**Context**

**Cybersecurity Maturity Model Certification (CMMC)** is a US Department of Defense (DoD) Cybersecurity mandate that is impacting the “DIB”, (Defense Industrial Base), who provide products and services to the DoD. Those impacted are primarily defense contractors ranging from those who lead major programs to smaller suppliers who provide sub-components are directly impacted. Additionally, University research related to the DoD is also required to meet CMMC benchmarks. CMMC requires the entire supply chain be included, at various level of depth depending on several parameters.

The US is most impacted. Friendly nations who contract with the DoD also be required to comply. CMMC will expand as NATO looks at this as an international standard. CMMC is likely to expand across all US Government contractors and in time could be a requirement for publicly traded companies.

CMMC requires the DIB to meet specific security requirements in their environment as detailed by the DoD. These requirements grow in number and complexity as an organization’s relationship to the DoD programs expands. For example, a small supplier might only need to meet Level One requirements where an organization who is a prime contractor on a major weapon system will need to reach Level Five including all levels below. A major requirement of CMMC is that an audit by an approved assessor to gain the certification needed to bid on RFPs. Ongoing monitoring and reassessments are part of the program as well.

**Scope**

Achieving the certification needed to bid on DoD RFPs will require existing enterprises to compare their own IT environments to the requirements and implement controls and processes that will allow them to pass this assessment. Many organizations in the DIB have mixed DoD and non-DoD customers. CMMC forces them to examine the flow of sensitive information known as Controlled Unclassified Information (CUI) through out their organization and control what systems and employees work with that information. Those who do not need access will need to be systematically prevented from doing so. Other requirements include encryption of data in transit and at rest. The entire IT infrastructure including clouds being used are subject to inspection. The path to completion is summed up here:

1. Review of current state to determine where CUI data might enter an organization and how it would flow.
2. Determination of who should be granted access to the CUI data.
3. Creation of a boundary that restricts where the CUI information is located.
4. Implementation of controls that meet CMMC needs including control of access to the CUI data.
5. Completion of an assessment by an approved auditor resulting in the CMMC accreditation.
6. Ensuring ongoing CMMC compliance and readiness for reoccurring audits of the environment.

The working group will look at all aspects of CMMC including the specific requirements. It will recommend best practices that will reduce the burden on the organization to complete these steps. It could make recommendations to the CMMC Advisory Board that would have mutual benefits to the DoD and the organizations working to be compliant under CMMC rules.

**Objective**

The objective of this working group is to create a clear pathway for a DIB to be able to implement CMMC. The working group will take a strategic and wholistic approach to create deliverables that will define an actionable plan.

***Deliverables***

The deliverables will be:

* An actionable plan that an agency/business can use as a guideline to implement CMMC
* Creation of best practices based on levels for an impacted organization to leverage.
* Delivery of a proof of concept. The proof of concept can be development of a lab tests CMMC controls in action. Assessors can examine the lab set-up to validate recommendations.

**Cadence and Membership**

The cadence of the meeting will be every other week from TBD. The co-chairs (TBD) will facilitate an environment to present new ideas and discussion topics. This environment will allow for questions to be asked and to find resolution to common challenge issues. Members from the Advisory Board and Assessors should be recruited into the team. A representative from ATARC will keep track of minutes/notes per meeting and make them available using the file sharing collaboration tool listed below.

**Members**

|  |  |  |  |
| --- | --- | --- | --- |
| Name | Email | Agency/Business | Responsibilities |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Rules of Engagement**

The working group rules of engagement are described as below:

* Meet bi-weekly from 10/22/2020 to 2021
* For subgroups to work on specific topic areas to inform the broader group
* Follow the group’s ground rules developed in the charter
* Decisions are made by the co-chairs

**File Sharing and Collaboration Tools**

*Access*

Access to the ATARC Huddle Instance is managed by Kiersten Patton (kpatton@atarc.org ).

*Documentation Repository*

TBD

**Version Control**

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Date | Author | Description |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |