Acquisition Letter MV-19-04

MEMORANDUM FOR THE GSA ACQUISITION WORKFORCE

FROM: JEFFREY A. KOSES
SENIOR PROCUREMENT EXECUTIVE
OFFICE OF ACQUISITION POLICY (MV)

e-Signed by Jeff Koses
on 2019-01-03

DAVID A. SHIVE
CHIEF INFORMATION OFFICER
OFFICE OF GSA IT (I)

e-Signed by David Shive
on 2019-01-03

SUBJECT: Acquisition Letter - Contract Requirements for GSA Information Systems

1. Purpose.

This memo provides guidance and establishes consistent language for the management of contracts or orders awarded by GSA that may involve GSA information systems. This Acquisition Letter (AL) consolidates and updates guidance in Acquisition Letter (AL) MV-16-01 as part of the effort to streamline and reduce burden on the government workforce and contractors.

More than 30 GSA security and non-security information technology policies, one GSAR provision, and one GSAR clause impacting contractors are streamlined and consolidated into two new Information Technology (IT) acquisition documents identified in Section 8 of this AL.

Eliminating the existing clause and provision as well as consolidating over 30 GSA policies into these two new documents will assist contractor and government employees with understanding and implementing applicable information system requirements as well as strengthen our information systems in accordance with current federal laws and policies.

2. Background.

In order to protect against cybersecurity threats and manage GSA information systems, it is important to ensure that contracts are compliant with Federal security standards and GSA requirements. GSA must provide security and protection for information systems that support the operations and assets of the agency, including those provided or managed by a contractor. Relevant areas that GSA's policies address include:

- Security Requirements
  - External information system;
  - Internal information system;
  - Low impact software as a service;

    - Cloud information system;
    - Mobile application;
- Privacy Protection;
- Controlled Unclassified Information;
- Incident Reporting Requirements;
- Software License Management;
- Telecommunications Policy; and
- Social Media Policy.

3. Deviation.
See Attachment A for the changes in the GSAR text as revised by this AL.

4. Effective Date.
This AL is effective immediately and remains in effect until rescinded or incorporated into the GSAM.

5. Cancellation.
AL MV-16-01 is hereby cancelled.

6. Applicability.
(a) The requirements in Section 8 apply to contracts, actions, or orders that may involve GSA information systems.

(b) The requirements of this AL do not apply to Federal Supply Schedules (FSS), Government-wide Acquisition Contracts (GWACs), or Multi-agency Contracts (MACs) at the master contract level, but may be applicable to actions or orders awarded by GSA under these contracts.

(c) The Product Service Codes (PSCs) listed in Attachment B are most likely to be affected by this AL. These PSCs are not an all-inclusive list. GSA contracts for other types of services outside of these segments may be affected. Accordingly, the GSA Contracting Officer (CO) shall familiarize themselves with the requirements in this AL and the policies referenced in section 8 below, to ensure that security requirements are incorporated as necessary.

7. Definitions.
"GSA information system" means an information system owned or operated by the U.S. General Services Administration or by a contractor or other organization on behalf of the U.S. General Services Administration. GSA information systems include the following types: external information systems, internal information systems, low impact software as a service, cloud information systems, and mobile applications. These are defined as follows:

a. "Cloud Information Systems" mean information systems developed using cloud computing. Cloud computing is a model for enabling ubiquitous, convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and

services) that can be rapidly provisioned and released with minimal management effort or service provider interaction. Cloud information systems include Infrastructure as a Service (IaaS), Platform as a Service (PaaS), or Software as a Service (SaaS).

b. "External Information Systems" mean information systems that reside in contractor facilities and typically do not connect to the GSA network. External information systems may be government owned and contractor operated or contractor owned and operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
c. "Internal Information Systems" mean information systems that reside on premise in GSA facilities AND directly connect to the GSA network. Internal systems are operated on behalf of GSA or the Federal Government (when GSA is the managing agency).
d. "Low Impact Software as a Service (LiSaaS) Systems" mean cloud applications that are implemented for a limited duration, considered low impact and would cause limited harm to GSA, and cost less than $100,000 to deploy.
e. "Mobile Application" means a type of application software designed to run on a mobile device, such as a smartphone or tablet computer.

"Information system" means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

8. Requirements.

(a) Except as described in Section 9, the CO shall incorporate the applicable sections or complete version of the following policies in the Statement of Work, or equivalent, for any procurement that may involve GSA information systems.

(i) *CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements.* The CO shall use CIO 09-48 in new contracts in lieu of both of the following:

(A) GSAR Provision 552.239-70 (Information Technology Security Plan and Security Authorization)

(B) GSAR Clause 552.239-71 (Security Requirements for Unclassified Information Technology Resources)

(ii) *CIO 12-2018, IT Policy Requirements Guide*.

(b) The CO shall coordinate with GSA IT when developing a Statement of Work, or equivalent and identify when these policies apply in the Security Considerations section of the acquisition plan. COs can contact vmo@gsa.gov to identify the GSA IT representative for requirements development coordination and acquisition plan approval. All applicable pre-award solicitations shall be submitted to IS-Contracts-Review@gsa.gov for GSA IT review and approval.

(c) For any procurements that may involve access to classified information or a classified information system, see GSAM 504.4 for additional requirements.

(d) The CO or Contracting Officer's Representative (COR) shall validate that all applicable contractor submissions meet contract requirements (e.g. statement of work, contractor's accepted proposal) and are provided by the contractor in accordance with the contract schedule. The CO or COR shall coordinate with GSA IT, specifically the GSA Information System Security Officer (ISSO) and/or Information System Security Manager (ISSM), as needed in determining contractor compliance. GSA ISSO/ISSMs are identified on the EA Analytics and Reporting (GEAR) portal at https://ea.gsa.gov/#!/FISMA_POC.

(e) The CIO policies, an FAQ webpage, and GSA IT points of contact are available on the Acquisition Portal at https://insite.gsa.gov/itprocurement.

9. Waiver Process.

(a) In cases where it is not cost effective or where it is unreasonably burdensome to include the applicable requirements from Section 8 of this AL in a procurement, the CO shall demonstrate in writing that the cost or practicality to include the requirement is unreasonably high or cumbersome. In such cases, a waiver may be granted by the acquisition approving official in accordance with the thresholds listed at GSAM 507.105(c) and in coordination with the GSA Chief Information Security Officer (CISO) and the Authorizing Official (AO) for the information system. All waivers shall be submitted to IS-Contracts-Review@gsa.gov for GSA CISO review and approval. GSA AOs for information systems are identified on the EA Analytics and Reporting (GEAR) portal at https://ea.gsa.gov/#!/FISMA_POC.

(b) The CO should limit the scope of waiver requests to only the requirements for which clear and convincing rationale can be provided to demonstrate that incorporation and implementation of the requirements into a contract is cost prohibitive or impracticable due to the unique circumstances of that particular procurement.

(c) The waiver request must provide the following information-

i. The description of the procurement and GSA information system;
ii. Identification of requirements requested for waiver;
iii. Sufficient justification for why the requirements should be waived; and
iv. Any residual risks that will be encountered by waiving the requirements.

(d) Further details about the waiver process and the waiver template (Attachment C) are located on the Acquisition Portal at https://insite.gsa.gov/itprocurement. Waivers must be documented in the contract file.

10. Point of Contact.

Any questions regarding the content of this Letter may be directed to Mr. Kevin Funk, General Services Acquisition Policy Division, by phone at 202-357-5805 or by email at kevin.funk@gsa.gov. Questions regarding GSA IT policies and requirements may be directed to the GSA IT point of contact identified on the Acquisition Portal at https://insite.gsa.gov/itprocurement.

11. Attachments

- Attachment A – GSAR Text
- Attachment B – Product Service Codes
- Attachment C – GSA Information System Contract Waiver Request Template

ATTACHMENT A
GSAR Text

GSAR Baseline: Change 94 and 95 effective 10/09/2018

- **Additions to baseline made by proposed rule are indicated by [bold text in brackets]**
- **Deletions to baseline made by proposed rule are indicated by strikethroughs**
- **Five asterisks (* * * * *) indicate that there are no revisions between the preceding and following sections**
- **Three asterisks (* * *) indicate that there are no revisions between the material shown within a subsection**

~~**539.7002 Solicitation provisions and contract clauses.**~~

~~(a) The contracting officer shall insert the provision at 552.239-70, Information Technology Security Plan and Security Authorization, in solicitations that include information technology supplies, services or systems in which the contractor will have physical or electronic access to government information that directly supports the mission of GSA.~~

~~(b) The contracting officer shall insert the clause at 552.239-71, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts containing the provision at 552.239-70. The provision and clause shall not be inserted in solicitations and contracts for personal services with individuals.~~

~~**552.239-70 Information Technology Security Plan and Security Authorization.**~~

~~As prescribed in 539.7002(a), insert the following provision:~~

~~Information Technology Security Plan and Security Authorization (Jun 2011)~~

~~All offers/bids submitted in response to this solicitation must address the approach for completing the security plan and certification and security authorization requirements as required by the clause at 552.239-71, Security Requirements for Unclassified Information Technology Resources.~~

~~(End of provision)~~

~~**552.239-71 Security Requirements for Unclassified Information Technology Resources.**~~

~~As prescribed in 539.7002(b), insert the following clause:~~

~~Security Requirements for Unclassified Information Technology Resources (Jan 2012)~~

~~(a) *General*. The Contractor shall be responsible for information technology (IT) security, based on General Services Administration (GSA) risk assessments, for all systems connected to a GSA network or operated by the Contractor for GSA, regardless of location. This clause is applicable to all or any part of the contract that includes information technology resources or services in which the Contractor has physical or electronic access to GSA's information that directly supports the mission of GSA, as indicated by GSA. The term information technology, as used in this clause, means any equipment, including telecommunications equipment that is~~

used in the automatic acquisition, storage, manipulation, management, control, display, switching, interchange, transmission, or reception of data or information. This includes major applications as defined by OMB Circular A-130. Examples of tasks that require security provisions include:

(1) Hosting of GSA e-Government sites or other IT operations;

(2) Acquisition, transmission, or analysis of data owned by GSA with significant replacement cost should the Contractors copy be corrupted;

(3) Access to GSA major applications at a level beyond that granted the general public; e.g., bypassing a firewall; and

(4) Any new information technology systems acquired for operations within the GSA must comply with the requirements of HSPD-12 and OMB M-11-11. Usage of the credentials must be implemented in accordance with OMB policy and NIST guidelines (*e.g.*, NIST SP 800-116). The system must operate within the GSA's access management environment. Exceptions must be requested in writing and can only be granted by the GSA Senior Agency Information Security Officer.

(b) *IT Security Plan*. The Contractor shall develop, provide, implement, and maintain an IT Security Plan. This plan shall describe the processes and procedures that will be followed to ensure appropriate security of IT resources that are developed, processed, or used under this contract. The plan shall describe those parts of the contract to which this clause applies. The Contractors IT Security Plan shall comply with applicable Federal laws that include, but are not limited to, 40 U.S.C. 11331, the Federal Information Security Management Act (FISMA) of 2002, and the E-Government Act of 2002. The plan shall meet IT security requirements in accordance with Federal and GSA policies and procedures. GSA's Office of the Chief Information Officer issued "CIO IT Security Procedural Guide 09–48, Security Language for Information Technology Acquisitions Efforts," to provide IT security standards, policies and reporting requirements. This document is incorporated by reference in all solicitations and contracts or task orders where an information system is contractor owned and operated on behalf of the Federal Government. The guide can be accessed at *http://www.gsa.gov/portal/category/25690*. Specific security requirements not specified in "CIO IT Security Procedural Guide 09–48, Security Language for Information Technology Acquisitions Efforts" shall be provided by the requiring activity.

(c) *Submittal of IT Security Plan*. Within 30 calendar days after contract award, the Contractor shall submit the IT Security Plan to the Contracting Officer and Contracting Officers Representative (COR) for acceptance. This plan shall be consistent with and further detail the approach contained in the contractors proposal or sealed bid that resulted in the award of this contract and in compliance with the requirements stated in this clause. The plan, as accepted by the Contracting Officer and COR, shall be incorporated into the contract as a compliance document. The Contractor shall comply with the accepted plan.

(d) *Submittal of a Continuous Monitoring Plan*. The Contractor must develop a continuous monitoring strategy that includes:

(1) A configuration management process for the information system and its constituent components;

(2) A determination of the security impact of changes to the information system and environment of operation;

(3) Ongoing security control assessments in accordance with the organizational continuous monitoring strategy;

(4) Reporting the security state of the information system to appropriate GSA officials; and

(5) All GSA general support systems and applications must implement continuous monitoring activities in accordance with this guide and NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*.

(e) *Security authorization*. Within six (6) months after contract award, the Contractor shall submit written proof of IT security authorization for acceptance by the Contracting Officer. Such written proof may be furnished either by the Contractor or by a third party. The security authorization must be in accordance with NIST Special Publication 800-37. This security authorization will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This security authorization, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document, and shall include a final security plan, a risk assessment, security test and evaluation, and disaster recovery/continuity of operations plan. The Contractor shall comply with the accepted security authorization documentation.

(f) *Annual verification*. On an annual basis, the Contractor shall submit verification to the Contracting Officer that the IT Security plan remains valid.

(g) *Warning notices*. The Contractor shall ensure that the following banners are displayed on all GSA systems (both public and private) operated by the Contractor prior to allowing anyone access to the system:

Government Warning

WARNINGWARNING**WARNING**

Unauthorized access is a violation of U.S. law and General Services Administration policy, and may result in criminal or administrative penalties. Users shall not access other users or system files without proper authority. Absence of access controls IS NOT authorization for access! GSA information systems and related equipment are intended for communication, transmission, processing and storage of U.S. Government information. These systems and equipment are subject to monitoring by law enforcement and authorized Department officials. Monitoring may result in the acquisition, recording, and analysis of all data being communicated, transmitted, processed or stored in this system by law enforcement and authorized Department officials. Use of this system constitutes consent to such monitoring.

WARNINGWARNING**WARNING**

(h) *Privacy Act notification*. The Contractor shall ensure that the following banner is displayed on all GSA systems that contain Privacy Act information operated by the Contractor prior to allowing anyone access to the system:

This system contains information protected under the provisions of the Privacy Act of 1974 (Pub. L. 93-579). Any privacy information displayed on the screen or printed shall be protected from unauthorized disclosure. Employees who violate privacy safeguards may be subject to disciplinary actions, a fine of up to $5,000, or both.

(i) *Privileged or limited privileges access*. Contractor personnel requiring privileged access or limited privileges access to systems operated by the Contractor for GSA or interconnected to a GSA network shall adhere to the specific contract security requirements contained within this contract and/or the Contract Security Classification Specification (DD Form 254).

(j) *Training*. The Contractor shall ensure that its employees performing under this contract receive annual IT security training in accordance with OMB Circular A-130, FISMA, and NIST requirements, as they may be amended from time to time during the term of this contract, with a specific emphasis on the rules of behavior.

(k) *GSA access*. The Contractor shall afford GSA access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, IT systems and devices, and personnel used in performance of the contract, regardless of the location. Access shall be provided to the extent required, in GSA's judgment, to conduct an inspection, evaluation, investigation or audit, including vulnerability testing to safeguard against threats and hazards to the integrity, availability and confidentiality of GSA data or to the function of information technology systems operated on behalf of GSA, and to preserve evidence of computer crime. This information shall be available to GSA upon request.

(l) *Subcontracts*. The Contractor shall incorporate the substance of this clause in all subcontracts that meet the conditions in paragraph (a) of this clause.

(m) *Notification regarding employees*. The Contractor shall immediately notify the Contracting Officer when an employee either begins or terminates employment when that employee has access to GSA information systems or data. If an employee's employment is terminated, for any reason, access to GSA's information systems or data shall be immediately disabled and the credentials used to access the information systems or data shall be immediately confiscated.

(n) *Termination*. Failure on the part of the Contractor to comply with the terms of this clause may result in termination of this contract.

(End of clause)

ATTACHMENT B
Product Service Codes

The following Product Service Codes (PSCs) were identified as most likely to involve work that is applicable. These PSCs are not an all-inclusive list—GSA contracts or orders for other types of services outside of these segments may be applicable.

Product-Service Code	Product-Service Description
7030	SOFTWARE
B547	SPECIAL STUDIES/ANALYSIS- ACCOUNTING/FINANCIAL MANAGEMENT (also referenced as STUDY/ACCOUNTING/ FINANCIAL MGT)
D303	IT AND TELECOM- DATA ENTRY
D305	IT AND TELECOM- TELEPROCESSING, TIMESHARE, AND CLOUD COMPUTING
D308	IT AND TELECOM- PROGRAMMING
D309	IT AND TELECOM- INFORMATION AND DATA BROADCASTING OR DATA DISTRIBUTION
D310	IT AND TELECOM- CYBER SECURITY AND DATA BACKUP
D311	IT AND TELECOM- DATA CONVERSION
D318	IT AND TELECOM- INTEGRATED HARDWARE/SOFTWARE/SERVICES SOLUTIONS
D325	IT AND TELECOM- DATA CENTERS AND STORAGE
R401	SUPPORT- PROFESSIONAL: PERSONAL CARE (NON-MEDICAL)
R430	SUPPORT- PROFESSIONAL: PHYSICAL SECURITY AND BADGING
R497	SUPPORT- PROFESSIONAL: PERSONAL SERVICES CONTRACTS
R610	SUPPORT- ADMINISTRATIVE:- PERSONAL PROPERTY MANAGEMENT
R611	SUPPORT- ADMINISTRATIVE: CREDIT REPORTING (also referenced as CREDIT REPORTING SERVICES)
R612	SUPPORT- ADMINISTRATIVE: INFORMATION RETRIEVAL
R615	SUPPORT- ADMINISTRATIVE: BACKGROUND INVESTIGATION
R702	SUPPORT- MANAGEMENT: DATA COLLECTION
R703	SUPPORT- MANAGEMENT: ACCOUNTING
R704	SUPPORT- MANAGEMENT: AUDITING
R710	SUPPORT- MANAGEMENT: FINANCIAL (also referenced as FINANCIAL SERVICES)

ATTACHMENT C
GSA Information System Contract Waiver Request Template

Date of Waiver Submission:	
Contract Number:	
Contract Product Service Code:	
Contract Product or Service Description:	
Contract Period of Performance (base and option(s)):	
Contract Value (base and option(s)):	
Contracting Officer:	
Contracting Officer Contact Info:	
Head of Contracting Activity:	
HCA Contact Info:	

Background. Please provide a brief overview of the procurement and a description of the information system.

Identification of requirements requested for waiver. Identify the requirements being requested for waiver.

Justification. Please provide a concise, clear and convincing rationale of why a requirement for a GSA information system should be waived for this particular contract.

Summary of residual risk. Please describe any risks that GSA will encounter by not including the requirements detailed above. Please also discuss any risk mitigation efforts that will be utilized.

Additional information. Please provide any additional information, not otherwise covered above, that the acquisition approval official (see GSAM 507.105(c)), Information System Authorizing Official (see https://ea.gsa.gov/#!/FISMA_POC) and Chief Information Security Officer may want to consider.

Contracting Officer	Signature	Date
Acquisition Approving Official	Signature	Date
Information System Authorizing Official	Signature	Date
Chief Information Security Officer	Signature	Date