Redspin
A Division of Clearwater

WHITE PAPER

The Relationship Between CMMC & NIST SP 800-171

NIST SP 800-171 (Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations) is a federal government standard that provides minimum requirements for nonfederal agencies (i.e., Department of Defense contractors) to adequately protect Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). In the past, self-attestation was the only requirement. As the threat landscape became more aggressive, an advanced cybersecurity maturity model, called the Cybersecurity Maturity Model Certification (CMMC) framework, was developed to improve the cybersecurity posture of the Defense Industrial Base (DIB) to adequately protect CUI/FCI.

THE CHALLENGE

Adversaries continue to target the Defense Industrial Base (DIB) via cyberattack vectors to gain access to sensitive data, causing significant damage to the Department of Defense (DoD's) supply chain, and ultimately, critical offensive and defensive capabilities. The DoD is aiming to reduce the estimated $600 billion in cybercrime losses impacting the nation's military supply chain every year by requiring third-party cyber security assessments of contractors that process, store, and/or transmit Federal Contract Information (FCI)/Controlled Unclassified Information (CUI). To combat these threats, the DoD released two clauses in the Code of Federal Regulations (CFR).

In 2016, the DoD released CFR 52.204-21, which identified 15 basic safeguarding requirements required by all Defense Industrial Base (DIB) primes and subs. Contractors would self-attest, annually, that the 15 practices were implemented and adhered to. Later in 2016, the DoD released the Defense Acquisition Regulation Supplement (DFARS) 252.204-7012, which aligned the practices with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171 revision 2 with a compliance date set for the end of the fiscal year 2017.

In early 2018, it was determined by the Office of the Under Secretary of Defense for Acquisition and Sustainment (OUSD(A&S)) that DoD Contractors were not accurately self-attesting to the security controls required to protect CUI in accordance with the Defense Federal Acquisition Regulation Supplement (DFARS) 252.204-7012.

In 2019, the DoD reached out to the industry to assist with the development of a program that can accurately assess the security of DoD contractor information systems before awarding a DoD contract, and thus CMMC was born.

THE SOLUTION

The Cybersecurity Maturity Model Certification (CMMC) is a DoD initiative to verify proper cybersecurity practices/processes are in place to adequately protect FCI and CUI within the DIB networks. The CMMC combines various cybersecurity standards and best practices, **which are mapped to NIST SP 800-171r2.** Certified independent third-party organizations will conduct CMMC assessments of current/potential DoD Contractors who store, process, or transmit CUI to assess CMMC compliance before awarding DoD contracts.

NIST SP 800-171 is considered an international standard, and thus partnering nations that support the DoD can comply with the requirements.

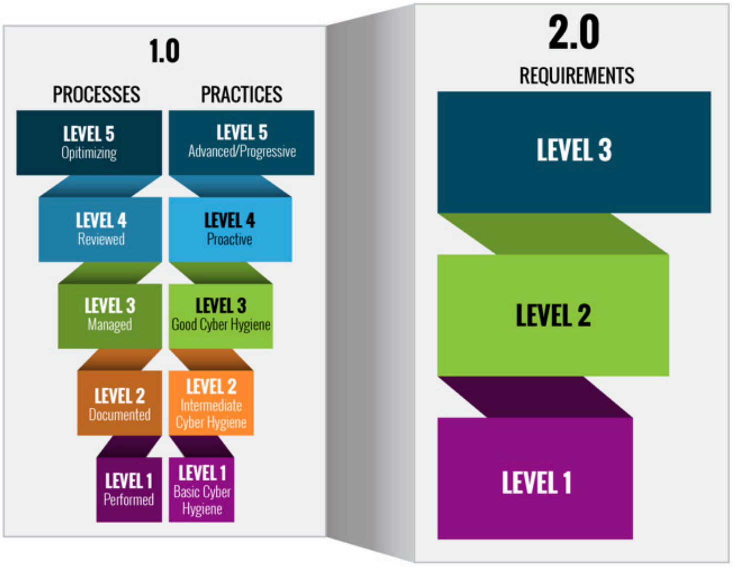
THE NIST SP 800-171R2 AND CMMC RELATIONSHIP

CMMC Level 1 – CMMC Level 1 is designed to protect FCI data. In accordance with CFR 52.204-21, 15 basic safeguarding practices are mapped to 15 practices within NIST SP 800-171r2, with two additional practices added for a total of 17 practices. In the CMMC model, level 1 requires an annual self-attestation from Organizations Seeking Certification (OSCs), that must be signed by the senior official within the OSC.

CMMC Level 2 – CMMC Level 2 is designed to protect CUI data. In accordance with DFARS 252.204-7012, OSCs must implement all 110 practices from NIST SP 800-171r2. This level requires a certification assessment from a CMMC Third-Party Assessment Organization (C3PAO) every three years. The certification methodology, adopted by the Cyber Accreditation Body (Cyber AB), is mapped to NIST SP 800-171a and scored as met, not met, inherited, or not applicable.

CMMC Level 3 – CMMC Level 3 is the final level of the CMMC Model. OSCs seeking this level of certification must first pass a level 2 certification from a C3PAO, then must pass a delta assessment of a set number of practices (Still to be determined) from NIST SP 800-172. This assessment is performed by the Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC).

There is still a requirement for contractors to submit their NIST SP 800-171 self-assessment annually into the Supplier Performance Risk System (SPRS).



Overview of CMMC 1.0 to 2.0 Model

THE DIFFERENCES BETWEEN CMMC AND NIST SP 800-171

Although CMMC maps directly to NIST SP 800-171r2, there are subtle differences in the program OSCs should be aware of. Those include:

- CMMC has a certification body called the Cybersecurity Assessor and Instructor Certification Organization (CAICO). The CAICO falls under the Cyber AB and is responsible for all CMMC training and exams associated with certifying assessors for the CMMC ecosystem. This is not the same for NIST SP 800-171r2, which anyone can perform an assessment against
- The CMMC Model is a cumulative model that builds on each level. Level 1 has 17 practices, which are added to the additional 93 practices of Level 2 equaling 110 practices in total
- CMMC only allows certain practices to be admitted to a Plan of Actions & Milestones (POA&M), while NIST 800-171 does not restrict any practices from a POA&M

- To start a CMMC assessment, OSCs must clear all open items in a POA&M. Any gaps identified during the assessment will be placed in a new POA&M, if permissible. Under NIST SP 800-171 an organization can have a POA&M in place at the start of the assessment
- OSCs will have 180 days to clear POA&M items under the CMMC model, compared to NIST 800-171 which does not have a time limit on POA&M items
- Under the CMMC Model, the C3PAO is the issuing authority for CMMC Certificates when an OSC passes the assessment. Under NIST 800-171, there is no certificate

SUMMARY

The overall objective of CMMC is to reduce the risk to the defense supply chain, and ultimately national security, from adversarial attacks on the DIB. Self-attestations of properly protecting FCI/CUI data was not working and required a more “hands-on” assessment methodology from industry professionals, with direct guidance from the Cyber AB, and oversight from the DoD.

WHY REDSPIN

Redspin is the first authorized C3PAO. Our team of experts can help you navigate the complexities of NIST and CMMC requirements to assist you on your journey to becoming CMMC certified.

- Nearly 100 security advisors and assessors, with many years of experience with federal regulations and guidelines, including FAR, FISMA, DFARS, and NIST, po to scale with you as needed.
- Possesses the know-how from performing over 1,000 NIST-based assessments in highly regulated industries.
- A large percentage of Redspin’s security advisors and assessors are military veterans with years of hands-on NIST experience.
- Our knowledgeable assessors give you the confidence that your people, processes, and technology are effective.

Redspin, an early adopter working with Cyber-AB to help define the program is the first Authorized CMMC C3PAO and is a RPO.

Redspin’s CMMC Services won the 2023 Cybersecurity Excellence Award for best National Cyber Defense Cybersecurity Industry Solution.

Redspin, a division of Clearwater, has become one of the most trusted cybersecurity companies for the Defense Industrial Base. Our exclusive focus on tailoring our CMMC assessment, training, consulting, and managed services for each client delivers peace of mind by lowering the risk of a security incident or breach, and meeting/maintaining compliance regulations. Since our founding in 2001, we’ve become a thought leader in IT security, helped countless clients control their security risk, develop their security strategy, and avoid a breach headline.

40 Burton Hills Blvd
Suite 200
Nashville, TN 37215

info@redspin.com
800.721.9177
www.redspin.com