Supervisory Control and Data Acquisition (SCADA) means a generic name for a computerized system that is capable of gathering and processing data and applying operational controls over long distances. Typical uses include power transmission and distribution and pipeline systems. SCADA was designed for the unique communication challenges (*e.g.*, delays, data integrity) posed by the various media that must be used, such as phone lines, microwave, and satellite. Usually shared rather than dedicated, as defined in NIST SP 800–82r3 (incorporated by reference, see §170.2).

System Security Plan (SSP) means the formal document that provides an overview of the security requirements for an information system or an information security program and describes the security controls in place or planned for meeting those requirements. The system security plan describes the system components that are included within the system, the environment in which the system operates, how the security requirements are implemented, and the relationships with or connections to other systems, as defined in NIST SP 800–53 R5 (incorporated by reference, see §170.2).

Temporary deficiency means a condition where remediation of a discovered deficiency is feasible, and a known fix is available or is in process. The deficiency must be documented in an operational plan of action. A temporary deficiency is not based on an 'in progress' initial implementation of a CMMC security requirement but arises after implementation. A temporary deficiency may apply during the initial implementation of a security requirement if, during roll-out, specific issues with a very limited subset of equipment is discovered that must be separately addressed. There is no standard duration for which a temporary deficiency may be active. For example, FIPS-validated cryptography that requires a patch and the patched version is no longer the validated version may be a temporary deficiency. (CMMC-custom term)

Test Equipment means hardware and/or associated IT components used in the testing of products, system components, and contract deliverables. (CMMC-custom term)

User means an individual, or (system) process acting on behalf of an individual, authorized to access a system, as defined in NIST SP 800–53 R5 (incorporated by reference, see §170.2).

§170.5 Policy.

(a) Protection of FCI and CUI on contractor information systems is of paramount importance to the DoD and can directly impact its ability to successfully conduct essential missions and functions. It is DoD policy that defense contractors and subcontractors shall be required to safeguard FCI and CUI that is processed, stored, or transmitted on contractor information systems by applying specified security requirements. In addition, defense contractors and subcontractors may be required to implement additional safeguards defined in NIST SP 800–172 Feb2021 (incorporated by reference, see §170.2), implementing DoD specified parameters to meet CMMC Level 3 security requirements (see table 1 to §170.14(c)(4)). These additional requirements are necessary to protect CUI being processed, stored, or transmitted in contractor information systems, when designated by a requirement for CMMC Status of Level 3 (DIBCAC) as defined by a DoD program manager or requiring activity. In general, the Department will identify a requirement for a CMMC Status of Level 3 (DIBCAC) for solicitations and resulting contracts supporting its most critical programs and technologies.

(b) Program managers and requiring activities are responsible for identifying the CMMC Status that will apply to a procurement. Selection of the applicable CMMC Status will be based on factors including but not limited to:

(1) Criticality of the associated mission capability;

(2) Type of acquisition program or technology;

(3) Threat of loss of the FCI or CUI to be shared or generated in relation to the effort;

(4) Impacts from exploitation of information security deficiencies; and

(5) Other relevant policies and factors, including Milestone Decision Authority guidance.

(c) In accordance with the implementation plan described in §170.3, CMMC

Program requirements will apply to new DoD solicitations and contracts, and shall flow down to subcontractors who will process, store, or transmit FCI or CUI in performance of the subcontract, as described in §170.23.

(d) In very limited circumstances, and in accordance with all applicable policies, procedures, and requirements, a Service Acquisition Executive or Component Acquisition Executive in the DoD, or as delegated, may elect to waive inclusion of CMMC Program requirements in a solicitation or contract. In such cases, contractors and subcontractors will remain obligated to comply with all applicable cybersecurity and information security requirements.

(e) The CMMC Program does not alter any separately applicable requirements to protect FCI or CUI, including those requirements in accordance with 48 CFR 52.204–21, *Basic Safeguarding of Covered Contractor Information Systems*, or covered defense information in accordance with 48 CFR 252.204–7012, *Safeguarding Covered Defense Information and Cyber Incident Reporting*, or any other applicable information protection requirements. The CMMC Program provides a means of verifying implementation of the security requirements set forth in 48 CFR 52.204–21, NIST SP 800–171 R2, and NIST SP 800–172 Feb2021, as applicable.

Subpart B—Government Roles and Responsibilities.

§170.6 CMMC PMO.

(a) The Office of the Department of Defense Chief Information Officer (DoD CIO) Office of the Deputy CIO for Cybersecurity (DoD CIO(CS)) provides oversight of the CMMC Program and is responsible for establishing CMMC assessment, accreditation, and training requirements as well as developing and updating CMMC Program policies and implementing guidance.

(b) The CMMC PMO is responsible for monitoring the CMMC AB's performance of roles assigned in this rule and acting as necessary to address problems pertaining to effective performance.

(c) The CMMC PMO retains, on behalf of the DoD CIO(CS), the prerogative to review decisions of the CMMC Accreditation Body as part of its oversight of the CMMC program and evaluate any alleged conflicts of interest purported to influence the CMMC Accreditation Body's objectivity.

(d) The CMMC PMO is responsible for sponsoring necessary DCSA activities including FOCI risk assessment and Tier 3 security background investigations for the CMMC Ecosystem members as specified in §§170.8(b)(4) and (5), 170.9(b)(3) through (5), 170.11(b)(3) and (4), and 170.13(b)(3) and (4).

(e) The CMMC PMO is responsible for investigating and acting upon indications that an active CMMC Status has been called into question. Indications that may trigger investigative evaluations include, but are not limited to, reports from the CMMC Accreditation Body, a C3PAO, or anyone knowledgeable of the security processes and activities of the OSA. Investigative evaluations include, but are not limited to, reviewing pertinent assessment information, and exercising the right to conduct a DCMA DIBCAC assessment of the OSA, as provided for under the 48 CFR 252.204–7020.

(f) If a subsequent DCMA DIBCAC assessment shows that adherence to the provisions of this rule and the required CMMC Status have not been achieved or maintained, the DIBCAC results will take precedence over any pre-existing CMMC Status recorded in SPRS, or its successor capability. The DoD will update SPRS to reflect that the OSA is out of compliance and does not meet DoD CMMC requirements. If the OSA is working on an active contract requiring CMMC compliance, then standard contractual remedies will apply.

§170.7 DCMA DIBCAC.

(a) DCMA DIBCAC assessors in support of the CMMC Program will:

(1) Complete CMMC Level 2 and Level 3 training.

(2) Conduct Level 3 certification assessments and upload assessment results into the CMMC instantiation of eMASS, or its successor capability.

(3) Issue Certificates of CMMC Status resulting from Level 3 certification assessments.

(4) Conduct Level 2 certification assessments of the Accreditation Body