

507.105 Contents of written acquisition plans.

(a) The content prescribed in FAR [7.105](#) shall be used in the preparation of written acquisition plans. Where a particular element described in FAR [7.105](#) does not apply, the acquisition plan should read “not applicable.” The dollar value, complexity (*e.g.*, commercial versus other than a commercial purchase) and method of acquisition (*e.g.*, full and open competition versus task/delivery order) of the supplies and services to be acquired will affect the scope and breadth of the acquisition plan.

(b) FAR [7.106](#) (*major systems*) and FAR [7.107](#) (*consolidation, bundling, or substantial bundling*) shall be addressed in the acquisition plan, if applicable.

(c) For leasehold interests in real property, a modified version of the contents of acquisition plans for leases is utilized.

(d) The requirement for a written acquisition plan may be waived by the appropriate level of an approving official listed in [507.103](#) (b). When the requirement for a written acquisition plan is waived, an oral acquisition plan is still required. The planner must obtain approval for the oral acquisition plan from the approving official.

(e) *Software*. If procuring software, specify the result of any software requirement alternatives analysis that has been completed in accordance with [511.170](#) (e).

(f) *Cyber-supply chain risk management for GSA-funded acquisitions*.

(1) The acquisition planner must discuss the scope of involvement (or planned involvement) of the GSA Chief Information Security Officer (CISO), or representative, as part of the acquisition planning team, to ensure cyber-supply chain risk considerations are addressed on a best effort basis based on availability of resources if the acquisition may involve GSA information systems and any of the following are applicable:

(i) *Hardware Devices*. Hardware devices that connect to the GSA enterprise network (wired or wireless).

(ii) *Critical Software*. Critical software that meets the current definition of Critical Software Under Executive Order (EO) 14028, Improving the Nation’s Cybersecurity, as defined by the National Institute of Standards and Technology (NIST).

(iii) *Federal Information Processing Standard (FIPS) 199 High-Impact Information System*. A high-impact information system could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, or individuals if there was a breach of security resulting in a potential loss of confidentiality, integrity, or availability.

(iv) *FIPS 199 Moderate-Impact Information System*. A moderate-impact information system could be expected to have a serious adverse effect on organizational operations, organizational assets, or individuals if there was a breach of security resulting in a potential loss of confidentiality, integrity, or availability.

(v) *FIPS 199 Low-Impact Information Systems*. Unless [507.105\(f\)\(1\)\(iii\)](#) or (iv) applies, this paragraph (f)(1) does not apply to the acquisition of low-impact information systems.

(2)For any other procurement requiring a written acquisition plan, the acquisition planner should discuss efforts to mitigate risks associated with cyber-supply chain risk management. Efforts and considerations could include:

- (i)Market research efforts (see [510.002\(c\)](#) and (d));
- (ii)Procuring products or services already approved in GSA's Enterprise Architecture Analytics and Reporting (GEAR) system;
- (iii)Procuring products or services with a current GSA IT Assessment and Authorization (A&A, or Authority to Operate (ATO)) or Federal Risk and Authorization Management Program (FedRAMP) Authorization;
- (iv)Considering contracting vehicles that have already evaluated awardees supply chain methods and assurances; or
- (v)Planning efforts with the GSA CISO.

- **507.105-70 Contents of oral acquisition plans.**

Parent topic: [Subpart 507.1 - Acquisition Plans](#)