

Subpart 4.3—Paper Documents

4.300 Scope of subpart.

This subpart provides policies and procedures on contractor-submitted paper documents.

[65 FR 28493, May 31, 1995]

4.301 Definition.

Printed or copied double-sided, as used in this subpart, means printing or reproducing a document so that information is on both sides of a sheet of paper.

[65 FR 36017, June 6, 2000]

4.302 Policy.

When electronic commerce methods (see 4.502) are not being used, a contractor should submit paper documents to the Government relating to an acquisition printed or copied double-sided on recycled paper whenever practicable. If the contractor cannot print or copy double-sided, it should print or copy single-sided on recycled paper.

[65 FR 36017, June 6, 2000]

4.303 Contract clause.

Insert the clause at 52.204-4, Printed or Copied Double-Sided on Recycled Paper, in solicitations and contracts that exceed the simplified acquisition threshold.

[65 FR 36017, June 6, 2000]

Subpart 4.4—Safeguarding Classified Information Within Industry

4.401 [Reserved]

4.402 General.

(a) Executive Order 12829, January 6, 1993 (58 FR 3479, January 8, 1993), entitled "National Industrial Security Program" (NISP), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829 amends Executive Order 10865, February 20, 1960 (25 FR 1583, February 25, 1960), entitled "Safeguarding Classified Information Within Industry," as amended by Executive

Order 10909, January 17, 1961 (26 FR 508, January 20, 1961).

(b) The National Industrial Security Program Operating Manual (NISPOM) incorporates the requirements of these Executive Orders. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of Central Intelligence, is responsible for issuance and maintenance of this Manual. The following DOD publications implement the program:

(1) *National Industrial Security Program Operating Manual* (NISPOM) (DOD 5220.22-M).

(2) *Industrial Security Regulation* (ISR) (DOD 5220.22-R).

(c) Procedures for the protection of information relating to foreign classified contracts awarded to U.S. industry, and instructions for the protection of U.S. information relating to classified contracts awarded to foreign firms, are prescribed in Chapter 10 of the NISPOM.

(d) Part 27, Patents, Data, and Copyrights, contains policy and procedures for safeguarding classified information in patent applications and patents.

[48 FR 42113, Sept. 19, 1983, as amended at 61 FR 31617, June 20, 1996]

4.403 Responsibilities of contracting officers.

(a) *Presolicitation phase*. Contracting officers shall review all proposed solicitations to determine whether access to classified information may be required by offerors, or by a contractor during contract performance.

(1) If access to classified information of another agency may be required, the contracting officer shall—

(i) Determine if the agency is covered by the NISP; and

(ii) Follow that agency's procedures for determining the security clearances of firms to be solicited.

(2) If the classified information required is from the contracting officer's agency, the contracting officer shall follow agency procedures.

(b) *Solicitation phase*. Contracting officers shall—

(1) Ensure that the classified acquisition is conducted as required by the

Federal Acquisition Regulation

4.502

NISP or agency procedures, as appropriate; and

(2) Include (i) an appropriate Security Requirements clause in the solicitation (see 4.404), and (ii) as appropriate, in solicitations and contracts when the contract may require access to classified information, a requirement for security safeguards in addition to those provided in the clause (52.204-2, Security Requirements).

(c) *Award phase.* Contracting officers shall inform contractors and subcontractors of the security classifications and requirements assigned to the various documents, materials, tasks, subcontracts, and components of the classified contract as follows:

(1) Agencies covered by the NISP shall use the Contract Security Classification Specification, DD Form 254. The contracting officer, or authorized representative, is the approving official for the form and shall ensure that it is prepared and distributed in accordance with the ISR.

(2) Contracting officers in agencies not covered by the NISP shall follow agency procedures.

[48 FR 42113, Sept. 19, 1983, as amended at 61 FR 31617, June 20, 1996]

4.404 Contract clause.

(a) The contracting officer shall insert the clause at 52.204-2, Security Requirements, in solicitations and contracts when the contract may require access to classified information, unless the conditions specified in paragraph (d) below apply.

(b) If a cost contract (see 16.302) for research and development with an educational institution is contemplated, the contracting officer shall use the clause with its Alternate I.

(c) If a construction or architect-engineer contract where employee identification is required for security reasons is contemplated, the contracting officer shall use the clause with its Alternate II.

(d) If the contracting agency is not covered by the NISP and has prescribed a clause and alternates that are substantially the same as those at 52.204-2, the contracting officer shall use the

agency-prescribed clause as required by agency procedures.

[48 FR 42113, Sept. 19, 1983, as amended at 61 FR 31617, June 20, 1996]

Subpart 4.5—Electronic Commerce in Contracting

AUTHORITY: 40 U.S.C. 486(c); 10 U.S.C. chapter 137; and 42 U.S.C. 2473(c).

SOURCE: 63 FR 58592, Oct. 30, 1998, unless otherwise noted.

4.500 Scope of subpart.

This subpart provides policy and procedures for the establishment and use of electronic commerce in Federal acquisition as required by Section 30 of the Office of Federal Procurement Policy (OFPP) Act (41 U.S.C. 426).

4.501 [Reserved]

4.502 Policy.

(a) The Federal Government shall use electronic commerce whenever practicable or cost-effective. The use of terms commonly associated with paper transactions (e.g., “copy,” “document,” “page,” “printed,” “sealed envelope,” and “stamped”) shall not be interpreted to restrict the use of electronic commerce. Contracting officers may supplement electronic transactions by using other media to meet the requirements of any contract action governed by the FAR (e.g., transmit hard copy of drawings).

(b) Agencies may exercise broad discretion in selecting the hardware and software that will be used in conducting electronic commerce. However, as required by Section 30 of the OFPP Act (41 U.S.C. 426), the head of each agency, after consulting with the Administrator of OFPP, shall ensure that systems, technologies, procedures, and processes used by the agency to conduct electronic commerce—

(1) Are implemented uniformly throughout the agency, to the maximum extent practicable;

(2) Are implemented only after considering the full or partial use of existing infrastructures, (e.g., the Federal Acquisition Computer Network (FACNET));