1. Introduction

The theft of intellectual property and sensitive information from all industrial sectors because of malicious cyber activity threatens economic security and national security. The Council of Economic Advisors estimates that malicious cyber activity cost the U.S. economy between $57 billion and $109 billion in 2016 [1]. The Center for Strategic and International Studies estimates that the total global cost of cybercrime was as high as $600 billion in 2017 [2].

Malicious cyber actors have targeted, and continue to target, the Defense Industrial Base (DIB) sector and the supply chain of the Department of Defense (DoD). The DIB sector consists of more than 300,000 companies that support the warfighter and contribute toward the research, engineering, development, acquisition, production, delivery, sustainment, and operations of DoD systems, networks, installations, capabilities, and services. The aggregate loss of intellectual property and certain unclassified information from the DoD supply chain undercuts U.S. technical advantages and innovation as well as significantly increases risk to national security.

As part of multiple lines of effort focused on the security of the DIB sector, the DoD is working with industry to enhance the protection of the following types of unclassified information within the supply chain:

- *Federal Contract Information (FCI*): FCI is information provided by or generated for the Government under contract not intended for public release [3].
- *Controlled Unclassified Information (CUI):* CUI is information that requires safeguarding or dissemination controls pursuant to and consistent with laws, regulations, and government-wide policies, excluding information that is classified under Executive Order 13526, Classified National Security Information, December 29, 2009, or any predecessor or successor order, or Atomic Energy Act of 1954, as amended [4].

To this end, the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) has developed the Cybersecurity Maturity Model Certification (CMMC) framework in concert with DoD stakeholders, University Affiliated Research Centers (UARCs), Federally Funded Research and Development Centers (FFRDCs), and the DIB sector.

This document focuses on the CMMC model. The model encompasses the *basic safeguarding requirements* for FCI specified in Federal Acquisition Regulation (FAR) Clause 52.204-21 and the *security requirements* for CUI specified in National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 Revision (Rev) 2 per Defense Federal Acquisition Regulation Supplement (DFARS) Clause 252.204-7012 [3, 4, 5]. DFARS clause 252.204-70

2 CMMC Model

2.1 Overview

The CMMC framework consists of the security requirements from NIST SP 800-171 Rev 2, *Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations,* and a subset of the requirements from NIST SP 800-172, *Enhanced Security Requirements for Protecting Controlled Unclassified Information: A Supplement to NIST Special Publication 800-171*. The model framework organizes these practices into a set of domains, which map directly to the NIST SP 800-171 Rev 2 families. There are three levels within CMMC—Level 1, Level 2, and Level 3—as described in the sections below.

2.2 CMMC Levels

2.2.1 Descriptions

The CMMC model measures the implementation of cybersecurity requirements at three levels. Each level consists of a set of CMMC practices:

- Level 1: Encompasses the *basic safeguarding requirements* for FCI specified in FAR Clause 52.204-21.
- Level 2: Encompasses the *security requirements* for CUI specified in NIST SP 800-171 Rev 2 per DFARS Clause 252.204-7012 [3, 4, 5].
- Level 3: Information on Level 3 will be released at a later date and will contain a subset of the *security requirements* specified in NIST SP 800-172 [6].

The CMMC levels and associated sets of practices across domains are cumulative. More specifically, for an organization to achieve a specific CMMC level, it must also demonstrate achievement of the preceding lower levels. For the case in which an organization does not meet its targeted level, it will be certified at the highest level for which it has achieved all applicable practices.

2.2.2 CMMC 2.0 Overview

Figure 1 provides an overview of the CMMC 2.0 Levels.

- System and Information Integrity (SI)

2.3 CMMC Practices

2.4.1 Overview

The CMMC model measures the implementation of the NIST SP 800-171 Rev 2 [4] security requirements. The practices originate from the safeguarding requirements and security requirements specified in FAR Clause 52.204-21 [3] and DFARS Clause 252.204-7012 [5], respectively.

- Level 1 is equivalent to all of the safeguarding requirements from FAR Clause 52.204-21.
- Level 2 is equivalent to all of the security requirements in NIST SP 800-171 Revision 2.
- Level 3 will be based on a subset of NIST SP 800-172 and more detailed information will be released at a later date.

2.4.2 List of Practices

This subsection itemizes the practices for each domain and at each level. Each practice has a practice identification number in the format – **DD.L#-REQ** – where:

- DD is the two-letter domain abbreviation;
- L# is the level number; and
- REQ is the NIST SP 800-171 Rev 2 or NIST SP 800-172 security requirement number.

Below the identification number, a short name identifier is provided for each practice, meant to be used for quick reference only. Finally, each practice has a complete practice statement.

3. Summary

The CMMC framework contains three levels. The CMMC practices provide threat mitigation across the levels, starting with basic safeguarding of FCI at Level 1, moving to the broad protection of CUI at Level 2, and culminating with reducing the risk from Advanced Persistent Threats (APTs) at Level 3. The CMMC framework is coupled with a certification program to verify the implementation of practices.

Created in collaboration with a community of DoD stakeholders, UARCs, FFRDCs, and the DIB sector, the CMMC framework addresses the needs of the DoD to protect its unclassified information during the acquisition and sustainment of products and services from the DIB. This model represents one of multiple lines of effort that the DoD and industry are pursuing to enhance the security of the DIB sector. These efforts are instrumental in establishing cybersecurity as a foundation for future DoD acquisitions.