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

PART 204—ADMINISTRATIVE AND INFORMATION MATTERS

* * * * *

SUBPART 204.73 -- SAFEGUARDING COVERED DEFENSE INFORMATION AND CYBER INCIDENT REPORTING

* * * * *

204.7302 Policy.

(a)**[(1)]** Contractors and subcontractors are required to provide adequate security on all covered contractor information systems.

[(2) Contractors required to implement NIST SP 800-171, in accordance with the clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber incident Reporting, are required at time of award to have at least a Basic NIST SP 800-171 DoD Assessment that is current (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-70XX).

(3) The NIST SP 800-171 DoD Assessment Methodology is located at https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.

(4) High NIST SP 800-171 DoD Assessments will be conducted by Government personnel using NIST SP 800-171A, "Assessing Security Requirements for Controlled Unclassified Information."

(5) The NIST SP 800-171 DoD Assessment will not duplicate efforts from any other DoD assessment or the Cybersecurity Maturity Model Certification (CMMC) (see subpart 204.7X), except for rare circumstances when a re-assessment may be necessary, such as, but not limited to, when cybersecurity risks, threats, or awareness have changed, requiring a re-assessment to ensure current compliance.]

* * * * *

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

204.7303 Procedures.

[(a)] Follow the procedures relating to safeguarding covered defense information at PGI 204.7303.

[(b) The contracting officer shall verify that the summary level score of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old, unless a lesser time is specified in the solicitation) (see 252.204-70XX) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted in Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/), prior to—

(1) Awarding a contract, task order, or delivery order to an offeror or contractor that is required to implement NIST SP 800-171 in accordance with the clause at 252.204-7012; or

(2) Exercising an option period or extending the period of performance on a contract, task order, or delivery order with a contractor that is that is required to implement the NIST SP 800-171 in accordance with the clause at 252.204-7012.]

* * * * *

204.7304 Solicitation provision[s] and contract clauses.

* * * * *

[(d) Use the provision at 252.204-70XX, Notice of NIST SP 800-171 DoD Assessment Requirements, in all solicitations, including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of commercially available off-the-shelf (COTS) items.

(e) Use the clause at 252.204-70YY, NIST SP 800-171 DoD Assessment Requirements, in all solicitations and contracts, task orders, or delivery orders, including those using FAR part 12 procedures for the acquisition of commercial items, except for those that are solely for the acquisition of COTS items.]

* * * * *

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

[SUBPART 204.7X –CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC)

204.7X00 Scope of subpart.

(a) This subpart prescribes policies and procedures for including the Cybersecurity Maturity Model Certification (CMMC) level requirements in DoD contracts. CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see https://www.acq.osd.mil/cmmc/index.html).

(b) This subpart does not abrogate any other requirements regarding contractor physical, personnel, information, technical, or general administrative security operations governing the protection of unclassified information, nor does it affect requirements of the National Industrial Security Program.

204.7X01 Policy.

(a) The contracting officer shall include in the solicitation the required CMMC level, if provided by the requiring activity. Contracting officers shall not award a contract, task order, or delivery order to an offeror that does not have a current (i.e., not more than 3 years old) CMMC certificate at the level required by the solicitation.

(b) Contractors are required to achieve, at time of award, aCMMC certificate at the level specified in the solicitation. Contractors are required to maintain a current (i.e., not more than 3 years old) CMMC certificate at the specified level, if required by the statement of work or requirement document, throughout the life of the contract, task order, or delivery order. Contracting officers shall not exercise an option period or extend the period of performance on a contract, task order, or delivery order, unless the contract has a current (i.e., not more than 3 years old) CMMC certificate at the level required by the contract, task order, or delivery order.

(c) The CMMC assessments shall not duplicate efforts from any other comparable DoD assessment, except for rare circumstances when a re-assessment may be necessary such as, but not limited to

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

when there are indications of issues with cybersecurity and/or compliance with CMMC requirements.

204.7X02 Procedures.

(a) When a requiring activity identifies a requirement for a contract, task order, or delivery order to include a specific CMMC level, the contracting officer shall not—

(1) Award to an offeror that does not have a CMMC certificate at the level required by the solicitation; or

(2) Exercise an option or extend any period of performance on a contract, task order, or delivery order unless the contractor has a CMMC certificate at the level required by the contract.

(b) Contracting officers shall use Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/) to verify an offeror or contractor's CMMC level.

204.7X03 Contract clause.

Use the clause at 252.204-70ZZ, Cybersecurity Maturity Model Certification Requirements, as follows:

(a) Until September 30, 2025, in solicitations 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 commercially available off-the-shelf (COTS) items, if the requirement document or statement of work requires a contractor to have a specific CMMC level. In order to implement a phased rollout of CMMC, inclusion of a CMMC requirement in a solicitation during this time period must be approved by OUSD(A&S).

(b) On or after October 1, 2025, in all solicitations 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.]

PART 212—ACQUISITION OF COMMERCIAL ITEMS

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

* * * * *

SUBPART 212.301—SOLICITATION PROVISIONS AND CONTRACT CLAUSES FOR THE ACQUISITION OF COMMERCIAL ITEMS

212.301 Solicitation provisions and contract clauses for acquisition of commercial items.

* * * * *

(f) The following additional provisions and clauses apply to DoD solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items. If the offeror has completed any of the following provisions listed in this paragraph electronically as part of its annual representations and certifications at https://www.acquisition.gov, the contracting officer shall consider this information instead of requiring the offeror to complete these provisions for a particular solicitation.

* * * * *

(ii) Part 204—Administrative and Information Matters.

* * * * *

[(G) Use the provision at 252.204-70XX, Notice of NIST SP 800-171 DoD Assessment Requirements, as prescribed in 204.7304(d).

(H) Use the clause at 252.204-70YY, NIST SP 800-171 DoD Assessment Requirements, as prescribed in 204.7304(e).

(I) Use the clause at 252.204-70ZZ, Cybersecurity Maturity Model Certification Requirements, as prescribed in 204.7X03(a) and (b).]

* * * * *

PART 217—SPECIAL CONTRACTING METHODS

* * * * *

SUBPART 217.2—OPTIONS

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

* * * * *

217.207 Exercise of options.

* * * * *

(c) In addition to the requirements at FAR 17.207(c), exercise an option only after**[:**

(1) D]~~d~~etermining that the contractor's record in the System for Award Management database is active and the contractor's Data Universal Numbering System (DUNS) number, Commercial and Government Entity (CAGE) code, name, and physical address are accurately reflected in the contract document. * * *

[(2) Verifying in the Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/) that—

(i) The summary level score of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old, unless a lesser time is specified in the solicitation) for each covered contractor information system that is relevant to an offer, contract, task order, or delivery order are posted (see 204.7303).

(ii) The contractor has a CMMC certificate at the level required by the contract, and that it is current (i.e., not more than 3 years old) (see 204.7X02).

* * * * *

PART 252—SOLICITATION PROVISIONS AND CONTRACT CLAUSES

* * * * *

SUBPART 252.2—TEXT OF PROVISIONS AND CLAUSES

* * * * *

[252.204-70XX Notice of NIST SP 800-171 DoD Assessment Requirements.

As prescribed in 204.7304(d), use the following provision:

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

NOTICE OF NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (DATE)

(a) *Definitions*.

"Basic Assessment", "Medium Assessment", and "High Assessment" have the meaning given in the clause 252.204-70YY, NIST SP 800-171 DoD Assessments.

"Covered contractor information system" has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this solicitation.

(b) *Requirement.* In order to be considered for award, if the Offeror is required to implement NIST SP 800-171, the Offeror shall have a current assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) (see 252.204-70YY) for each covered contractor information system that is relevant to the offer, contract, task order, or delivery order. The Basic, Medium, and High NIST SP 800-171 DoD Assessments are described in the NIST SP 800-171 DoD Assessment Methodology located at https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html.

(c) *Procedures.*

(1) The Offeror shall verify that summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) are posted in the Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/) for all covered contractor information systems relevant to the offer.

(2) If the Offeror does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the Offeror may conduct and submit a Basic Assessment to webptsmh@navy.mil for posting to SPRS in the format identified in paragraph (d) of this provision.

(d) *Summary level scores.* Summary level scores for all assessments will be posted 30 days post-assessment in SPRS to

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* An Offeror may follow the procedures in paragraph (c)(2) of this provision for posting Basic Assessments to SPRS.

(i) The email shall include the following information:

(A) Cybersecurity standard assessed (e.g., NIST SP 800-171 Rev 1).

(B) Organization conducting the assessment (e.g., Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan;

(*2*) A brief description of the system security plan architecture, if more than one plan exists;

(D) Date the assessment was completed;.

(E) Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement); and

(F) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(ii) If multiple system security plans are addressed in the email described at paragraph (d)(1)(i) of this section, the Offeror shall use the following format for the report:

System Security Plan	CAGE Codes supported	Brief description of the plan	Date of assessment	Total Score	Date score of 110 will

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

	by this plan	architecture			achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system assessed:

(i) The standard assessed (e.g., NIST SP 800-171 Rev 1).

(ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, i.e., medium or high. Summary level score (e.g., 105 out of 110, not the individual value assigned for each requirement).

(vi) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(3) *Accessibility.*

(i) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(ii) Authorized representatives of the Offeror for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

(iii) A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this section. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(End of provision)

252.204-70YY NIST SP 800-171 DoD Assessment Requirements.

As prescribed in 204.7304(e), use the following clause:

NIST SP 800-171 DOD ASSESSMENT REQUIREMENTS (DATE)

(a) *Definitions.*

"Basic Assessment" means a contractor's self-assessment of the contractor's implementation of NIST SP 800-171 that—

(1) Is based on the Contractor's review of their system security plan(s) associated with covered contractor information system(s);

(2) Is conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology; and

(3) Results in a confidence level of "Low" in the resulting score, because it is a self-generated score.

"Covered contractor information system" has the meaning given in the clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

"High Assessment" means an assessment that is conducted by Government personnel using NIST SP 800-171A, Assessing Security Requirements for Controlled Unclassified Information that—

(1) Consists of—

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review;

(iii) 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; and

(iv) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "High" in the resulting score.

"Medium Assessment" means an assessment conducted by the Government that—

(1) Consists of—

(i) A review of a contractor's Basic Assessment;

(ii) A thorough document review;

(iii) Discussions with the contractor to obtain additional information or clarification, as needed; and

(2) Results in a confidence level of "Medium" in the resulting score.

(b) *Applicability.* This clause applies to covered contractor information systems that are required to comply with the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-171, in accordance with Defense Federal Acquisition Regulation System (DFARS) clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, of this contract.

(c) *Requirements.* The Contractor shall provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, as described in NIST SP 800-171 DoD Assessment Methodology at

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, if necessary.

(d) *Procedures.* Summary level scores for all assessments will be posted in the Supplier Performance Risk System (SPRS) (https://www.sprs.csd.disa.mil/) to provide DoD Components visibility into the summary level scores of strategic assessments.

(1) *Basic Assessments.* A contractor may submit, via encrypted email, summary level scores of Basic Assessments conducted in accordance with the NIST SP 800-171 DoD Assessment Methodology to webptsmh@navy.mil for posting to SPRS.

(i) The email shall include the following information:

(A) Version of NIST SP 800-171 against which the assessment was conducted.

(B) Organization conducting the assessment (e.g., Contractor self-assessment).

(C) For each system security plan (security requirement 3.12.4) supporting the performance of a DoD contract—

(*1*) All industry Commercial and Government Entity (CAGE) code(s) associated with the information system(s) addressed by the system security plan;

(*2*) A brief description of the system security plan architecture, if more than one plan exists;

(D) Date the assessment was completed;.

(E) Summary level score (e.g., 95 out of 110, NOT the individual value for each requirement); and

(F) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

(ii) If multiple system security plans are addressed in the email described at paragraph (b)(1)(i) of this section, the Contractor shall use the following format for the report:

System Security Plan	CAGE Codes supported by this plan	Brief description of the plan architecture	Date of assessment	Total Score	Date score of 110 will achieved

(2) *Medium and High Assessments.* DoD will post the following Medium and/or High Assessment summary level scores to SPRS for each system security plan assessed:

(i) The standard assessed (e.g., NIST SP 800-171 Rev 1).

(ii) Organization conducting the assessment, e.g., DCMA, or a specific organization (identified by Department of Defense Activity Address Code (DoDAAC)).

(iii) All industry CAGE code(s) associated with the information system(s) addressed by the system security plan.

(iv) A brief description of the system security plan architecture, if more than one system security plan exists.

(v) Date and level of the assessment, i.e., medium or high. Summary level score (e.g., 105 out of 110, not the individual value assigned for each requirement).

(vi) Date that all requirements are expected to be implemented (i.e., a score of 110 is expected to be achieved) based on information gathered from associated plan(s) of action developed in accordance with NIST SP 800-171.

(e) *Rebuttals*.

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

(1) DoD will provide Medium and High Assessment summary level scores to the Contractor and offer the opportunity for rebuttal and adjudication of assessment summary level scores prior to posting the summary level scores to SPRS (see SPRS User's Guide https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf).

(2) Upon completion of each assessment, the contractor has 14 business days to provide additional information to demonstrate that they meet any security requirements not observed by the assessment team or to rebut the findings that may be of question.

(f) *Accessibility.*

(1) Assessment summary level scores posted in SPRS are available to DoD personnel, and are protected, in accordance with the standards set forth in DoD Instruction 5000.79, Defense-wide Sharing and Use of Supplier and Product Performance Information (PI).

(2) Authorized representatives of the Contractor for which the assessment was conducted may access SPRS to view their own summary level scores, in accordance with the SPRS Software User's Guide for Awardees/Contractors available at https://www.sprs.csd.disa.mil/pdf/SPRS_Awardee.pdf.

(3) A High NIST SP 800-171 DoD Assessment may result in documentation in addition to that listed in this clause. DoD will retain and protect any such documentation as "Controlled Unclassified Information (CUI)" and intended for internal DoD use only. The information will be protected against unauthorized use and release, including through the exercise of applicable exemptions under the Freedom of Information Act (e.g., Exemption 4 covers trade secrets and commercial or financial information obtained from a contractor that is privileged or confidential).

(g) *Subcontracts.*

(1) The Contractor shall insert the substance of this clause, including this paragraph (g), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items (excluding COTS items).

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

(2) The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment, as described in https://www.acq.osd.mil/dpap/pdi/cyber/strategically_assessing_contractor_implementation_of_NIST_SP_800-171.html, for all covered contractor information systems relevant to its offer that are not part of an information technology service or system operated on behalf of the Government.

(3) If a subcontractor does not have summary level scores of a current NIST SP 800-171 DoD Assessment (i.e., not more than 3 years old unless a lesser time is specified in the solicitation) posted in SPRS, the subcontractor may conduct and submit a Basic Assessment, in accordance with the NIST SP 800-171 DoD Assessment Methodology, to webptsmh@navy.mil for posting to SPRS along with the information required by paragraph (d) of this clause.

(End of clause)

252.204-70ZZ Contractor Compliance with the Cybersecurity Maturity Model Certification Level Requirement.

As prescribed in 204.7X03(a) and (b), insert the following clause:

CONTRACTOR COMPLIANCE WITH THE CYBERSECURITY MATURITY MODEL CERTIFICATION LEVEL REQUIREMENT (DATE)

(a) *Scope.* The Cybersecurity Maturity Model Certification (CMMC) CMMC is a framework that measures a contractor's cybersecurity maturity to include the implementation of cybersecurity practices and institutionalization of processes (see https://www.acq.osd.mil/cmmc/index.html).

(b) *Requirements.* The Contractor shall have a current (i.e. not older than 3 years) CMMC certificate at the CMMC level required by this contract and maintain the CMMC certificate at the required level for the duration of the contract.

(c) *Subcontracts.* The Contractor shall—

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.
ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.

(1) Insert the substance of this clause, including this paragraph (c), in all subcontracts and other contractual instruments, including subcontracts for the acquisition of commercial items, excluding commercially available off-the-shelf items; and

(2) Prior to awarding to a subcontractor, ensure that the subcontractor 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 subcontractor.

(End of clause)]

* * * * *

ATTENTION: THIS IS A CONFIDENTIAL, DELIBERATIVE, AND PRE-DECISIONAL DEFENSE ACQUISITION REGULATIONS SYSTEM DOCUMENT, PROTECTED FROM UNAUTHORIZED DISCLOSURE PURSUANT TO THE FREEDOM OF INFORMATION ACT AND OTHER LEGAL AUTHORITIES. THIS DOCUMENT SHALL NOT BE DISTRIBUTED OUTSIDE AUTHORIZED RULEMAKING CHANNELS WITHOUT THE PRIOR APPROVAL OF A REPRESENTATIVE OF THE DEFENSE ACQUISITION REGULATIONS SYSTEM. IF YOU HAVE RECEIVED THIS DOCUMENT IN ERROR, YOU MAY NOT READ, COPY, DISTRIBUTE, OR USE THE DOCUMENT OR INFORMATION CONTAINED THEREIN. FURTHERMORE, YOU MUST IMMEDIATELY NOTIFY THE SENDER BY REPLY EMAIL OR OTHER MEANS AND THEN DELETE OR DESTROY ALL COPIES OF THE DOCUMENT.

ANY DISTRIBUTION OF THIS DOCUMENT MUST CONTAIN THIS LEGEND.