

## 204.7300

### 204.7300 Scope.

(a) This subpart applies to contracts and subcontracts requiring safeguarding of unclassified controlled technical information resident on or transiting through contractor unclassified information systems.

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

### 204.7301 Definitions.

As used in this subpart—

*Adequate security* means protective measures that are commensurate with the consequences and probability of loss, misuse, or unauthorized access to, or modification of information.

*Controlled technical information* means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination. Controlled technical information is to be marked with one of the distribution statements B through F, in accordance with DoD Instruction 5230.24, Distribution Statements on Technical Documents. The term does not include information that is lawfully publicly available without restrictions.

*Cyber incident* means actions taken through the use of computer networks that result in an actual or potentially adverse effect on an information system and/or the information residing therein.

*Technical information* means technical data or computer software, as those terms are defined in the clause at DFARS 252.227-7013, Rights in Technical Data—Non Commercial Items, regardless of whether or not the clause is incorporated in this solicitation or contract. Examples of technical information include research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information,

## 48 CFR Ch. 2 (10-1-14 Edition)

and computer software executable code and source code.

### 204.7302 Policy.

(a) DoD and its contractors and subcontractors will provide adequate security to safeguard unclassified controlled technical information on their unclassified information systems from unauthorized access and disclosure.

(b) When safeguarding is applied to controlled technical information resident on or transiting contractor unclassified information systems—

(1) Contractors must report to DoD certain cyber incidents that affect unclassified controlled technical information resident on or transiting contractor unclassified information systems. Detailed reporting criteria and requirements are set forth in the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information.

(2) A cyber incident that is properly reported by the contractor shall not, by itself, be interpreted under this clause as evidence that the contractor has failed to provide adequate information safeguards for unclassified controlled technical information, or has otherwise failed to meet the requirements of the clause at 252.204-7012. When a cyber incident is reported, the contracting officer shall consult with a security manager of the requiring activity prior to assessing contractor compliance. The contracting officer shall consider such cyber incidents in the context of an overall assessment of the contractor's compliance with the requirements of the clause at 252.204-7012.

### 204.7303 Contract clause.

Use the clause at 252.204-7012, Safeguarding of Unclassified Controlled Technical Information, in all solicitations and contracts, including solicitations and contracts using FAR part 12 procedures for the acquisition of commercial items.