

CMMC Preparation Study

An examination of CMMC perspectives, plans and approaches among DoD contractors



Introduction

During December 2020 and January 2021, Apptega and SecureStrux conducted the inaugural CMMC Certification Preparation Study.

Individual study participants represented **130 prime contractors and subcontractors** in the U.S. Department of Defense (DoD) **Defense Industrial Base (DIB)**. Participants included business owners, CIOs, CISOs, and other Heads of IT, Security and Compliance

Participants provided insights into their CMMC perspectives, current NIST 800-171 compliance status, approach and scope of their CMMC preparation, and cost estimates. This report examines their feedback and provides correlations that serve as benchmarks to assist all contractors in the DIB with their plans for CMMC certification. For the purpose of examining variations correlated with organization size, participants were grouped into two categories; Smaller contractors with 100 employees or less, and Larger contractors with more than 100 employees.

01: Executive Summary of Findings

- 81% of the study participants indicated that **CMMC is an important initiative** needed to protect sensitive information within the DIB. None of the participants indicated that CMMC is not an important initiative.
- In spite of agreement on the importance of CMMC, nearly one-third of the participants indicated that **CMMC will create unnecessary burdens and costs**, and compliance with NIST 800-171 is sufficient without CMMC. This perspective varied widely between larger and smaller contractors.
- Two-thirds of the participants indicated that moving quickly to demonstrate compliance with **CMMC will create a competitive advantage for their organization**.
- Nearly 50% of the participants indicated that they expect to see **business growth opportunities** linked to achieving CMMC readiness and certification.
- **Most contractors are taking a hybrid approach to preparation**, utilizing both internal personnel and consulting assistance. Very few are completely dependent on a consultant.
- Most contractors are **including their entire organization in the scope of CMMC preparation and certification**. The percentage of smaller contractors taking an all-company approach is higher than average, and most larger contractors are taking a divisional, or enclave approach.
- **Cost expectations vary widely** and, not surprisingly, are lower for smaller organizations. Unexpectedly, the projected cost of CMMC preparation and certification is not inversely correlated to the current degree of compliance with NIST 800-171.



Table of Contents

Introduction	2
01: Executive Summary of Findings	3
02: CMMC Perspectives	5
02-1: The Importance of CMMC	6
02-2: Is CMMC an Unnecessary Burden?	7
02-3: CMMC & Competitive Advantages in the DIB Supply Chain	8
02-4: CMMC & Business Growth Opportunities	9
03: Certification Levels, Scope & Approaches	10
03-1: Planned CMMC Certification Levels	11
03-2: Scope of CMMC Preparation & Certification	12
03-3: Approaches	13
04: Compliance with NIST 800-171	14
05: Cost Expectations	16
05-1: Cost Variability & Organization Size	18
05-2: Cost Variability & Degree of Compliance with NIST 800-171	18
05-3: Cost Variability & Approach to CMMC Preparation & Certification	19
05-4: Cost Variability & Certification Levels	19
06: CUI, FCI, CTI, & ECI	20
07: Participant Demographics	22
07-1: Organization Types	23
07-2: Organization Sizes	23
08: Conclusion	24
09: About the Study Sponsors	24
Apptega	24
SecureStrux	24

02: CMMC Perspectives



02-1: The Importance of CMMC

More than four out of five study participants believe CMMC is an important initiative needed to protect sensitive information within the DIB.

The results of our first study question focused on CMMC perspectives are encouraging and seem to indicate a strong alignment between the priorities of contractors in the DIB and those of the DoD.

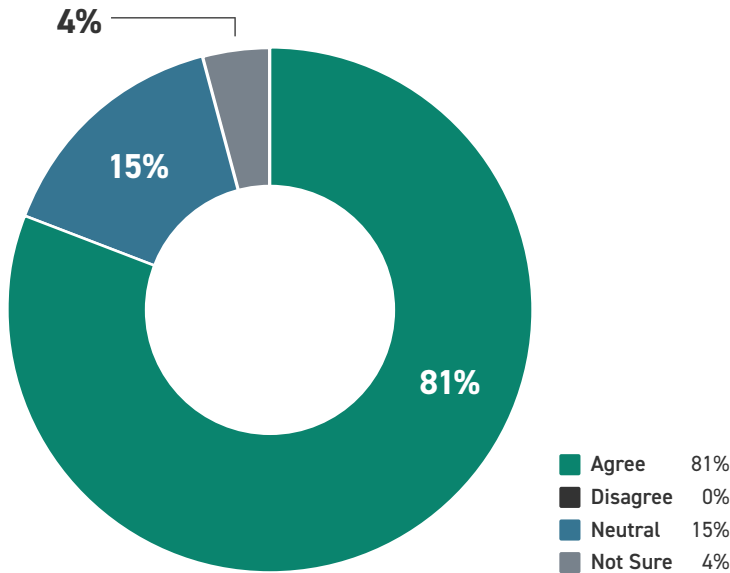
Regarding the need for CMMC to ensure protection of sensitive data within the DIB, 81% of study participants indicated that CMMC is an important initiative. Further indicating strong alignment,

None of the participants indicated that CMMC is not an important initiative. 15% are neutral on the importance of CMC and 4% are not sure.

These results are consistent regardless of the size of the organization and regardless of the organization type - prime contractor (prime) or subcontractor (sub).

SURVEY QUESTION

CMMC is an important initiative, needed to protect sensitive information within the DIB



INSIGHTS

81% of study participants indicated that CMMC is an **important initiative**

19% are **neutral or not sure** of CMC importance

0% of the study participants indicated that CMMC is **not important**

02-2: Is CMMC an Unnecessary Burden?

Nearly one-third of the participants indicated that CMMC will create unnecessary burdens.

In contrast to the results of our question on the importance of CMMC, 30% of the study participants agreed that CMMC will create unnecessary burdens and costs, and compliance with NIST 800-171 is sufficient without CMMC. Perhaps they agree that additional protections are needed but feel that certain attributes of CMMC are overly stringent.

Note that CMMC is evolving rapidly and this study was conducted before the recent announcement of possible reciprocity later this year between the CMMC program and the Federal Risk and Authorization Management Program (FedRAMP). Our next study will examine this in more detail.

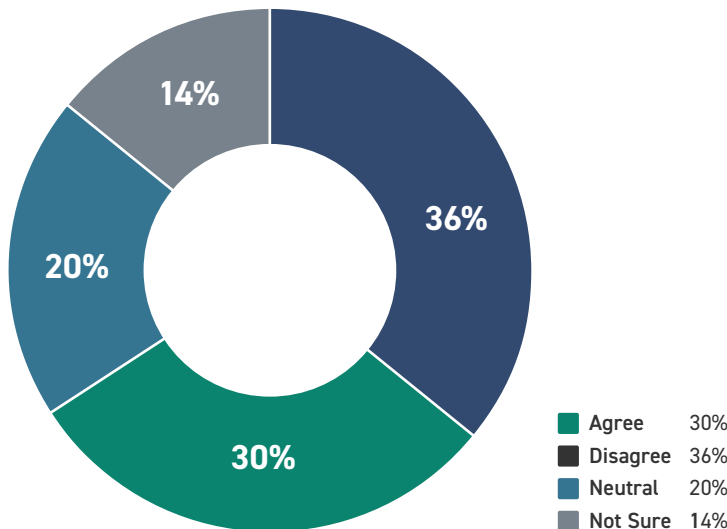
36% of participants indicated that CMMC does not create unnecessary burdens and costs. 20% are neutral and 14% are not sure.

Interestingly, these results vary widely based on company size. Only 25% of smaller organizations indicated that CMMC will create unnecessary burdens and costs, but 42% of larger organizations indicate the same.

This disparity and other factors including NIST 800-171 compliance and cost expectations examined later in the report may indicate that smaller organizations are underestimating the cost and complexity of CMMC preparation and certification.

SURVEY QUESTION

CMMC will create unnecessary burdens and costs; Compliance with NIST 800-171 is sufficient



INSIGHTS

25% of smaller organizations indicated that CMMC will create unnecessary burdens and costs

42% of larger organizations indicated the same

02-3: CMMC & Competitive Advantages in the DIB Supply Chain

More than two-thirds of the participants indicated that moving quickly to demonstrate compliance with CMMC will create a competitive advantage in the DIB supply chain.

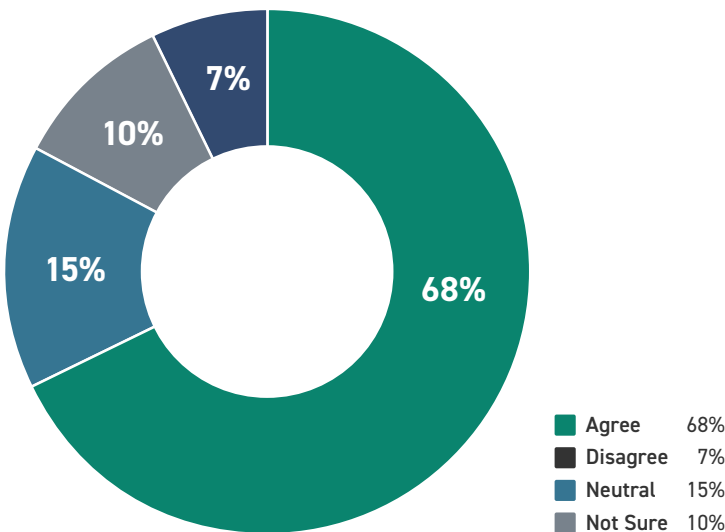
Even though nearly one-third of study participants feel that CMMC will create unnecessary burdens and costs, 68% indicated that moving quickly to demonstrate CMMC compliance is valuable and will create competitive advantages when competing for contracts in the DIB supply chain.

Only 7% of participants indicated that CMMC compliance would not create competitive advantages. 15% are neutral and 10% are not sure.

These results are consistent regardless of the size of the organization and regardless of the organization type - prime or sub.

SURVEY QUESTION

Moving quickly to demonstrate compliance with CMMC will create a competitive advantage for us in the DIB supply chain



INSIGHTS

68% indicated that moving quickly to demonstrate CMMC compliance **will create competitive advantages**

7% indicated that CMMC compliance **will not create competitive advantages**

02-4: CMMC & Business Growth Opportunities

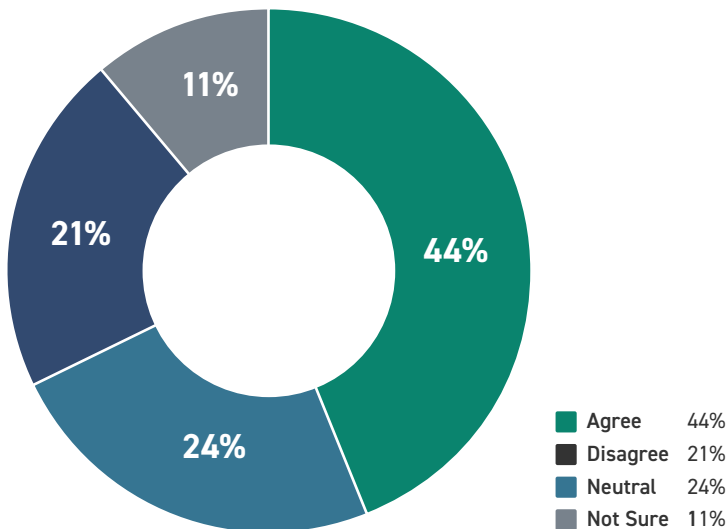
Nearly half of the participants indicated that they expect to see business growth opportunities linked to achieving CMMC readiness and certification.

In line with the feedback on competitive advantages, 44% of the participants indicated that they expect to see business growth opportunities from CMMC readiness and certification. 21% do not expect to see business growth opportunities, 24% are neutral, and 11% are not sure.

These results are consistent regardless of the size of the organization and regardless of the organization type - prime or sub.

SURVEY QUESTION

We expect to see business growth opportunities linked to achieving CMMC readiness and certification

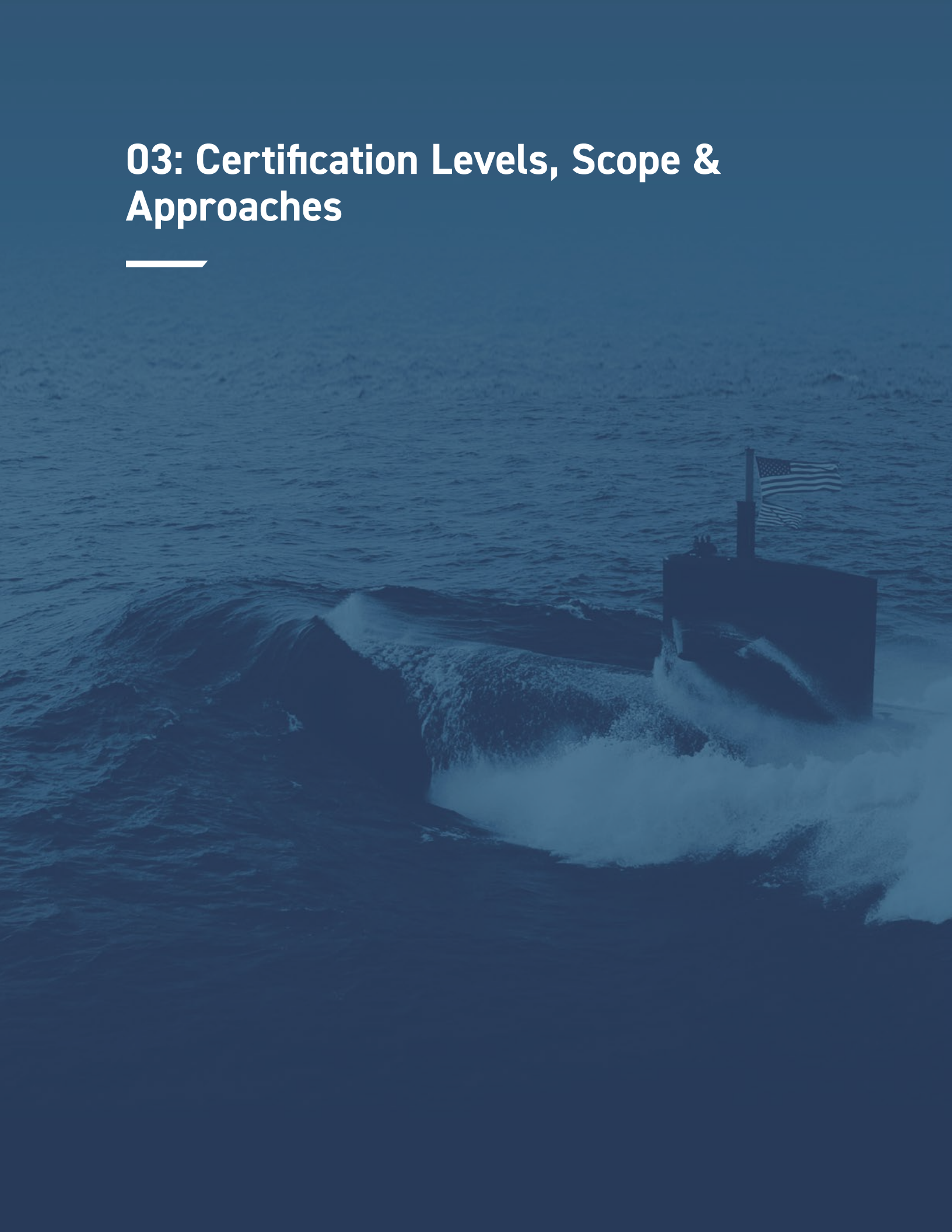


INSIGHTS

44% of the participants indicated they **expect to see business growth opportunities**

35% of the participants indicated they are **neutral or not sure**

03: Certification Levels, Scope & Approaches



03-1: Planned CMMC Certification Levels

More than three-quarters of the study participants are planning or preparing for certification at CMMC Level 3.

86% of study participants indicated that they are pursuing certification at only one level. 14% indicated plans for certification at two or more levels. Interestingly, this ratio is consistent for smaller and larger organizations.

Of those organizations planning for certification at Levels 1 or 2, only one-third are planning for certification only at Levels 1 or 2. 67% are also planning for certification at Levels 3, 4 or 5.

Although the CMMC-AB estimates that the majority of contractors in the DIB will only require certification at Level 1, 77% of the study participants indicate that they will require certification at least at Level 3, and 83% at Levels 3, 4 and 5 combined.

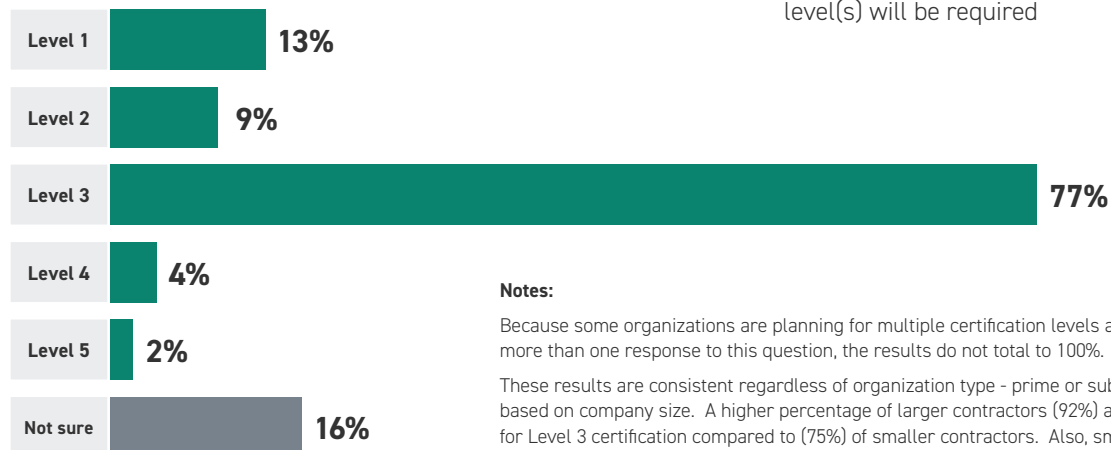
This notable difference between the CMMC-AB estimate and the study findings may be due to several factors impacting the breadth of the study:

- Difficulty in identifying and inviting smaller subcontractors that are multiple layers down in the DIB supply chain,
- Relatively small sample size of participants in the study,
- Higher degrees of interest in the study may be exhibited by contractors with known access to CUI, requiring certification at Levels 3, 4 or 5.

Interestingly, 16% of the study participants indicated that they do not yet know which certification level(s) will be required.

SURVEY QUESTION

Planned CMMC Certification Levels



INSIGHTS

16% of the study participants indicated that they **do not yet know** which certification level(s) will be required

Notes:

Because some organizations are planning for multiple certification levels and selected more than one response to this question, the results do not total to 100%.

These results are consistent regardless of organization type - prime or sub - but vary based on company size. A higher percentage of larger contractors (92%) are preparing for Level 3 certification compared to (75%) of smaller contractors. Also, smaller contractors are slightly more weighted to Levels 4 & 5 (9%) compared to only (4%) of larger contractors.

03-2: Scope of CMMC Preparation & Certification

More than two-thirds of the study participants plan to include their entire organization in the scope of CMMC preparation and certification.

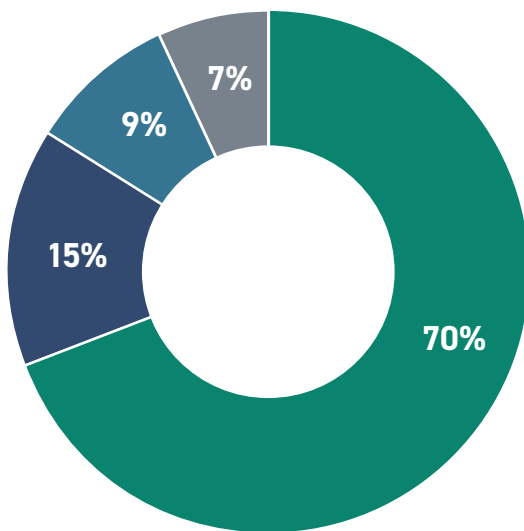
70% of contractors are including their entire organization in the scope of CMMC preparation and certification. Not surprisingly, this all-company approach varies widely from smaller organizations to larger organizations.

Among smaller organizations, 73% plan to take an all-company approach, but for very large organizations (more than 1,000 employees), only 29% are doing the same.

Most of these very large organizations, 71%, are taking a divisional or enclave approach to CMMC preparation and certification. In the survey comments, this was cited as a means to reduce the disruption, effort, and cost of the certification.

SURVEY QUESTION

Which best describes the scope of your CMMC Certification?



INSIGHTS

73% of **smaller organizations** plan to take an all-company approach to CMMC certification

71% of **larger organizations** are taking a divisional or enclave approach to CMMC certification

03-3: Approaches

Most contractors are using a hybrid approach to preparation, utilizing both internal personnel and consulting assistance. Very few are completely dependent on a consultant.

55% of survey participants are taking a hybrid approach to CMMC, utilizing both internal personnel and consulting assistance. 43% are taking a DIY approach, managing the entire preparation process internally, while only 13% are entirely dependent on a consultant to manage the process.

These results are consistent regardless of the size of the organization, with one notable exception – none of the larger contractors represented in the study are entirely dependent on a consultant.

SURVEY QUESTION

Which best describes the scope of your CMMC Certification?

INSIGHTS

55% of survey participants are taking a hybrid approach to CMMC



- **Hybrid:** DIY and RPO or other consultant
- **DIY:** Managing preparation entirely in-house
- **Mostly Outsourced:** To an RPO or other consultant
- **Not sure**

Notes:

Some organizations are taking a divisional or enclave approach with multiple projects for CMMC preparation. These organizations taking different approaches to separate projects selected more than one response to this question. Because of this, the results do not total to 100%.

04: Compliance with NIST 800-171



04: Compliance with NIST 800-171

Most of the participating organizations are more than 80% compliant with NIST 800-171.

Study participants were asked to rate their current degree of compliance with NIST 800-171, in 10% increments between 0-100%.

When comparing the ratings for smaller and larger organizations, the larger companies exhibited a higher degree of compliance:

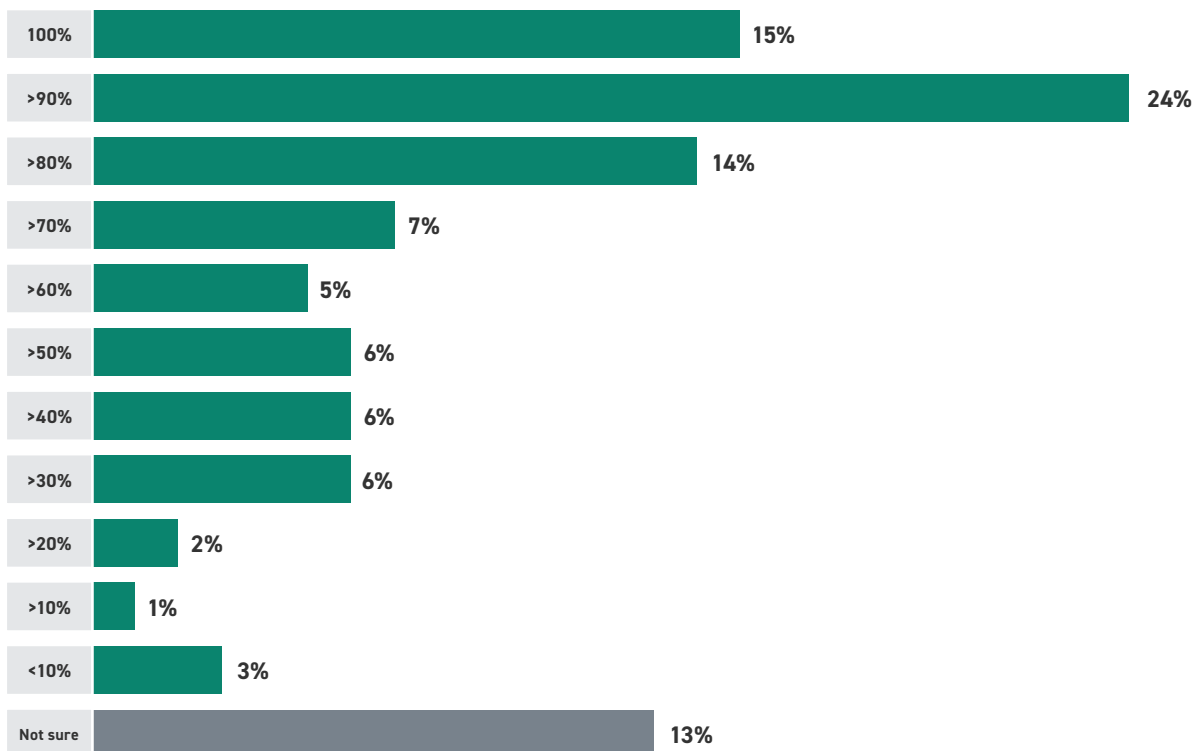
INSIGHTS

- 52% are above 80% compliant
- 18% are below 50% compliant
- 13% are unsure

DEGREE OF COMPLIANCE	SMALLER	LARGER
> 80%	45%	75%
< 50%	24%	8%
Not sure	16%	4%

SURVEY QUESTION

Which best describes your current compliance with NIST 800-171?



05: Cost Expectations



05: Cost Expectations

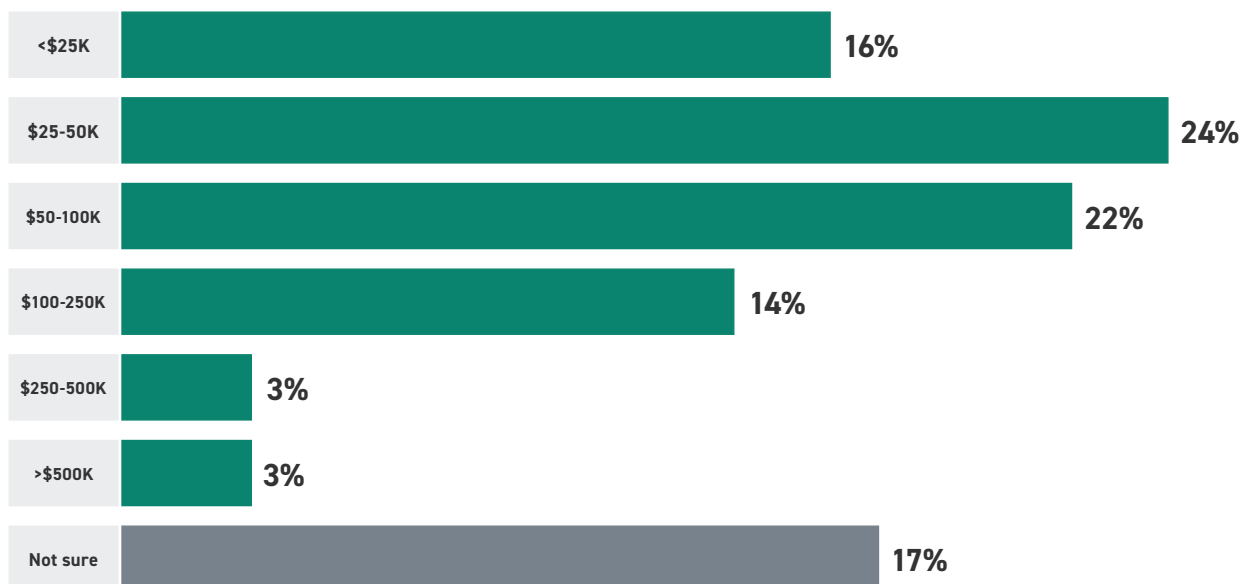
The average estimated cost for CMMC preparation and certification exceeds \$100k but this varies widely based on organization size, approach to CMMC, certification level, and degree of compliance with NIST 800-171.

INSIGHTS

\$117,000 is the **average estimated cost** for CMMC preparation and certification for all study participants

SURVEY QUESTION

Cost estimates for CMMC preparation and certification



Notes:

The midpoint of each cost range was used for calculating the averages. For "Less than \$25k", \$12,500 was used. For "Greater than \$500k", \$1,000,000 was used.

05-1: Cost Variability & Organization Size

Not surprisingly, the average cost estimates were below the average for smaller organizations and above the average for larger organizations:

ORGANIZATION SIZE	COST ESTIMATE
Smaller (less than 100 employees)	\$78,000
Larger (100 employees or more)	\$228,000

05-2: Cost Variability & Degree of Compliance with NIST 800-171

Cost estimates seem to vary based on the degree of compliance with NIST 800-171, but not as expected:

With the expectation that most contractors are using their compliance with NIST 800-171 as the starting point for CMMC preparation, this correlation between NIST compliance and CMMC cost estimates is surprising. We expected to see lower cost estimates from the organizations with the highest degree of compliance with NIST.

However, these cost variances are also impacted by organization size. In Section 04, we noted that

larger organizations exhibit a higher degree of Compliance with NIST 800-171 and in section 05-1, we found that cost estimates for larger organizations are significantly higher than the average. Another possible explanation for this inverse correlation is that many smaller contractors lack experience with NIST 800-171 and may be underestimating the cost of CMMC preparation and certification.

COMPLIANCE	COST ESTIMATE
Greater than 80%	\$164,000
51% - 80%	\$71,000
0% - 50%	\$66,000

05-3: Cost Variability & Approach to CMMC Preparation & Certification

Cost estimates also vary widely based on the approach taken to CMMC preparation and certification:

APPROACH	COST ESTIMATE
DIY - managing preparation entirely in-house	\$160,000
Hybrid Approach - utilizing both internal personnel and consulting assistance	\$78,000

Notes:

Due to the low number of organizations indicating they are entirely dependent on a consultant, cost estimates were not analyzed for this approach.

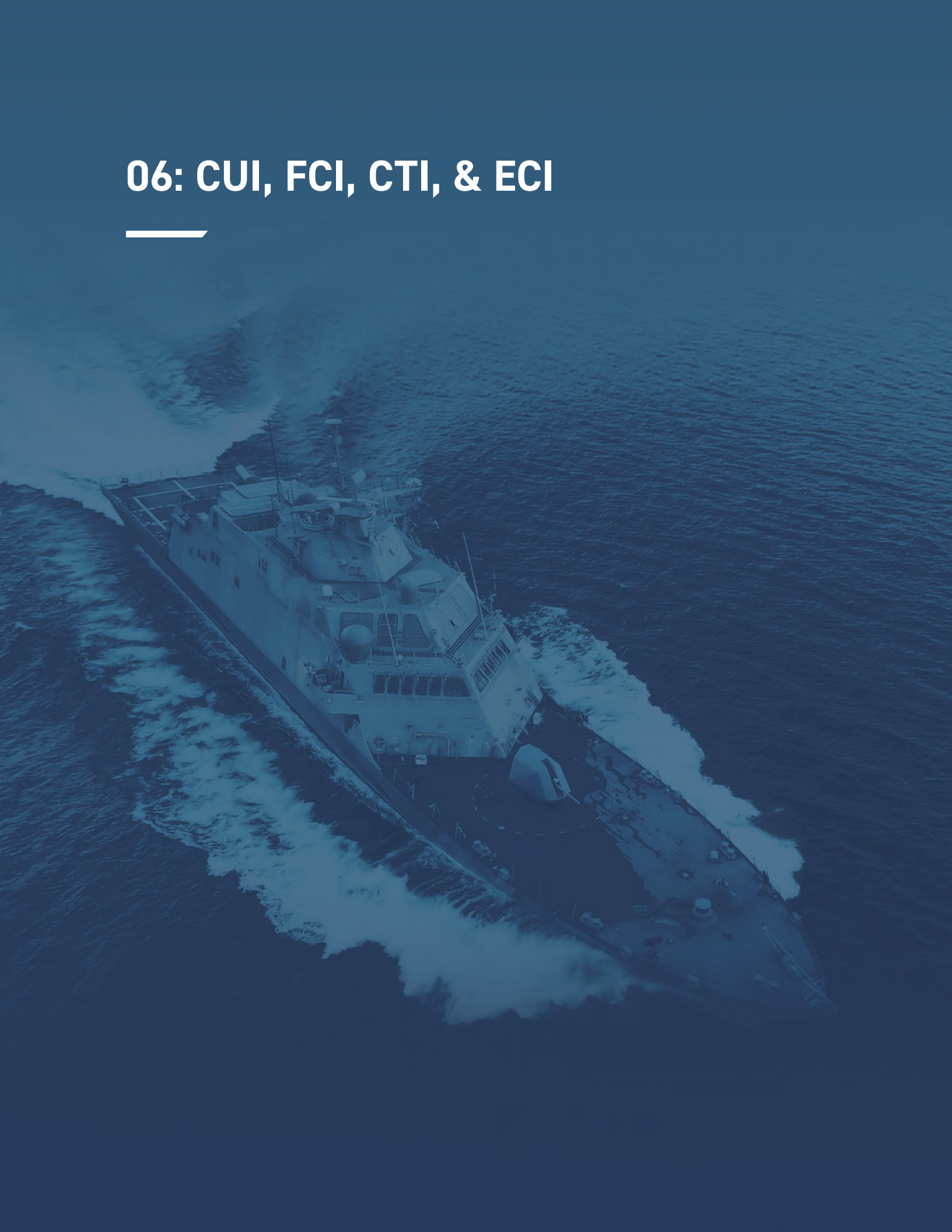
05-4: Cost Variability & Certification Levels

Cost estimates seem to vary based on CMMC certification levels, but not as expected:

With the expectation that certification at lower levels should be easier and less costly, this variability is surprising. We expected to see lower cost estimates from the organizations preparing for certification at Levels 1 & 2. Once again, company size is also impacting these cost estimates. In Section 03-1 we observed that a higher percentage of larger contractors (92%) are preparing for Level 3 certification compared to (75%) of smaller contractors. Also, smaller contractors are slightly more weighted to Levels 4 & 5 (9%) compared to only (4%) of larger contractors.

CERTIFICATION LEVEL	COST ESTIMATE
Levels 1 & 2	\$93,000
Level 3	\$128,000
Levels 4 & 5	\$70,000

06: CUI, FCI, CTI, & ECI



06: CUI, FCI, CTI, & ECI

The majority of organizations represented by study participants are handling or plan to handle Controlled Unclassified Information (CUI) and other types of sensitive information.

These results exhibited several notable variations between larger contractors and smaller contractors:

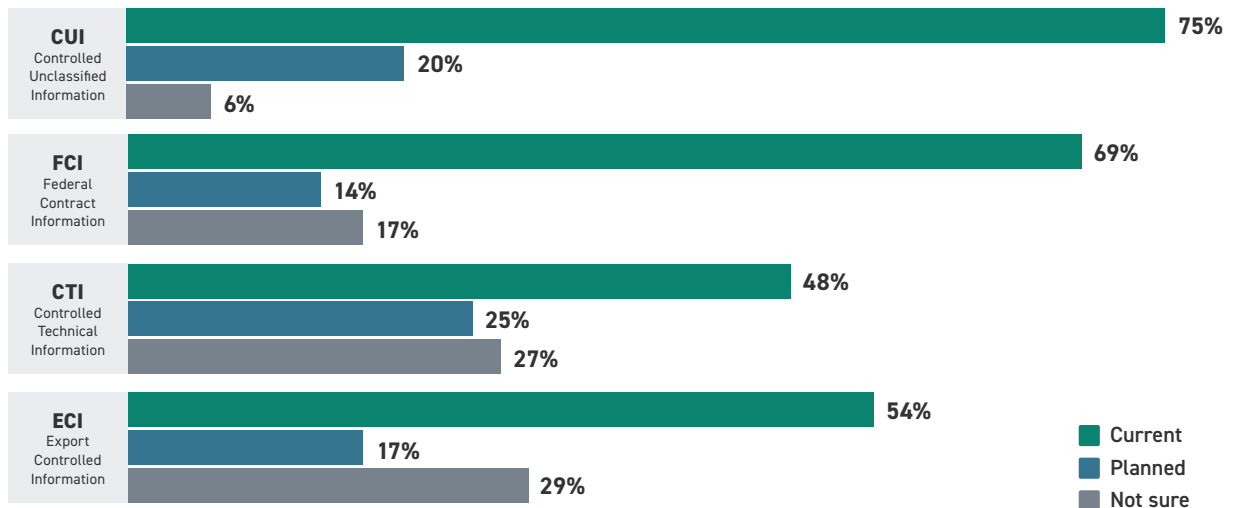
- 20% of participants from smaller contractors are not sure if they are handling FCI.
- 31% of participants from smaller contractors are not sure if they are handling CTI. This compares to only 11% of participants from larger contractors.
- 33% of participants from smaller contractors are not sure if they are handling ECI. This compares to only 17% of participants from larger contractors.

Organizations currently handling or planning to handle sensitive information are broken down as follows:

TYPES	ALL	SMALLER	LARGER
CUI	95%	94%	100%
FCI	83%	80%	100%
CTI	73%	69%	89%
ECI	71%	67%	83%

SURVEY QUESTION

Which of the following does your organization handle?

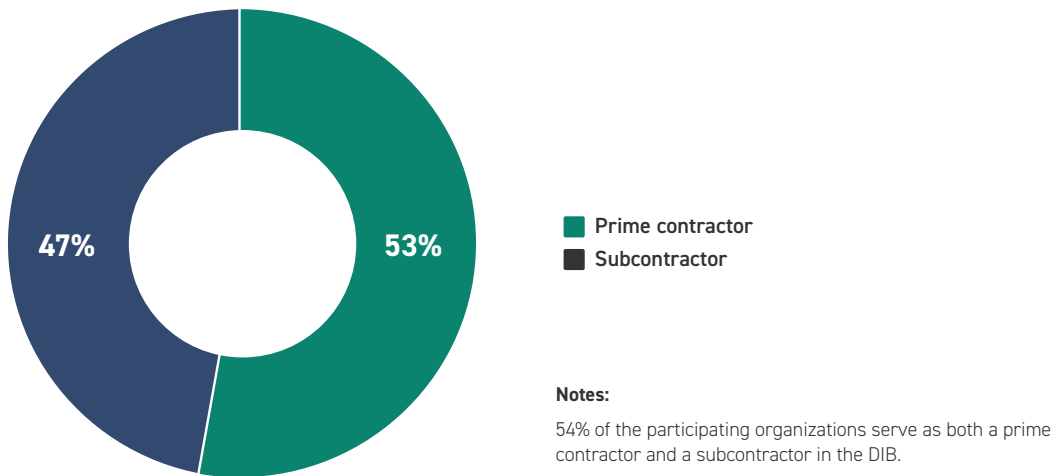


07: Participant Demographics



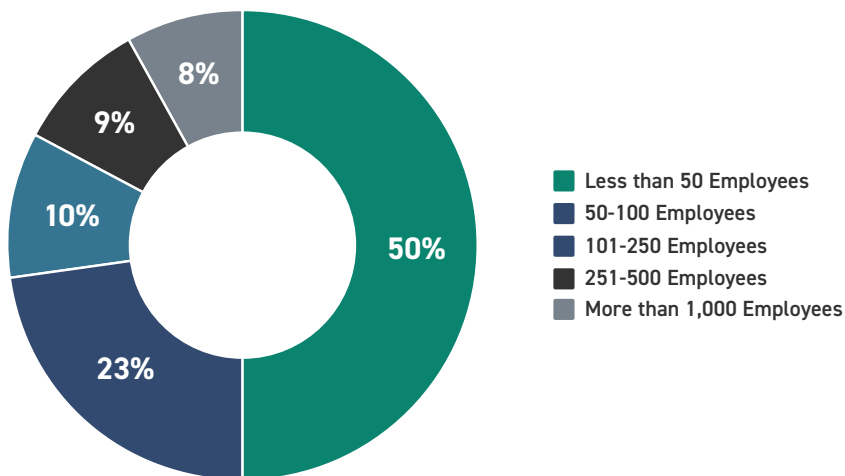
07-1: Organization Types

Participation in the study was almost evenly split between prime contractors and subcontractors.



07-2: Organization Sizes

Half of the study participants represent organizations with fewer than 50 employees.



08: Conclusion

It is clear from the results of the study that CMMC will have a significant impact on DIB budgeting and planning for certification.

It is also clear that the DIB (81%) agrees with the need to protect sensitive information and CMMC is expected to help achieve those goals. In contrast, 30% of the study participants indicated that CMMC will create unnecessary burdens and costs. Perhaps they agree that additional protections are needed but feel that certain attributes of CMMC are overly stringent.

Heading toward the goal of CMMC compliance, it is encouraging to see that 52% of participating organizations are already at least 80% compliant with NIST SP 800-171.

The results of the study also show that organizations are looking at CMMC certification as a growth opportunity and expect to gain competitive advantages in the DIB supply chain by moving quickly to demonstrate CMMC compliance.

09: About the Study Sponsors



As cyber-threats and regulatory mandates continue to expand; organizations are challenged by the difficulties of implementing effective cybersecurity and compliance programs. With Apptega, organizations of all sizes, including Fortune 500 enterprises and Managed Security Service Providers (MSSPs), are meeting the challenges of cybersecurity and compliance. Apptega is at the intersection of simple user experiences and patent-pending technology, providing an innovative platform paired with industry frameworks used to build, manage and report great cybersecurity.

www.apptega.com



As a cybersecurity firm with deep roots in the DoD cybersecurity community, we provide specialized services in the areas of compliance, vulnerability management, cybersecurity strategies, and engineering solutions. Since 2008, we've partnered with hundreds of organizations within and outside the DoD to understand and proactively manage their risk. Our deep knowledge of the defense industry allows us to seamlessly translate best practices to our defense contractor, commercial, manufacturing, and air & space clients.

www.securestrux.com