KING & SPALDING

Client Alert

Data, Privacy and Security

DoD Releases Version 1.0 of the Cybersecurity Maturity Model Certification Framework

MARCH 5, 2020

For more information, contact:

Robert Hudock
+1 202 626 5521
rhudock@kslaw.com

Adam Solander
+1 202 626 5542
asolander@kslaw.com

Steve Cave
+1 202 626 9628
scave@kslaw.com

Rick Vacura
+1 703 245 1018
rvacura@kslaw.com

Igor Gorlach
+1 713 276 7326
igorlach@kslaw.com

Anush Emelianova
+1 404 572 4616
aemelianova@kslaw.com

King & Spalding

Washington, D.C.
1700 Pennsylvania Avenue, NW
Washington, D.C. 20006-4707
Tel: +1 202 737 0500

Atlanta, GA
1180 Peachtree Street, NE
Atlanta, GA 30309
Tel: +1 404 572 4600

On January 31, 2020, the Department of Defense (DoD) released the latest version (Version 1.0) of its Cybersecurity Maturity Model Certification (CMMC) framework, setting forth future cybersecurity requirements for thousands of DoD contractors and subcontractors. Outside of the DoD, the framework may influence courts' and regulators' understanding of what constitutes reasonable and appropriate security measures more broadly.

The CMMC is a certification framework that measures a contractor's ability to safeguard Controlled Unclassified Information (CUI) and Federal Contract Information (FCI). CMMC implementation will require cybersecurity audits by CMMC Third Party Assessment Organizations (C3PAOs) for more than 300,000 companies. The DoD announced that it will include the new requirements in certain requests for information (RFIs) starting in June 2020, and requests for proposals (RFPs) in September 2020, and that all contractors will be required to obtain CMMC certifications by Fiscal Year 2026. The phased rollout approach is a change from DoD's previous statements that it could implement CMMC more broadly this year. The required level of certification for a contract award will be indicated in each DoD solicitation. The DoD is currently drafting a rulemaking to implement CMMC, with the intent to publish a final rule by September 2020.

THE CMMC ACCREDITATION BODY

The DoD is currently working on a Memorandum of Understanding between the DoD and the newly-formed CMMC Accreditation Body (AB). The AB Board of Directors consists of 13 individuals from private industry. The AB will be responsible for managing, operating, and sustaining the CMMC program, CMMC training, and evaluating and accrediting individual assessors and C3PAOs. C3PAOs will conduct CMMC assessments, which are comprised of on-site evaluations of the capabilities, practices, and process maturity defined in the CMMC model. The DoD has indicated that it will provide initial training guidance to the AB in the first quarter of 2020.

The AB will then use DoD materials to make training available to individual assessors and C3PAOs.

CMMC PRE-ASSESSMENTS

While the DoD develops CMMC's regulatory and contractual framework, and the AB determines processes for accrediting and training individual assessors and C3PAOs, the AB advises contractors and potential contractors to conduct pre-assessments using the most current draft of CMMC. Pre-assessments will allow entities to be prepared to obtain a certification at the appropriate level in the short timeframe granted by the DoD's requirements. Retaining legal counsel to oversee risk assessments, including CMMC pre-assessments, is advisable, due to the sensitive nature of such assessments and the potential liability that could result from the disclosure of non-privileged assessment results.

CMMC VERSION 1.0

Under the CMMC framework, defense contractors and subcontractors will be required to undergo a C3PAO assessment of their internal cybersecurity technical practices and process maturity against published standards. Each assessment must be guided by the CMMC and can result in certification at one of five levels, with Level 1 as the lowest level and Level 5 as the highest level. Much like HITRUST, CMMC recognizes a progression of maturity levels, ranging from simple documentation of security practices to establishing a standardized measurement and management framework on top of policy documentation. A Level 4 or 5 certification demonstrates the contractor's ability to reduce the risk of Advanced Persistent Threats (APTs). An APT is defined as an adversary that possesses sophisticated levels of expertise and significant resources which allow it to create opportunities to achieve its objectives by using multiple attack vectors (e.g., cyber, physical, and deception).

The CMMC framework focuses on 17 domains: Access Control, Asset Management, Audit and Accountability, Awareness and Training, Configuration Management, Identification and Authentication, Maintenance, Media Protection, Personnel Security, Physical Protection, Recovery, Risk Management, Security Assessment, Situational Awareness, System and Communications Protection, System and Information Integrity. Each domain consists of a set of processes and capabilities (and in turn, practices) across the five levels. With the exception of Asset Management, Recovery, and Situational Awareness (threat monitoring), these domains originate from the security-related areas in Federal Information Processing Standards (FIPS) Publication 200 and the related security requirement families from NIST SP 800-171.

Below are overviews of the CMMC maturity process and practice progressions.

CMMC MATURITY PROCESS PROGRESSION

Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Performed 0 processes * Select practices are documented where required	*Documented* 2 processes * Each practice is documented, including Level 1 practices * A policy exists that includes all activities	*Managed* 3 processes * Each practice is documented, including lower levels * A policy exists that includes all activities * A plan exists, is maintained, and resourced that includes all activities	*Reviewed* 4 processes * Each practice is documented, including lower levels * A policy exists that includes all activities * A plan exists, is maintained, and resourced that includes all activities * Activities are reviewed and measured for effectiveness, and results are shared with management	*Optimizing* 5 processes * Each practice is documented, including lower levels * A policy exists that includes all activities * A plan exists, is maintained, and resourced that includes all activities * Activities are reviewed and measured for effectiveness, and results are shared with management * There is a standardized, documented approach across all applicable organizational units

CMMC PRACTICE PROGRESSION

Level 1	**Level 2**	**Level 3**	**Level 4**	**Level 5**
Basic cyber hygiene 17 practices * Equivalent to all practices in FAR 48 C.F.R. § 52.204-21	*Intermediate cyber hygiene* 72 practices * Comply with the FAR * Includes a select subset of 48 practices from the NIST SP 800-171 r1 * Includes an additional 7 practices to support intermediate cyber hygiene	*Good cyber hygiene* 130 practices * Comply with the FAR * Includes all practices from NIST SP 800-171 r1 * Includes an additional 20 practices to support good cyber hygiene	*Proactive* 156 practices * Comply with the FAR * Includes all practices from NIST SP 800-171 r1 * Includes a select subset of 11 practices from Draft NIST SP 800-171B * Includes additional 15 practices to demonstrate a proactive cybersecurity program	*Advanced / Progressive* 171 practices * Comply with the FAR * Includes all practices from NIST SP 800-171 r1 * Includes a select subset of additional 4 practices from Draft NIST SP 800-171B * Includes additional 11 practices to demonstrate a proactive cybersecurity program

The DoD provides an overview of the CMMC components in its briefing PDF, which accompanies the full CMMC Version 1.0 document.

ABOUT KING & SPALDING

This alert provides a general summary of recent legal developments. It is not intended to be and should not be relied upon as legal advice. In some jurisdictions, this may be considered “Attorney Advertising.” View our Privacy Notice.