imagine IT

The Q1 2025 State of Cybersecurity

imit.com

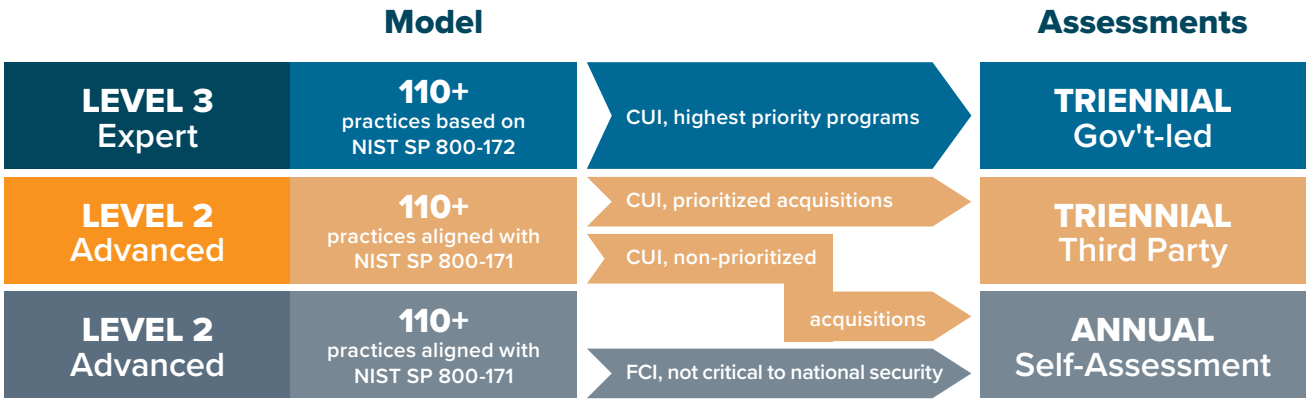
CMMC V2 Final Rule Highlights for DoD Contractors that Work with MSP's

The final rule is here:
https://www.federalregister.gov/documents/2024/10/15/2024-22905/cybersecurity-maturity-model-certification-cmmc-program

It is a long document, but if you search for "msp" you will get to the applicable section.

I have spent a lot of time reviewing the Final Rule document and engaging with peers. In early December I also engaged with a CMMC auditor (C3PAO).

Bottom line, the DoD listened to the supply chain community and relaxed the rules for MSP's. This is very good news.



Before I get to the highlights, here are some Definitions...

CMMC = Cybersecurity Maturity Model Certification.
OSA = Org Seeking Assessment (your org). Must obtain a CMMC certification (likely L2).
CUI = Controlled Unclassified Information (the DoD data your org needs to protect).
CSP = Cloud Service Provider (generally those that store CUI). Must be FedRAMP Moderate certified.
ESP = External Service Provider.
MSP = An ESP (not a CSP) that provides technical support services to its clients would be considered an MSP, since it does not host its own cloud platform offering. An ESP may utilize cloud offerings to deliver services to clients without being a CSP. An ESP that manages a third-party cloud service on behalf of an OSA would not be considered a CSP.
RMM = Remote Monitoring & Management system. MSP tool to remotely monitor and access OSA systems.
EDR = System that monitors for malicious activity that may have bypassed antivirus solutions.
FIPS = A type of file encryption required for CUI storage.

Here are the Final Rule MSP highlights…

- MSP's will be in-scope of a CMMC audit and will be required to participate.
- In the vast majority of scenarios, MSP's will not be required to be CMMC certified. That said, it would benefit all involved if the MSP adhered to CMMC controls. For Imagine IT specifically, we are continuing to work towards the CompTIA Cybersecurity Trustmark (CCT) certification (annually 3rd party audited), which aligns well with CMMC. MSP's can likely utilize their existing security vendors (like RMM and EDR). This allows the MSP to keep support costs as-is and maintain tool familiarity.
- For RMM and MSP remote access, MSP's must set up technical and policy controls to block their staff from the ability to download files (to avoid downloading CUI).
- MSP's must utilize data-backup vendors that meet CMMC requirements (FedRAMP Moderate), even if the CUI is FIPS encrypted before being backed up. If there are export controls, there will be a smaller list of vendors for the OSA or MSP to choose from. This will need to be vetted when the OSA engages with their DoD customer.
- The OSA "may" be required to be in a 365 GCC High tenant. It depends upon whether files exist that have export controls. This will need to be vetted when the OSA engages with their DoD customer.

Enforcement and Penalties

- 75% of self-assessed orgs thought they were compliant. Only 4% to-date are.
- OSA disqualification / contract termination.
- Fines, especially if related to false claims can be as high as $27k per false claim.
- Whistleblowers receive up to 30% of the fine proceeds.
- There is no apparent dispute resolution mechanism.

What are the Potential Costs to Obtain and Maintain CMMC Compliance

Assessment Phase (S)	Level 1 self-assessment*	Level 2 self-assessment*	Level 2 certification assessment	Level 3 certification assessment
Periodicity	Annual	Triennial	Triennial	Triennial
Plan and Prepare the Assessment	$1,803	$14,426	$20,699	$1,905
Conduct the Assessment	$2,705	$15,542	$76,743	$1,524
Report Assessment Results	$909	$2,851	$2,851	$1,876
Affirmations	$560	*$4,377	*$4,377	*$5,628
Subtotal	$5,977	$37,196	$104,670	$10,933
**POA&M	$0	$0	$0	$1,869
Total	$5,977	$37,196	$104,670	$12,802

How to Vet an MSP's CMMC Capabilities

Here is some low-hanging fruit...

- If the MSP holds a CMMC L2 certification (which is 3rd party audited), they are good to go. However, audits are backlogged, and it might be a few years before these audits are performed.

- If the MSP is a Registered Practitioner Organization (RPO), they have the ability to guide your org, but they still may need to fully adopt CMMC controls internally.

- If the MSP is currently working towards an audited framework, like CMMC, NIST 800-171, CIS, or CCT, ask for quarterly progress reports in your contractual agreements.

- Ask if they have a Governance-Risk-Compliance (GRC) platform as a central location to document assessments, gaps, progress, Supplier Performance Risk System (SPRS) score, and a Plan of Action & Milestones (POA&M).

Here are some additional questions I obtained from Microsoft Copilot...

When evaluating an IT Managed Service Provider (MSP) for their Cybersecurity Maturity Model Certification (CMMC) expertise, consider asking the following questions:

1. ***Are you familiar with NIST 800-171, DFARS 7012, and CMMC?***
   - *Ensure the MSP has experience with these standards, as they are foundational to CMMC compliance.*
2. ***Can you provide a tailored Shared Responsibility Matrix (SRM)?***
   - *This matrix outlines the division of security responsibilities between your organization and the MSP.*
3. ***What is your process for handling Controlled Unclassified Information (CUI)?***
   - *Ensure they have robust processes for handling and protecting CUI, as this is a critical aspect of CMMC compliance.*
4. ***Are all your applicable employees U.S. persons?***
   - *This is crucial for compliance with certain CMMC requirements, especially if handling Controlled Unclassified Information (CUI).*
5. ***Are you compliant with CMMC requirements yourself?***
   - *An MSP that meets CMMC standards is more likely to effectively guide your organization through the certification process.*

These questions can help you gauge the MSP's readiness and capability to support your CMMC compliance journey.