AUTHENTICATED
U.S. GOVERNMENT
INFORMATION
GPO

(3) Changing the scope of agency or geographical coverage of existing schedules; or

(4) Adding or deleting special item numbers, national stock numbers, or revising their description.

(b) Requests should be forwarded to the General Services Administration, Federal Supply Service, Office of Acquisition (FC), Washington, DC 20406.

[48 FR 42368, Sept. 19, 1983, as amended at 54 FR 29282, July 11, 1989; 56 FR 55372, Oct. 25, 1991; 59 FR 53718, Oct. 25, 1994; 62 FR 40237, July 25, 1997]

PART 39—ACQUISITION OF INFORMATION TECHNOLOGY

Sec.
39.000 Scope of part.
39.001 Applicability.
39.002 Definitions.

Subpart 39.1—General

39.101 Policy.
39.102 Management of risk.
39.103 Modular contracting.
39.104 Information technology services.
39.105 Privacy.
39.106 Year 2000 complaints.
39.107 Contract clause.

Subpart 39.2—Electronic and Information Technology

39.201 Scope of subpart.
39.202 Definition.
39.203 Applicability.
39.204 Exceptions.

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

SOURCE: 61 FR 41470, Aug. 8, 1996, unless otherwise noted.

39.000 Scope of part.

This part prescribes acquisition policies and procedures for use in acquiring—

(a) Information technology, including financial management systems, consistent with other parts of this regulation, OMB Circular No. A–127, Financial Management Systems, and OMB Circular No. A–130, Management of Federal Information Resources; and

(b) Electronic and information technology.

[66 FR 20897, Apr. 25, 2001]

39.001 Applicability.

This part applies to the acquisition of information technology by or for the use of agencies except for acquisitions of information technology for national security systems. However, acquisitions of information technology for national security systems shall be conducted in accordance with 40 U.S.C. 11302 with regard to requirements for performance and results-based management; the role of the agency Chief Information Officer in acquisitions; and accountability. These requirements are addressed in OMB Circular No. A–130.

[61 FR 41470, Aug. 8, 1996, as amended at 70 FR 57455, Sept. 30, 2005]

39.002 Definitions.

As used in this part—

Modular contracting means use of one or more contracts to acquire information technology systems in successive, interoperable increments.

National security system means any telecommunications or information system operated by the United States Government, the function, operation, or use of which—

(1) Involves intelligence activities;

(2) Involves cryptologic activities related to national security;

(3) Involves command and control of military forces;

(4) Involves equipment that is an integral part of a weapon or weapons system; or

(5) Is critical to the direct fulfillment of military or intelligence missions. This does not include a system that is to be used for routine administrative and business applications, such as payroll, finance, logistics, and personnel management applications.

Year 2000 compliant with respect to information technology, means that the information technology accurately processes date/time data (including, but not limited to, calculating, comparing, and sequencing) from, into, and between the twentieth and twenty-first centuries, and the years 1999 and 2000 and leap year calculations, to the extent that other information technology, used in combination with the information technology being acquired,

properly exchanges date/time data with it.

[61 FR 41470, Aug. 8, 1996, as amended at 62 FR 274, Jan. 2, 1997; 62 FR 44830, Aug. 22, 1997; 63 FR 9068, Feb. 23, 1998; 66 FR 2133, Jan. 10, 2001]

Subpart 39.1—General

39.101 Policy.

(a) Division A, Section 101(h), Title VI, Section 622 of the Omnibus Appropriations and Authorization Act for Fiscal Year 1999 (Pub. L. 105–277) requires that agencies may not use appropriated funds to acquire information technology that does not comply with 39.106, unless the agency's Chief Information Officer determines that noncompliance with 39.106 is necessary to the function and operation of the agency or the acquisition is required by a contract in effect before October 21, 1998. The Chief Information Officer must send to the Office of Management and Budget a copy of all waivers for forwarding to Congress.

(b) In acquiring information technology, agencies shall identify their requirements pursuant to OMB Circular A–130, including consideration of security of resources, protection of privacy, national security and emergency preparedness, accommodations for individuals with disabilities, and energy efficiency. When developing an acquisition strategy, contracting officers should consider the rapidly changing nature of information technology through market research (see part 10) and the application of technology refreshment techniques.

(c) Agencies must follow OMB Circular A–127, Financial Management Systems, when acquiring financial management systems. Agencies may acquire only core financial management software certified by the Joint Financial Management Improvement Program.

(d) In acquiring information technology, agencies shall include the appropriate information technology security policies and requirements.

[61 FR 41470, Aug. 8, 1996, as amended at 64 FR 32748, June 17, 1999; 64 FR 72446, Dec. 27, 1999; 70 FR 57452, Sept. 30, 2005]

39.102 Management of risk.

(a) Prior to entering into a contract for information technology, an agency should analyze risks, benefits, and costs. (See part 7 for additional information regarding requirements definition.) Reasonable risk taking is appropriate as long as risks are controlled and mitigated. Contracting and program office officials are jointly responsible for assessing, monitoring and controlling risk when selecting projects for investment and during program implementation.

(b) Types of risk may include schedule risk, risk of technical obsolescence, cost risk, risk implicit in a particular contract type, technical feasibility, dependencies between a new project and other projects or systems, the number of simultaneous high risk projects to be monitored, funding availability, and program management risk.

(c) Appropriate techniques should be applied to manage and mitigate risk during the acquisition of information technology. Techniques include, but are not limited to: prudent project management; use of modular contracting; thorough acquisition planning tied to budget planning by the program, finance and contracting offices; continuous collection and evaluation of risk-based assessment data; prototyping prior to implementation; post implementation reviews to determine actual project cost, benefits and returns; and focusing on risks and returns using quantifiable measures.

39.103 Modular contracting.

(a) This section implements Section 5202, Incremental Acquisition of Information Technology, of the Clinger-Cohen Act of 1996 (Public Law 104–106). Modular contracting is intended to reduce program risk and to incentivize contractor performance while meeting the Governments need for timely access to rapidly changing technology. Consistent with the agency's information technology architecture, agencies should, to the maximum extent practicable, use modular contracting to acquire major systems (see 2.101) of information technology. Agencies may also use modular contracting to acquire non-major systems of information technology.