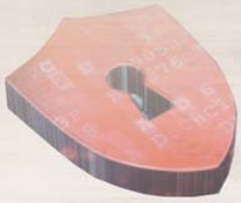
PERRY JOHNSON REGISTRARS, INC.



Cybersecurity Maturity Model Certification (CMMC) 2.0

When the US Government's plans for the Cybersecurity Maturity Model Certification (CMMC) program were initially released on January 31, 2020, it appeared to many like a huge obstacle to overcome. Complex, with five separate levels of certification and a multitude of supporting documents and other information, CMMC was a daunting prospect – not only in conceptual difficulty but in financial burden.

Luckily for those facing up to the necessary task of achieving CMMC, it was decided in 2021 to reevaluate and restructure the original model – leading to the release of CMMC version 2.0 in November of 2021.

Motivated not only by the undue cost burden on small businesses in particular, the Department of Defense (DoD) announced during a Town Hall meeting on November 9th, 2021 that the new alterations to the CMMC framework would be driven by five factors:

- Expense
- Companies not in control of CUI (Controlled Unclassified Information)
- Companies with CUI control not deemed critical to national security
- Companies with CUI control managing information critical to national security
- Companies supporting most sensitive defense programs

The simplified 2.0 framework reduces the number of CMMC levels from five to three – these are based upon risk in relation to national security. The levels formerly known as two and four were determined to never have been assessed individually, but integrated with the others. With their removal, the levels are as follows:

- **Level 1: Foundational** – For companies with FCI (Federal Contract Information) only, which requires protection but is considered non-critical to national security. This level will require self-assessments to NIST 800-171.
- **Level 2: Advanced** – For companies with CUI control, which may require third-party and/or self-assessment based upon the type of information being handled. Advanced/Level 2 will mirror NIST SP 800-171 (110 security practices).
- **Level 3: Expert** – These highest-priority, highest-risk companies handle CUI that is considered very critical to national security. They must be assessed directly by government entities rather than using self-assessments or third-party inputs. Expert/Level 3 will be based on a subset of NIST SP 800-172 requirements.

Of the approximately 300,000 companies in the DIB supply chain that will be affected by the roll-out of CMMC, the majority will require Level 1 certification, with a smaller set requiring Level 2, and a small handful needing the most stringent Level 3 considerations. At this time, the DoD has not released a full timeline for implementation. The piloting program has been temporarily suspended, but all signs point to operations resuming in the next 9-24 months. C3PAOs (service providers chosen and accredited by the CMMC Accreditation Body) may conduct voluntary assessments in the meantime, and training that has already been undertaken and completed under CMMC Version 1.0 can be updated at no additional cost.

At PJR, we understand that CMMC as a whole – not just the changes brought by Version 2.0 – can be overwhelming. We're here to help: join our mailing list and follow our social media to stay up-to-date on the latest news and other information. PJR is happy to offer assistance with level 1 self-assessments and looks forward to offering Level 2 assessments in the not-too-distant future. We look forward to working with your company through the process of achieving CMMC! If you have question regarding CMMC or would like more information, call us at **(248) 358-3388** or email **pjr@pjr.com**.

The Department intends to post the CMMC 2.0 model for Levels 1 and 2, their associated Assessment Guides, and scoping guidance to this website: **https://www.acq.osd.mil/cmmc/model.html** in the coming weeks for informational purposes. Level 3 information will likewise be posted as it becomes available.