CMMC
Contractor Assumptions Versus Actuality

Carter Schoenberg, CISSP | QTE | CCP
Vice President & Chief Cybersecurity Officer
ABOUT SoundWay

✓ Cyber AB Authorized C3PAO
  • One of only 42 C3PAOs Nationwide

✓ Expert Cybersecurity Professionals
  ▪ CMMC Certified Assessor (CCA)
  ▪ CMMC Certified Professional (CCP)
  ▪ Industry Certifications:
    CISSP | Security+ | PMP

✓ TOP SECRET Facility Clearance

✓ HUBZone, SDVOSB, WOSB

✓ FAR & DFARS Compliant or over 12 years

SoundWay Consulting Incorporated ("SoundWay")
was founded by Diane Bellegarde, a U.S. Army Service-Disabled Veteran, in 2011.

SoundWay provides information technology, mission support & cybersecurity professional services to the U.S. Department of Defense (DoD), Intelligence Community (IC), federal government civil agencies, and commercial businesses.

SoundWay’s commercial business is focused on providing cybersecurity compliance, CMMC certification readiness, & as a C3PAO we are authorized to conduct CMMC certification Assessments.

Since 2018, SoundWay has worked tirelessly to become a leader in cybersecurity; dedicated to demystifying & simplifying Government compliance mandates & making compliance affordable for its fellow contractor community.
The Cybersecurity Maturity Model Certification (CMMC) initiated in 2019 as a means to ensure Government Contractors are “actually implementing” adequate cybersecurity measures to prevent adversaries of the United States from gaining sensitive information.

Regulatory requirement for Government Contractors (GovCon) that support the Defense Department to undergo third party assessments to independently validate the GovCon’s cyber hygiene.

L1 = 59 objectives that must be attested to (wet ink) by business owner annually

L2 = 320 objectives that must be independently assessed by an approved party

L3 = L2 + additional controls (Must be L2 certified and then assessed by Government)
Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations

Initial Public Draft

Ron Ross
Victoria Pillitteri
Computer Security Division
Information Technology Laboratory

This publication is available free of charge from:
https://doi.org/10.6028/NIST.SP.800-171r3.ipd

May 2023

<table>
<thead>
<tr>
<th>Model</th>
<th>Assessment</th>
</tr>
</thead>
<tbody>
<tr>
<td>110 Controls from SP 800-171</td>
<td>Contracts that are generally specific to</td>
</tr>
<tr>
<td>+ All Controls from NIST SP 800-172</td>
<td>Space and Military applications</td>
</tr>
<tr>
<td></td>
<td>(Supporting Space Force, SCON, HANSCOM, etc.)</td>
</tr>
<tr>
<td></td>
<td>- Estimated 400-500 companies</td>
</tr>
<tr>
<td>All 110 Controls from SP 800-171</td>
<td>Contracts with DFARS Clause 252.254-7012</td>
</tr>
<tr>
<td></td>
<td>and/or Requirements for NIST SP 800-171</td>
</tr>
<tr>
<td></td>
<td>- Estimated 80,000 companies</td>
</tr>
<tr>
<td>17 Controls from NIST SP 800-171</td>
<td>General contracts that do not have CII</td>
</tr>
<tr>
<td></td>
<td>- Estimated 120,000 companies</td>
</tr>
</tbody>
</table>
Period of Performance: Jan 2021 – Present (2.5 Years)

Number of Evaluations: 15

Client Profile (Number of employees): 10-500

Locations: Virginia, Maryland, California, Colorado, Florida, Texas
What percentage completed a SPRS score without an SSP? 87%
What was the lowest score a company issued themselves? 85 out of 110
What was the “actual” average score once we reviewed? 29 out of 110 (Highest: 34)
What percentage had an incident response capability? 6%
What percentage originally thought they were in great shape? 93%
Huge disconnect between what DoD and Cyber-AB want versus real life

CMMC is perceived as an “IT” compliance initiative

Believe CMMC will never make into FAR/DFARs

Lack of experienced practitioners supporting SMB markets

Wasted monies on LPTA approach that equates to snake oil
TIME IS AN ISSUE

2024?
1 C3PAO for every 1000 GovCons

Now

RFIs

RFPs

6/2023

2/2024

10/2024
REALISTIC TIMELINES

1 C3PAO for every 1000 GovCons
If an Organization Seeking CMMC Level 2 Certification utilizes an MSSP, those related activities are in scope of the actual assessment.

- Log Analysis
- Incident Reporting
- Access Control
- Privileged Access
- Data Protection at Rest

Why? Security Protection Asset Considerations
Assets that provide security functions or capabilities to contractor’s CMMC Assessment Scope, irrespective of whether or not these assets process, store, or transmit CUI.

- Document in the asset inventory
- Document in the SSP
- Document in the network diagram of the CMMC Assessment Scope
- Prepare to be assessed against CMMC practices
The Certification issued by an C3PAO applies to “Their System” not “What they Do for You”.

Considerations:
- U.S. Citizens Only?
- Backgrounds?
- SSP Supplementals?
- Accessibility to personnel during your own L2 assessment (if so, at what $$)
- Data at Rest Safeguards?
- 1st and 3rd Party Cyber Liability Insurance?