General Services Administration
Washington, DC 20405

ADM 2800.12B, Change 151
March 11, 2022

GSA ORDER

Subject: General Services Administration Acquisition Manual; GSAR Case 2016-G511, Contract Requirements for GSA Information Systems

1. Purpose. This order transmits a revision to the General Services Administration Acquisition Manual (GSAM) to clarify, update, and streamline guidance for the management of GSA-awarded contracts or orders which involve GSA information systems.

2. Background. This case amends the GSAM to maintain consistency with the Federal Acquisition Regulation (FAR) and to consolidate and incorporate existing cybersecurity and other information technology requirements previously implemented through various Office of the Chief Information Officer (OCIO) policies.

   The changes fall into four categories:
   1. Consolidating requirements to follow existing agency security IT policies into a streamlined IT security guide titled “CIO 09-48, GSA IT Security Procedural Guide: Security and Privacy Acquisition Requirements”.
   2. Consolidating requirements to follow existing agency non-security IT policies into a streamlined policy titled “CIO 12-2018: IT Policy Requirements Guide”.
   3. Streamlining existing GSA guidance related to information technology.
   4. Deleting GSAR provision 552.239-70 *Information Technology Security Plan and Security Authorization* and GSAR clause 552.239-71 06 *Security Requirements for Unclassified Information Technology Resources.*

3. Effective date. March 11, 2022.

4. Explanation of changes. This case includes regulatory and nonregulatory changes. For full text changes of the amendment see Attachment A, GSAR Text Line-In/Line-Out.

   This amendment revises the regulatory language of the following GSAR subparts, changes summarized below:

   - **501.106 OMB approval under the Paperwork Reduction Act:** amended Table 1 by adding an entry for “511.171” and removing the entry for “552.239-71”

   - **502.101 Definitions:** added definitions (in alphabetical order) for GSA Information System (to include defining sub-terms) and Information System.

   - **511.171 Requirements for GSA Information Systems:** added guidance for contracting officers to ensure compliance with GSA and federal IT policies regarding IT security and implemented a waiver process.

- **539.70 Additional Requirements for Purchases Not in Support of National Security Systems**: deleted heading under GSAR and moved to a new title under GSAM.

- **539.7000 Scope of Subpart:** deleted subpart under GSAR and replaced with prescription and guidance under GSAM.

- **539.7001 Policy:** deleted subpart under the GSAR and replaced with guidance in the GSAM.

- **539.7002 Solicitation provisions and contract clause:** deleted to ensure parity with the FAR and GSA consolidated IT policy.

- **552.239-70 Information Technology Security Plan and Security Authorization:** provision deleted to remove outdated language and requirements.

- **552.239-71 Security Requirements for Unclassified Information Technology Resources:** clause deleted to eliminate duplicative, outdated, and complex requirements.

- **570.101 Applicability:** amended Table 1 under paragraph (b) by adding Part 539.

This amendment revises the non-regulatory language of the following GSAM subparts, changes summarized below:

- **511.102 Security of Information Technology Data:** deleted this section in its entirety.

- **511.170 Information Technology Coordination and Standards:** added new section "(a) Information System Requirements", referenced guidance in new GSAR subsection 511.171 for any procurements that may involve GSA Information Systems, and re-alphabetized list.

- **539.001 Applicability:** added (a) references to national security systems, classified information, and national security systems involving weapons; (b) requirements for individual access management, and (c) referenced 511.170 for additional requirements for GSA Information Systems.

- **539.70 Requirements for GSA Information Systems**: revised title to more clearly identify the content.

- **539.7000 Scope of subpart**: added language to describe the scope of subpart 539.70.

- **539.7001 Policy:** added language that ensures that GSA will provide information security to all agencies accessing its system, all employees have the appropriate security clearance, and all contractor submissions meet the GSA IT security requirements.

5. Cancellations. Acquisition Letter MV-19-04 and its supplement are hereby cancelled.

6. Point of contact. For clarification of content, contact Ms. Johnnie McDowell in the GSA Acquisition Policy Division at GSARPolicy@gsa.gov.

JEFFREY KOSES
Digitally signed by JEFFREY KOSES
Date: 2022.03.10 07:05:23 -05'00'

Jeffrey A. Koses
Senior Procurement Executive
Office of Acquisition Policy
Office of Government-wide Policy

GSAR Case 2016-G511
“Contract Requirements for GSA Information Systems”

GSAR/GSAM Text, Line-In/Line-Out

GSAR Baseline: Change 150 effective 03/04/2022
• Additions to baseline made by rule are indicated by **[bold text in brackets]**
• Deletions to baseline made by 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
• Regulatory GSAR language is indicated by shaded text
• Non-regulatory GSAM language is indicated by unshaded text

Part 501 - General Services Administration Acquisition Regulation System

Subpart 501.1 - Purpose, Authority, Issuance

* * * * *

GSAR Reference	OMB Control No.
* * *	
[511.171]	**[3090-0300]**
* * *	
~~552.239-71~~	~~3090-0294~~

* * * * *

Part 502 - Definitions of Words and Terms

Subpart 502.1 - Definitions

Subpart 502.101 - 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 including:

(1) "Cloud Information System" means 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) 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). Cloud information systems may connect to the GSA network.

(2) "External Information System" means 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).

(3) "Internal Information System" means information systems that reside on premise in GSA facilities and may connect to the GSA network. Internal systems are operated on behalf of GSA or the Federal Government (when GSA is the managing agency)."

(4) "Low Impact Software as a Service (LiSaaS) System" means cloud applications that are implemented for a limited duration, considered low impact and would cause limited harm to GSA.

(5) "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.]

*** * ***

*** * * * ***

Part 511 - Describing Agency Needs

* * * * *

Part 511.1 - Selecting and Developing Requirements Documents

* * *

~~**511.102 Security of Information Technology Data**~~

~~For actions that pertain to information systems or contractor managed government data, use the guidance identified under GSA's office of the Senior Agency Information Security Officer publication CIO IT Security Procedural Guide 09-48. The guide can be accessed at http://www.gsa.gov/portal/category/25690. The contracting officer shall coordinate with program officials or requiring activities to ensure that the solicitation includes the appropriate information security requirements. The information security requirements must be sufficiently detailed to enable contractors to fully understand the information security regulations, mandates, and requirements under the contract or task order.~~

511.170 Information Technology Coordination and Standards.
[(a) *Information Systems Requirements*. See 511.171 for guidance for any procurements that may involve GSA Information Systems.]
[(b)]~~(a)~~ * * *
[(c)]~~(b)~~ * * *
[(d)]~~(c)~~ * * *
[(e)]~~(d)~~ * * *

* * *

[511.171 Requirements for GSA Information Systems.

(a) *CIO Coordination.* The contracting officer shall ensure the requirements office has coordinated and identified possible CIO policy inclusions with the GSA IT prior to publication of a Statement of Work, or equivalent as well as the Security Considerations section of the acquisition plan to determine if the CIO policies apply. The CIO policies and GSA IT points of contact are available on the Acquisition Portal at https://insite.gsa.gov/itprocurement.

(b) *GSA Requirements*. For GSA procurements (contracts, actions, or orders) that may involve GSA Information Systems, excluding GSA's government-wide contracts e.g. Federal Supply Schedules and Governmentwide Acquisition Contracts, the contracting

officer shall incorporate the coordinated Statement of Work or equivalent including the applicable sections of the following policies into solicitations and contracts:

(1) *CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements*; and

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

(c) *Waivers.*

(1) In cases where it is not effective in terms of cost or time or where it is unreasonably burdensome to include *CIO 09-48, IT Security Procedural Guide: Security and Privacy IT Acquisition Requirements* or *CIO 12-2018, IT Policy Requirements Guide* in a contract or order, a waiver may be granted by the Acquisition Approving Official in accordance with the thresholds listed at 507.103(b), the Information System Authorizing Official, and the GSA IT Approving Official.

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

(A) The description of the procurement and GSA Information Systems;

(B) Identification of requirement requested for waiver;

(C) Sufficient justification for why the requirements should be waived; and

(D) Any residual risks that will be encountered by waiving the requirements.

(3) Waivers must be documented in the contract file.

(d) *Classified Information.* For any procurements that may involve access to classified information or a classified information system, see subpart 504.4 for additional requirements.]

* * * * *

* * * * *

Part 539— ACQUISITION OF INFORMATION TECHNOLOGY

539.001 Applicability.

[(a) In accordance with FAR 39.001, this part does not apply to acquisitions of information or information systems in support of national security systems. Refer to subpart 504.4 for guidance for any procurements that may involve access to classified information or a classified information system. See subpart 507.70 for guidance for purchases in support of national security systems involving weapons systems.

(b) Refer to 504.1370 and 542.302 for additional requirements for individual access management (i.e., HSPD-12) to GSA Information Systems.

(c) Refer to 511.170 for additional requirements for GSA Information Systems.]

* * * * *

~~Subpart 539.70—Additional Requirements for Purchases Not in Support of National Security Systems~~

~~539.7000 Scope of subpart.~~

~~This subpart prescribes acquisition policies and procedures for use in acquiring information technology supplies, services and systems not in support of national security systems, as defined by FAR part 39.~~

~~539.7001 Policy.~~

~~(a) GSA must provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source. Section 3544(a)(1)(A)(ii) of the Federal Information Security Management Act (FISMA) describes Federal agency security responsibilities as including "information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency."~~

~~(b) Employees responsible for or procuring information technology supplies, services and systems shall possess the appropriate security clearance associated with the level of security classification related to the acquisition. They include, but are not limited to contracting officers, contract specialists, project/program managers, and contracting officer representatives.~~

~~(c) Contracting activities shall coordinate with requiring activities and program officials to ensure that the solicitation documents include the appropriate information security requirements. The information security requirements must be sufficiently detailed to enable service providers to fully understand the information security regulations, mandates, and requirements that they will be subject to under the contract or task order.~~

~~(d) GSA's Office of the Senior Agency Information Security 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 that shall be inserted 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 .~~

~~539.7002 Solicitation provisions and contract clause.~~

~~Except for solicitations and contracts for personal services with individuals—~~

~~(a) 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) Insert the clause at 552.239-71, Security Requirements for Unclassified Information Technology Resources, in solicitations and contracts containing the provision in paragraph (a) of this section.~~

[Subpart 539.70—Requirements for GSA Information Systems]

[539.7000 Scope of subpart.

This subpart prescribes acquisition policies and procedures for use in acquiring GSA Information Systems.]

[539.7001 Policy.

(a) GSA must provide information security for the information and information system that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source.

(b) Employees responsible for procuring or managing information technology supplies, services and systems shall possess the appropriate security clearance associated with the level of security classification related to the acquisition. They include, but are not limited to contracting officers, contract specialists, project/program managers, and contracting officer representatives.

(c) The contracting officer or contracting officer's representative 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 contracting officer or contracting officer's representative shall coordinate with GSA IT as needed in determining contractor compliance. Guidance for identifying the applicable GSA IT point of contact is located on the Acquisition Portal at https://insite.gsa.gov/itprocurement.]

Part 552— SOLICITATION PROVISIONS AND CONTRACT CLAUSES

* * * * *

Subpart 552.2—Text of Provisions and Clauses

* * * * *

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)~~

* * *

* * * * *

Part 570— ACQUIRING LEASEHOLD INTERESTS IN REAL PROPERTY

Subpart 570.1—General

570.101 Applicability.

(a) * * *

(b) In addition, the GSAR rules in the table below apply. Other provisions of 48 CFR Chapter 5 (GSAR) do not apply to leases of real property unless specifically cross-referenced in this part 570.

GSAR Rules Applicable to Acquisitions of Leasehold Interests in Real Property

501 502 503 509.4 514.407	515.209-70 515.305 517.202 517.207 519.7	519.12 522.805 522.807 538.270 533	536.271 537.2 **[539]** 552 553

* * * * *