be incorporated in the contract, to ensure the continuation of these services in crisis situations. Contracting officers shall consult with a functional manager to assess the sufficiency of the contractor-provided written plan. Contractors will activate such plans only during periods of crisis, as authorized by the contracting officer, who does so at the direction of the appropriate functional commander or civilian equivalent.

(c) The contracting officer shall follow the procedures at 252.237-7023(b)(20)(C) in preparing an acquisition plan.

237.7603 Solicitation provision and contract clause.

(a) Use the clause at 252.237–7023, Continuation of Essential Contractor Services in all solicitations and contracts for services that are in support of mission-essential functions.

(b) Use the provision at 252.237–7024, Notice of Continuation of Essential Contractor Services in all solicitations for services that include the clause 252.237–7023.

237.7603 Solicitation provision and contract clause.

(a) Use the clause at 252.237–7023, Continuation of Essential Contractor Services in all solicitations and contracts for services that are in support of mission-essential functions.

(b) Use the provision at 252.237–7024, Notice of Continuation of Essential Contractor Services in all solicitations for services that include the clause 252.237–7023.

PART 239—ACQUISITION OF INFORMATION TECHNOLOGY

Subpart 239.1—General

Sec. 239.101 Policy.

Subpart 239.70—Exchange or Sale of Information Technology

239.7001 Policy.

Subpart 239.71—Security and Privacy for Computer Systems

239.7100 Scope of subpart.

239.7101 Definition.

239.7102 Policy and responsibilities.

239.7102–1 General.

239.7102–2 Compromising emanations—TEMPEST or other standard.

239.7102–3 Information assurance contractor training and certification.

239.7103 Contract clauses.

Subpart 239.72—Standards

239.7201 Solicitation requirements.

Subpart 239.73 [Reserved]
Defense Acquisition Regulations System, DOD

239.7102–3

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;
(6) DoD Instruction 8500.2, Information Assurance Implementation;
(7) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management; and
(8) DoD Manual 8570.01–M, Information Assurance Workforce Improvement Program.

(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.