

Beginning in 2020, the United States Government initiated sweeping acquisition change to government contractors. Starting with the Department of Defense (DOD) and subsequently with the General Services Administration (GSA), new minimum cybersecurity requirements to compete for government contracts is now in effect. Starting with Requests for Information (RFI) and later with Requests for Proposals (RFP), government contractors must be able to demonstrate conformance with the Cybersecurity Maturity Model Certification (CMMC). Starting November 30, 2020, "all" defense contractors that were awarded work from January 2017 until now likely acknowledged conformance with the National Institute of Standards and Technology Special Publication 800-171 "Protecting Controlled Unclassified Information in Non-Federal Systems and Organizations". Self reporting scorecards are now required and misrepresenting may trigger a false claims act.

### What is CMMC and Why Now?

CMMC is the evolution of pre-existing contractual obligations defined in the Defense Federal Acquisition Regulations back in December of 2016. Organizations were tasked to self-attest to meeting 110 security controls OR have clearly defined plan of actions and milestones to meet the goals and objectives of the National Institute of Standards and Technology Special Publication 800-171.

CMMC has 5 levels and the vast majority of organizations are anticipated to comply with Level 1, which requires basic of cybersecurity controls to be in place. It is also anticipated that between 15,000-20,000 organizations will be expected to comply at Levels 4 or 5, which demonstrates the contractor has proactive or advanced cyber risk management practices.

### What Challenges Should I Expect to Encounter?

The U.S. Government has advised that having a CMMC certification is not required to bid on work but is required at time of award. Through its collaboration with the CMMC Accreditation Board (CMMC-AB), it has been determined that approximately six months is necessary to prepare for certification at Levels 3 and higher.

### The Acquisition Paradigm

Statistics show that an average time it takes the U.S. Government to award a contract is approximately 120 days (can vary greatly depending on scope and number of bidders). This leaves a gap of approximately two months that is otherwise needed to prepare for Level 3 and higher.



### Waiting Equals Risk

*SoundWay has experts with extensive past performance in providing assistance to contractors. We are an official Registered Provider Organization (RPO) through the CMMC-AB. Do not delay and chance losing that premier contracting opportunity by misjudging the time and budgetary requirements to meet these goals and objectives.*



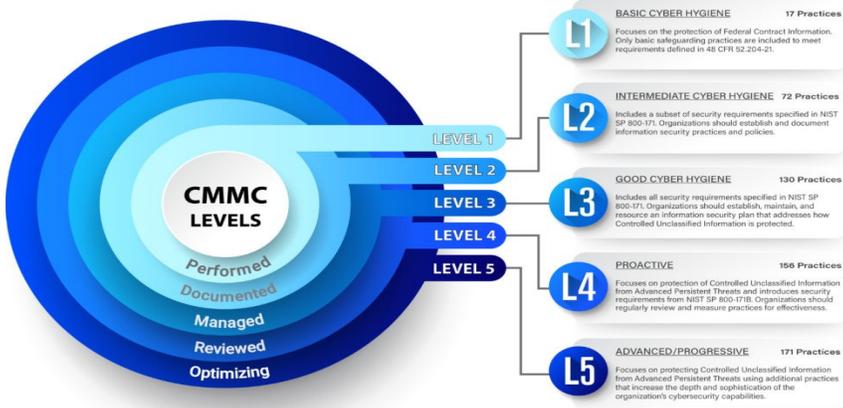
### Not All Companies Are the Same

In addition to being an approved RPO, SoundWay Consulting is also positioned to be one of the very few Level 5 Certified Third Party Assessor Organizations (C3PAO) approved by the CMMC-AB later in 2021. Unlike most consulting firms that claim they will help you, *we stand by our work.* (In the event of a failed audit by the CMMC-AB or claims by State Attorney Generals for failing to meet legal requirements, SoundWay will provide defensive support for up to 40 man-hours at no charge.)

We accomplish this by having a solid understanding of what is required not only by the CMMC-AB but also understanding what additional exposure to harm organizations face when not properly prepared to meet State data protection laws. Our consultants work closely with technologists and legal experts alike.

As an RPO, when we identify recommendations to complete Plans of Actions and Milestones (POA&M) to conform with CMMC, we also provide solutions to each recommendation.

As recently observed with the GSA STARS3 and POLARIS Government Wide Acquisition Contracts (GWACs), CMMC is no longer limited to just



Defense. Later in 2021, it is anticipated the U.S. Department of Homeland Security (DHS) and Treasury will require similar proof of having mature cyber best practices. Do not delay, get prepared now.

To learn more about how SoundWay can help you significantly improve your competitive position and simultaneously reduce exposure to harm stemming from legal liabilities not covered by the CMMC requirements, contact us for a free consultation at (571) 210-0624 or email us at [CMMC@soundwayconsulting.com](mailto:CMMC@soundwayconsulting.com).

### Cyber is about Risk not Compliance



As a Registered Provider Organization (RPO), SoundWay has been vetted by the CMMC-AB to ensure our consultants are trained on the model as well as successfully completed background investigations.



SoundWay is an approved C3PAO candidate merely awaiting our formal on-site assessment by the U.S. Government.

