Booz | Allen | Hamilton

CYBERSECURITY UPDATES FOR SUPPLIERS

MAY 2021

- CYBERSECURITY ENVIRONMENT & REQUIREMENTS
- NEW CYBERSECURITY RULES
- CMMC FRAMEWORK

CYBERSERCURITY ENVIRONMENT & REQUIREMENTS

TODAY’S CYBERSECURITY ENVIRONMENT

- Malicious cyber activity continues to threaten both our economic and national security (~$600B lost to cyber attacks annually worldwide) and adversaries continue to heavily target Defense Industrial Base (DIB) information systems

- DoD and Industry need to continue to work to enhance the protection of controlled unclassified information (CUI) within the supply chain

WHY CHANGE IS NEEDED?

- DoD IG found DoD contractors are not consistently implementing mandated NIST SP 800-171 Rev. 2 system security requirements for safeguarding CUI, as required by DFARS 252.204-7012

- Likewise, DFARS 252.204-7012 does not provide a standard methodology for verifying a contractor's implementation of the security requirements, instead relying solely on self-attestation

- Finally, the current security requirements in NIST SP 800-171 Rev. 2 do not sufficiently address additional threats to include Advanced Persistent Threats (APTs)

- Because of these issues/shortcomings, DoD determined that the status quo was not acceptable and developed a two-pronged approach to assess and verify the DIB's ability to protect CUI on its information systems or networks

THE APPROACH - "TRUST, BUT VERIFY"

NIST SP 800-171 DOD ASSESSMENT METHODOLOGY

- A standard m*ethodology* to assess contractor implementation of the cybersecurity requirements in NIST SP 800-171 Rev. 2, "Protecting Controlled Unclassified Information (CUI) In Nonfederal Systems and Organizations"
- *Objective:* *Provide DoD with the ability to assess a contractor's implementation of NIST SP 800-171 security requirements*

CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) FRAMEWORK

- A multi-level cybersecurity certification framework administered by certified third-party assessor organizations to measures the institutionalization of processes and implementation of cybersecurity practices by DoD contractors
- *Objective:* Assurances that a contractor can adequately protect CUI at a level commensurate with the contract's risk, while simultaneously accounting for information flow down to its suppliers in a multi-tier supply chain

NEW CYBERSERCURITY RULES

Interim Final Rule - DFARS Case 2019-D041 - Assessing Contractor Implementation of Cybersecurity Requirements

- Rule Amends the DFARS (effective 12/01/20) to include the following new provisions/clauses:
  - **252.204-7019**, Notice of NIST SP 800-171 DoD Assessment Requirement
  - **252.204-7020**, NIST SP800-171 Assessment Requirements
  - **252.204-7021**, Cybersecurity Maturity Model Certification (CMMC) Requirements

NIST SP 800-171 Assessment Requirements

DFARS 252.204-7019, NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENT

DFARS 252.204-7020, NIST SP 800-171 ASSESSMENT REQUIREMENTS

- Provides for the assessment of a contractor’s implementation of NIST SP 800-171 Rev. 2 security requirements, as required by DFARS 252.204-7012
- The Assessment uses a standard scoring methodology, and three assessment levels (Basic, Medium, and High), which reflect the depth of the assessment performed and the associated level of confidence in the score resulting from the assessment
- A Basic Assessment is a self-assessment completed by the contractor, while Medium or High Assessments are completed by the Government
- The results of a current assessment must be documented in the Supplier Performance Risk System (SPRS) to provide DoD with visibility into the scores

NIST SP 800-171 Assessment Requirements

Question 1: When should we expect to see these requirements?

- Effective 12/1/2020 Contracting Officers are required to include the 252.204-7019 and 252.204-7020 clauses in all solicitations and contracts, task orders, or delivery orders except for those that are solely for the acquisition of COTS items

- Contracting Officers are further required to verify that the summary level score of a current NIST SP 800-171 DoD Assessment (i.e. Not more than 3 years older) are posted in Supplier Performance Risk System (SPRS)

  - Upon award of a contract, task order, or delivery order that contains 252.204-7012;

  - Upon exercising an option period or extending the period of performance on a contract, task order, or delivery order with a contractor that contains 252.204-7012

NIST SP 800-171 Assessment Requirements

<u>Question 2: Is this requirement applicable to suppliers?</u>

- To the extent that 252.204-7019 & 7020 are included in our prime contracts, <u>and the suppliers are subject to NIST SP 800-171 security requirements</u> pursuant to DFARS 7012, the substance of the clause is required in all subcontracts including subcontracts for the acquisition of commercial items (excluding COTS items)

- Starting 12/1/2020 Contractor shall not award a subcontract unless the supplier (1) has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment and (2) submitted the score to be registered in SPRS

NIST SP 800-171 Assessment Requirements

<u>Question 3: What happens if a supplier is unable to certify to its compliance with DFARS 252.204-7020?</u>

- If the DFARS 7020 clause is included in our Prime contract, the supplier must also be compliant with 7020 if they are subject to NIST SP 800-171 security requirements pursuant to DFARS 7012

- We are encouraging all existing suppliers to complete a NIST 800-171 self-assessment and send the score to SPRS database to be prepared for a situation where the contract could be modified to include the requirement in the future

- For existing Booz Allen suppliers on an existing subcontract who have (1) previously confirmed non-applicability to DFARS 7012 and (2)who are working under one of the viable options, these subcontracts are not subject to the NIST SP 800-171 security requirements, and thus are also not subject to DFARS 7020

CMMC FRAMEWORK

Cybersecurity Maturity Model Certification (CMMC)

252.204-7021, CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) REQUIREMENTS

- CMMC framework adds a comprehensive and scalable certification element to verify the implementation of processes and practices associated with the achievement of a cybersecurity maturity level
- Designed to provide increased assurance to the DoD that a DIB contractor can adequately protect CUI at a level commensurate with the contract’s risk, accounting for information flow down to its suppliers in a multi-tier supply chain
- Assessments will be conducted by accredited CMMC Third Party Assessment Organizations (C3PAOs)
- Upon completion of a CMMC assessment, a company is awarded a three-year certification by an independent CMMC Accreditation Body (AB) at the appropriate CMMC level, and the certification level is documented in SPRS to enable verification by the Govt.

CMMC - The Latest

- DoD is implementing a phased rollout of CMMC through 2025
- Inclusion of CMMC requirements, via DFARS 252.204-7021, in a solicitation during the intervening time period must be approved by USD(A&S), and the DoD intends to first begin with 15 “Pathfinder” Contracts. Once this list is finalized, Booz Allen will evaluate potential impacts and/or bidding interest
- Starting October 1, 2025 CMMC will apply to all DoD solicitations and contracts, including those for the acquisition of commercial items (except those exclusively COTS items) valued at greater than the micro-purchase threshold, and Contracting Officers will not make award, or exercise an option on a contract, if the offeror or contractor does not have current (i.e. three years) certification for the required CMMC level
- CMMC certification requirements are required to be flowed down to suppliers at all tiers, based on the sensitivity of the unclassified information flowed down to each supplier

CMMC

Question 1: How is CMMC different from NIST SP 800-171?

- CMMC Level 3 encompasses the 110 security requirements specified in NIST SP 800-171 Rev. 2, however Level 3 also incorporates 20 additional practices and processes from other standards, references, and sources
- In addition to assessing a company's implementation of cybersecurity practices, the CMMC also assesses the company's institutionalization of cybersecurity processes
- Specific CMMC Level 4 & 5 requirements are still being finalized and are expected to change. To date the DoD has indicated that industry should not expect to see CMMC Level 4 or 5 in any near-term procurements

CMMC

Question 2: Has Booz Allen undergone a CMMC certification and/or been assigned a CMMC level?

- No, as of the date of this training there are currently no DIB companies that have undergone a CMMC assessment or been assigned a CMMC level

- The CMMC-AB is still building the C3PAO accreditation process with formal adoption and approval by the CMMC AB in the coming months. No C3PAOs are yet formally designated nor accredited by the CMMC-AB

CMMC

Question 3: When will we begin seeing CMMC requirements?

- Up until 9/30/2025 inclusion of CMMC requirements in a solicitation, via DFARS 252-204.7021, will require prior approval from USD(A&S), with 15 “Pathfinder” RFPs/Contracts intended to be piloted in GFY21

- Beginning 10/1/2025 the DFARS will require inclusion of CMMC requirements in all solicitation and contracts or task orders or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for solicitations and contracts or orders solely for the acquisition of COTS items

CMMC

Question 4: Will CMMC requirements apply to existing contracts?

- At this time DoD has communicated that CMMC requirements will be forward looking only. i.e. no CMMC specific requirements will be added to existing contracts

CMMC

<u>Question 5: Will CMMC requirements be applicable to suppliers?</u>

Yes!

- To the extent 252.204-7021 is included in our prime contracts the substance of the clause is required in all subcontracts including subcontracts for the acquisition of commercial items (excluding COTS items)
- Once CMMC is implemented, prior to awarding to a supplier, we must ensure that the supplier has a current (i.e., not older than 3 years) CMMC certificate at the CMMC level that is appropriate for the information that is being flowed down to the supplier. [DFARS -7021c(2)]