's a light at the end of the tunnel.

42% of contractors report experiencing **peace of mind** as a result of investments made in CMMC readiness.

Additionally, another 38% have already realized **financial benefits or business development opportunities** as a result of CMMC readiness investments.

Next Steps

Where do you go from here?

The survey reveals significant gaps in CMMC readiness that carry clear business consequences. As the DoD begins phased enforcement under the CMMC Final Rule, delayed preparation may lead to lost contract opportunities, especially for contractors handling Controlled Unclassified Information (CUI), who are likely required to obtain third-party certification at Level 2.

Self-assessments alone are insufficient for many. A lack of documented policies, procedures, and evidence continues to be a top barrier. Without these, even well-equipped organizations may fail to certify. The findings point to a need for better planning, clearer scoping, and sustained investment to remain competitive in the defense supply chain.

01

Identify Your CMMC Level

Clarify whether your contracts involve FCI or CUI. This drives your required level of compliance and determines the assessment path (self-assessment vs. third-party certification).

02

Complete a Gap Assessment

Don't wait. Benchmark your current practices against the CMMC requirements using a Registered Practitioner Organization (RPO) or internal review aligned with the CMMC Assessment Guides.

03

Budget Beyond Certification

Certification is not a one-time event. Sustainment costs, such as continuous monitoring, documentation updates, and audit preparation, are a critical part of long-term compliance.

321-241-4510 Alluvionic.com info@alluvionic.com Melbourne, FL