PERRY JOHNSON
REGISTRARS, INC.

CMMC FAQs

Frequently Asked Questions regarding The Cybersecurity Maturity Model Certification

Acronyms and Definitions

C3PAO - is a Certifying body- however final certificates are issued by the CMMC-AB

FARS - Federal Acquisition Requirements - existing contractors state they comply with FAR. So as not to reinvent the wheel, these are standard requirements for all areas of the government to use in their solicitations.

DFARS - Specific requirements added to DoD contracts

FCI - Federal Contract Information - this is information provided by or generated for the Government Under contract that IS NOT intended for public release (MlI safeguard FCI)

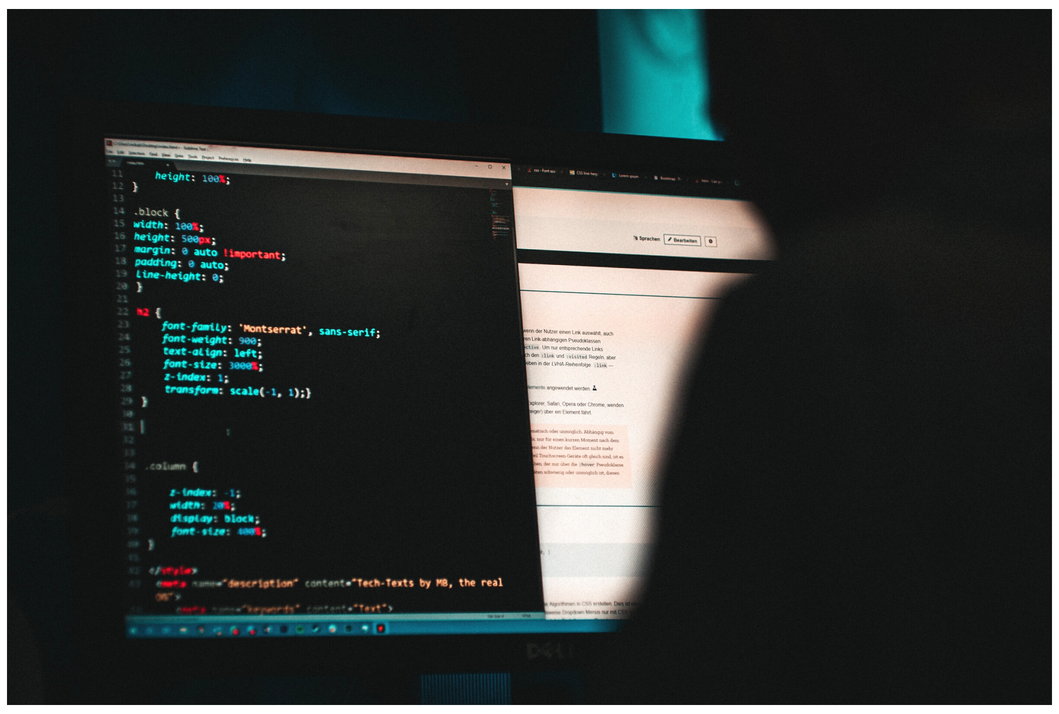
CUI - Controlled Unclassified Information - this is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations and govt wide policies (ML3- Protect)

CTI - Controlled Technical information (out of the scope of CMMC)

Frequently Asked Questions

Q: I heard that all DoD contracts will include a CMMC requirement starting in September 2020; is this true?

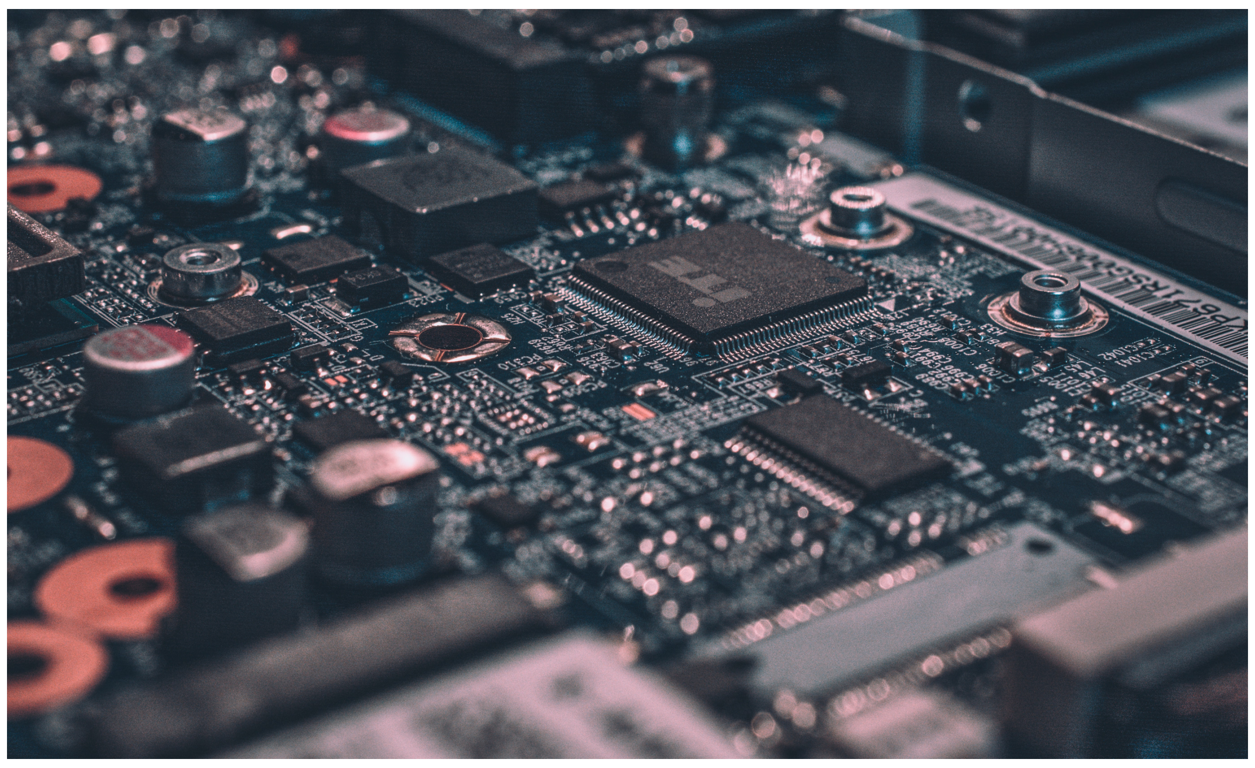
A: We do not speak for the DoD, but they have previously indicated that they intend to introduce CMMC requirements into solicitations on a gradual basis starting in September 2020. We do not have any more detailed visibility into DoD's specific plan.



Frequently Asked Questions (cont.)

Q: Will Third-Party Providers (TPP), like Managed Service Providers (MSP), who support Organizations Seeking Certification (OSC) by contract that receive, store, and transmit* FCI/CUI data be required to be CMMC certified?

A: Basic Answer: TPPs are expected to be required to certify under the DoD rule change.
More Details: TPPs MUST meet CURRENT DFARS 252.204-7012 requirements if they receive, store, and transmit CUI data under DFARS 252.204-7012(m). MSPs must also meet unique requirements in 252.204-7012(b)(2)(ii)(D). Those requirements should be represented "word for word" within the contract terms and conditions or service level agreement (SLA). The TPPs, until they are CMMC certified, must participate during the assessment of the OSC to validate and verify certain practices and requirements between the OSC and TPP for certification.
TPP Exception: Those TPP's that only provide services such as "maintenance", "consulting services", etc. and only requires "access", but do not require receiving, transmitting, or storing FCI/CUI from an OSC's environment, could then be included as any other "1099 subcontractor" with remote or direct system access. All device(s) and personnel training, practices, processes and governance required of the OSC would govern the TPP contracted activities.



Q: What level of maturity will my organization need to be certified to?

A: Any contractor or subcontractor who handles FCI (Federal Contract Information) will be required to become certified to Maturity Level 1 of the CMMC. It is expected that 90% of the defense supply chain will fall into this category. For organizations that handled CUI (Controlled Unclassified Information) a certification to level 3 will be required.

Q: How do I know if my organization is working with CUI?

A: A number of resources and information surrounding CUI can be found on the national archives website (https://www.archives.gov/cui), including categories and types of information that are considered CUI. Another way you can determine if you are currently handling or creating CUI as part of your DoD contract is to review the contract itself and see if CUI is specified. Another option is to reach out to your contracting officer and ask them if CUI is involved with the project.

Q: Are there a lot of accredited C3PAOs?

A: Not yet. The CMMC-AB is building the C3PAO accreditation process with formal adoption and approval by the CMMC AB in the coming months. No C3PAOs are yet formally designated nor accredited by the CMMC-AB, therefore we cannot provide a list. Additional information on C3PAO accreditation process and the CMMC certification process are available at https://www.cmmcab.org/.

Q: If the CMMC standard is still in flux and there aren't any Assessors or C3PAOs, should an organization wait for the final standard to be available before it begins preparing for CMMC?

A: In short, NO! If your organization conducts business with the DOD and your contract includes the DFARS 252.204.7012; you must comply with the guidance identified in NIST SP 800-171 (https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final). Ensuring compliance with that current DFARS regulation has the benefit of easing compliance with CMMC when it is complete. We suggest organizations start preparation now.

Q: How should I start preparing for CMMC?

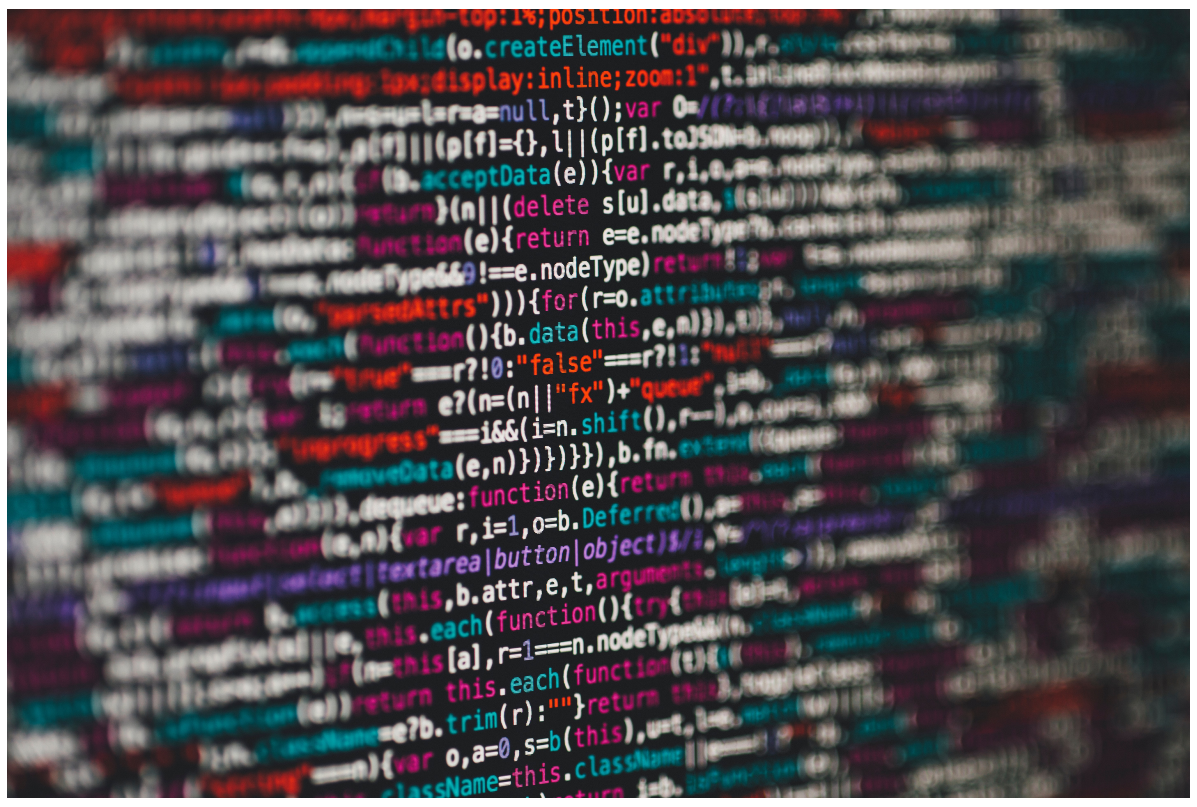
A: The CMMC model is and appendices are available for free from the Office of the Under Secretary of Defense for Acquisition & Sustainment's website (https://www.acq.osd.mil/cmmc/draft.html), which contains all of the practices and processes required for each level. Another important step is to understand what kind of information you handle and store, and identify where it is located, how it is received and who has access to it. You will be able to understand the scope of the systems that will need to adhere to CMMC requirements by identifying where the data enters your organization and where it is stored and processed.

Q: What is the anticipated timeline for the roll out of CMMC requirements in DoD contracts?

A: There is currently a planned gradual roll-out of new contracts requiring CMMC between now and 2026. It is expected that 15 new contracts will require CMMC in 2021, moving up to 75 in 2022, and continuing to grow until all new contracts will require CMMC in 2026.

Q: When will I be able to have my CMMC assessment conducted?

A: Training is currently scheduled to be available for assessors in early 2021, with a plan for assessments to start being conducted by the middle of 2021 by trained assessors working for accredited C3PAO (Certified third party assessment organizations).



Q: How is a CMMC certification obtained?

A: Your company must contact a third-party assessor. After you identify the level required of your organization in the RFP, the assessor will determine whether or not your environment meets the requirements to be certified at that level. Self-certification is not an option. Your certification level will be public knowledge, but specific findings regarding your environment will not be publicly available.

Q: How much will a CMMC certification cost?

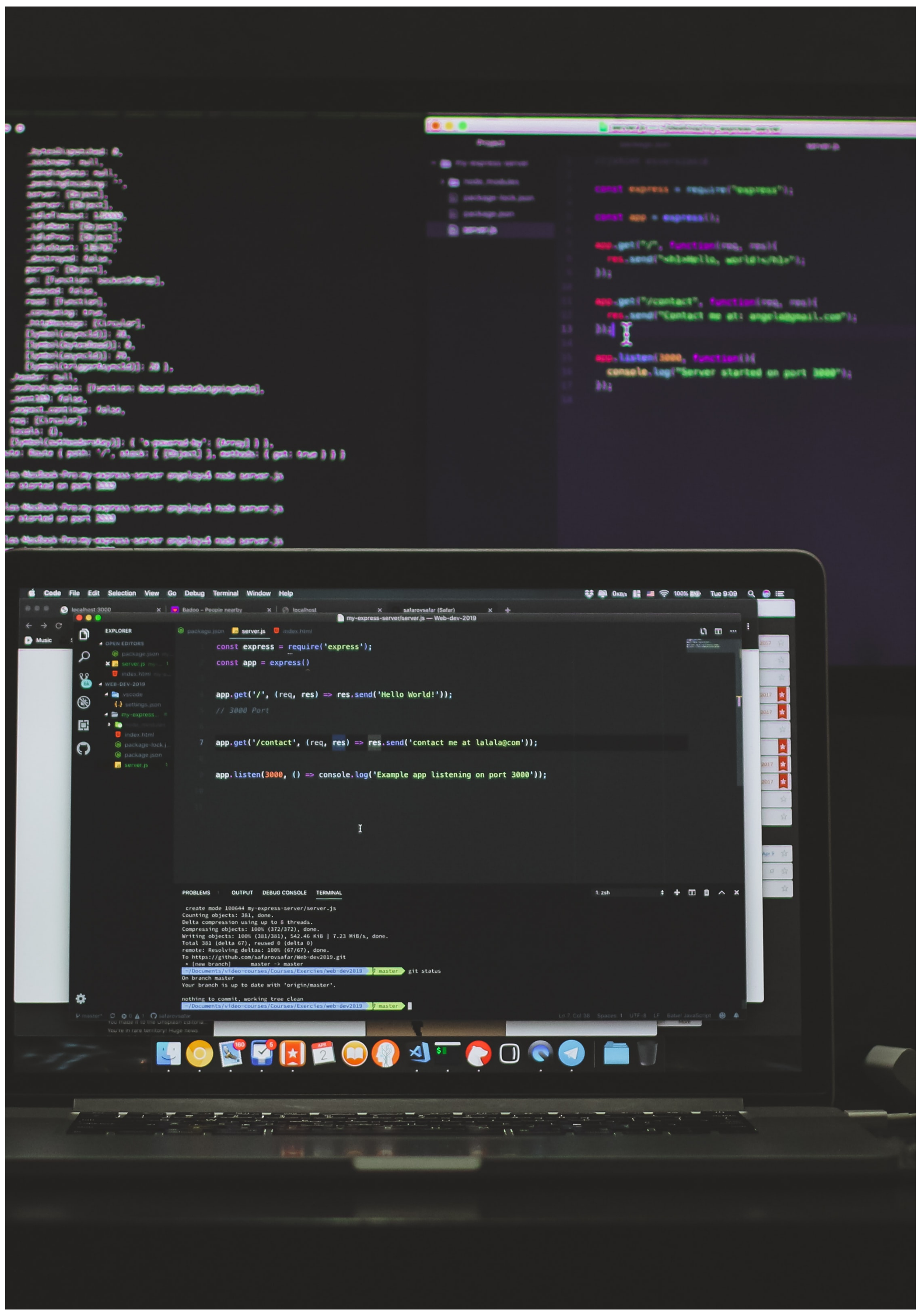
A: The costs of the actual certification are going to be reimbursable under this program. However, costs to implement cybersecurity systems and processes in order to comply with the required certification level will be borne by the company.

Q: What Level of certification will I need?

A: The diversity of the DIB does not lend itself to a one-size-fits-all approach to security. To that effect, the levels of CMMC are meant to sequentially build upon one another. Level 1 is seen as the most universal level of hygiene, while levels 2, 3, 4, and 5, grow more and more complex. Depending on the nature of your organization, the DoD may request more from your cybersecurity environment than others. Your unique CMMC security will become explicitly clear as soon as Requests for Information are sent, as the DoD will appraise your organization based on a contract you currently hold with them. Representatives from the Office of the Under Secretary of Defense have indicated that the vast majority of the DIB will be required to obtain a Level 1 certification.

Q: Who issues the final certificate?

A: Final certificates are issued by the CMMC-AB.



```
const express = require('express');
const app = express()

app.get('/', (req, res) => res.send('Hello World!'));
// 3000 Port

app.get('/contact', (req, res) => res.send('contact me at lalala@com'));

app.listen(3000, () => console.log('Example app listening on port 3000'));
```

```
 create mode 100644 my-express-server/server.js
Counting objects: 381, done.
Delta compression using up to 8 threads.
Compressing objects: 100% (372/372), done.
Writing objects: 100% (381/381), 542.46 KiB | 7.23 MiB/s, done.
Total 381 (delta 67), reused 0 (delta 0)
remote: Resolving deltas: 100% (67/67), done.
To https://github.com/safarovsafar/Web-dev2019.git
 * [new branch]      master -> master
~/Documents/video-courses/Courses/Exercies/web-dev2019  master  git status
On branch master
Your branch is up to date with 'origin/master'.

nothing to commit, working tree clean
~/Documents/video-courses/Courses/Exercies/web-dev2019  master 
```

PERRY JOHNSON
REGISTRARS, INC.

CMMC FAQs