King & Spalding
Client Alert

DECEMBER 8, 2020

Department of Defense's New Assessment Methodology Takes Effect

For more information, contact:

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

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

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

Rick Vacura
+1 202 626 9629
rvacura@kslaw.com

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

King & Spalding

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

Northern Virginia
1650 Tysons Blvd
Suite 400
McLean, VA 22102
Tel: +1 703 245 1000

As of November 30, 2020 government contractors and offerors must ensure that they follow the Department of Defense's (DOD) new assessment methodology set forth in its September interim rule (Interim Rule). The two frameworks that will be pertinent to DOD contracting are NIST SP 800-171 and the Cybersecurity Maturity Model Certification (CMMC).

With respect to NIST SP 800-171, contractors and offerors must ensure that they complete a NIST SP 800-171 Basic Assessment and submit the summary level score and other required information to the Supplier Performance Risk System (SPRS). If the DOD elects to conduct a higher-level Assessment, contractors will need to be prepared to support the Assessment. Contractors must also ensure that their subcontractors post their score to the SPRS, and that their subcontractor agreements include provisions addressing this requirement.

As for the CMMC, contractors and offerors will be required to obtain a certification where the "requirement document or statement of work requires a contractor to have a specific CMMC level." It is not clear yet which solicitations will include this requirement. As indicated by DOD in previous guidance, the CMMC certification requirements will be gradually rolled out, with general applicability scheduled for October 1, 2025.

NIST SP 800-171 ASSESSMENT METHODOLOGY

The Defense Federal Acquisition Regulation Supplement clause 252.204-7012 has long required DOD contractors to apply the security requirements of NIST SP 800-171 to "covered contractor information systems" that are not part of an IT service or system operated on behalf of the government.

Under the Interim Rule, beginning on November 30, 2020, offerors to whom the NIST SP 800-171 Assessment requirement applies will be required to follow the new NIST SP 800-171 DOD Assessment Methodology and post their Assessment to the SPRS in order to be considered for an award. Such an Assessment must be from the three

years preceding the award. Moreover, such an Assessment must follow the new standards for a "Basic" Assessment. The Basic Assessment is a self-assessment pursuant to which the contractor begins with the total score of 110 and reduces points for each unimplemented requirement, with reductions weighted based on their impact to the covered contractor information system, until a summary level score is calculated. The summary level score is posted on the SPRS. No specific score is required for the completion of a Basic Assessment, but a contractor must identify a date by which it expects to achieve a score of 110.

To submit the Basic Assessment, contractors are required to complete the following:

1. System Security Plan name (if more than one system is involved);
2. CAGE code associated with the plan;
3. A brief description of the plan architecture;
4. Date of the assessment;
5. Total score; and
6. The date a score of 110 will be achieved.

In addition to the Basic Assessment, the DOD may conduct a "Medium" or "High" Assessment of the contractor during performance. A "Medium" assessment consists of (i) a review of a contractor's Basic Assessment, (ii) a thorough document review, and (iii) discussions with the contractor to obtain additional information or clarification, as needed and results in a confidence level of "Medium" in the resulting score. A High Assessment adds to these processes a verification, examination, and demonstration of a contractor's system security plan to validate that NIST SP 800–171 security requirements have been implemented as described in the contractor's system security plan. The DOD will determine the summary level score for Medium and High Assessments. Contractors are required to provide the DOD with access to their facilities, systems, and personnel when it is necessary for the DOD to conduct or renew a higher-level Assessment.

Contractors are also required to ensure that any subcontractors post their Assessments to the SPRS prior to engaging such subcontractors.

ROLLING OUT THE CMMC FRAMEWORK REQUIREMENTS

In the second part of the Interim Rule, the DOD reiterated a phased rollout of the CMMC certification requirement, with full adoption planned for October 1, 2025. Additional information on the CMMC Framework itself is available in our March 5, 2020 client alert.

On October 1, 2025, the CMMC certification requirement will become applicable to all DOD solicitations and contracts, including those for the acquisition of commercial items (excluding those exclusively for the acquisition of commercially available off the shelf items) valued at greater than the micro-purchase threshold. Until then, the requirements are prescribed for use in solicitations and contracts "if the requirement document or statement of work requires a contractor to have a specific CMMC level." Approval from the Office of the Undersecretary of Defense for Acquisition and Sustainment is required before including a CMMC requirement in a solicitation. Contracting officers are required to verify in the SPRS that the offeror's or contractor's CMMC certification is current and meets the required level prior to making the award. As with the NIST SP 800-171 Assessment, the certification must be from the three years preceding the contract.

The Interim Rule also codified regulations requiring a contractor to maintain the requisite CMMC level for the duration of the contract; ensure that its subcontractors also have the appropriate CMMC level prior to awarding a subcontract (although it is not clear which level is appropriate); and include the corresponding requirements in all subcontracts or other contractual instruments.

While these new regulations established the regulatory shell for the incorporation of the CMMC certification into DOD contracting, there are details that will need to be worked out during the rollout phase, and likely outside of the regulations text. For example, the Interim Rule did not address whether CMMC Assessors will provide credit to contractors for achieving other security standards, such as ISO 27001 certification or a NIST SP 800-171 Assessment. Thus, while contractors maintain and improve security standards, they should continue monitoring the guidance from DOD and the CMMC Accreditation Body.

ABOUT KING & SPALDING

Celebrating more than 130 years of service, King & Spalding is an international law firm that represents a broad array of clients, including half of the Fortune Global 100, with 1,200 lawyers in 22 offices in the United States, Europe, the Middle East and Asia. The firm has handled matters in over 160 countries on six continents and is consistently recognized for the results it obtains, uncompromising commitment to quality, and dedication to understanding the business and culture of its clients.

ABU DHABI	CHARLOTTE	GENEVA	MOSCOW	RIYADH	TOKYO
ATLANTA	CHICAGO	HOUSTON	NEW YORK	SAN FRANCISCO	WASHINGTON, D.C.
AUSTIN	DUBAI	LONDON	NORTHERN VIRGINIA	SILICON VALLEY	
BRUSSELS	FRANKFURT	LOS ANGELES	PARIS	SINGAPORE	