

SUBPART 239.71--SECURITY AND PRIVACY FOR COMPUTER SYSTEMS

(Revised June 25, 2004)

239.7100 Scope of subpart.

This subpart includes information assurance and Privacy Act considerations. Information assurance requirements are in addition to provisions concerning protection of privacy of individuals (see FAR Subpart 24.1).

239.7101 Definition.

“Information assurance,” as used in this subpart, means measures that protect and defend information, that is entered, processed, transmitted, stored, retrieved, displayed, or destroyed, and information systems, by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for the restoration of information systems by incorporating protection, detection, and reaction capabilities.

239.7102 Policy and responsibilities.

239.7102-1 General.

(a) Agencies shall ensure that information assurance is provided for information technology in accordance with current policies, procedures, and statutes, to include—

- (1) The National Security Act;
- (2) The Clinger-Cohen Act;
- (3) National Security Telecommunications and Information Systems Security Policy No. 11;
- (4) Federal Information Processing Standards;
- (5) DoD Directive 8500.1, Information Assurance; and
- (6) DoD Instruction 8500.2, Information Assurance Implementation.

(b) For all acquisitions, the requiring activity is responsible for providing to the contracting officer—

- (1) Statements of work, specifications, or statements of objectives that meet information assurance requirements as specified in paragraph (a) of this subsection;
- (2) Inspection and acceptance contract requirements; and
- (3) A determination as to whether the information technology requires protection against compromising emanations.

239.7102-2 Compromising emanations—TEMPEST or other standard.

For acquisitions requiring information assurance against compromising emanations, the requiring activity is responsible for providing to the contracting officer—

Defense Federal Acquisition Regulation Supplement

Part 239—Acquisition of Information Technology

(a) The required protections, i.e., an established National TEMPEST standard (e.g., NACSEM 5100, NACSIM 5100A) or a standard used by other authority;

(b) The required identification markings to include markings for TEMPEST or other standard, certified equipment (especially if to be reused);

(c) Inspection and acceptance requirements addressing the validation of compliance with TEMPEST or other standards; and

(d) A date through which the accreditation is considered current for purposes of the proposed contract.

239.7103 Contract clause.

Use the clause at 252.239-7000, Protection Against Compromising Emanations, in solicitations and contracts involving information technology that requires protection against compromising emanations.