Cybersecurity Maturity Model Certification Initial Impact on the Defense Industrial Base

Hala Strohmier
strohmierh@uncw.edu

Geoff Stoker
stokerg@uncw.edu

Manoj Vanajakumari
vanajakumarim@uncw.edu

Ulku Clark
clarku@uncw.edu

Jeff Cummings
cummingsj@uncw.edu

Minoo Modaresnezhad
modaresm@uncw.edu

University of North Carolina Wilmington
Wilmington, NC 28412 USA

Abstract

The Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) published the Cybersecurity Maturity Model Certification (CMMC) framework in January 2020. The CMMC is a major federal effort intended to strengthen the ability of Defense Industrial Base (DIB) members to protect Federal Contract Information (FCI) and Controlled Unclassified Information (CUI). In this article, we briefly recount the history of unclassified information handling in the U.S. Federal Government that led to the current situation and explain why the CMMC was created, what it is, and what it entails. Through a series of interviews with a small sample of current large and small DIB members, we explore some of the perceptions, perceived challenges, and expected impacts of the CMMC on the DIB. We also consider the chances that the CMMC will accomplish its intended goals and describe a planned future larger study of the CMMC effort and its effects on the DIB.

Keywords: Cybersecurity Maturity Model Certification (CMMC)

An updated manuscript may be found on the JISAR website; https://jisar.org