**GENERAL SERVICES ADMINISTRATION**

**48 CFR Parts 501, 502, 511, 539, 552, and 570**

**[GSAR Case 2016-G511; Docket No. 2021-0018; Sequence No. 1]**

**RIN 3090-AJ84**

# General Services Acquisition Regulation (GSAR); GSAR Case 2016-G511, Contract Requirements for GSA Information Systems

**AGENCY:** Office of Acquisition Policy, General Services Administration (GSA).

**ACTION:** Proposed rule.

**SUMMARY:** GSA is proposing to amend the General Services Administration Acquisition Regulation (GSAR) to streamline and update requirements for contracts that involve GSA information systems. The revision of GSA’s cybersecurity and other information technology requirements will lead to the elimination of a duplicative and outdated provision and clause from the GSAR. The proposed rule will replace the outdated text with existing policies of the GSA Office of the Chief Information Officer (OCIO) and provide centralized guidance to ensure consistent application across the organization. The updated GSA policy will align cybersecurity requirements based on the items being procured by ensuring contract requirements are coordinated with GSA's Chief Information Security Officer.

**DATES:** Interested parties should submit written comments to the Regulatory Secretariat at one of the address shown below on or before **[INSERT DATE 60 DAYS AFTER DATE OF PUBLICATION IN THE FEDERAL REGISTER]** to be considered in the formation of the final rule.

**ADDRESSES:** Submit comments in response to GSAR case 2016-G511 to: Regulations.gov: *http://www.regulations.gov*. Submit comments via the Federal eRulemaking portal by searching for "GSAR Case 2016-G511". Select the link "Comment Now" that corresponds with GSAR Case 2016-G511. Follow the instructions provided at the "Comment Now" screen. Please include your name, company name (if any), and "GSAR Case 2016-G511" on your attached document. If your comment cannot be submitted using *https://www.regulations.gov*, call or email the points of contact in the FOR FURTHER INFORMATION CONTACT section of this document for alternate instructions.

*Instructions*: Please submit comments only and cite GSAR Case 2016-G511 in all correspondence related to this case. Comments received generally will be posted without change to *https://www.regulations.gov*, including any personal and/or business confidential information provided. To confirm receipt of your comment(s), please check *https://www.regulations.gov* approximately two-to-three days after submission to verify posting.

**FOR FURTHER INFORMATION CONTACT:** Ms. Johnnie McDowell, Procurement Analyst, at 202-718-6112 or *gsarpolicy@gsa.gov*, for clarification of content. For information pertaining to status or publication schedules, contact the Regulatory Secretariat Division at 202-501-4755 or *gsaregsec@gsa.gov*. Please cite GSAR Case 2016-G511.

**SUPPLEMENTARY INFORMATION:**

**I. Background**

GSA's cybersecurity requirements mandate that contractors protect the confidentiality, integrity, and availability of unclassified GSA information and information systems from cybersecurity vulnerabilities and threats. This rule will require contracting officers to incorporate applicable GSA cybersecurity requirements within the statement of work to ensure compliance with Federal cybersecurity requirements and implement best practices for preventing cyber incidents. These GSA requirements mandate applicable controls and standards (e.g., U.S. National Institute of Standards and Technology, U.S. National Archives and Records Administration Controlled Unclassified Information standards).

In general, the proposed changes are necessary to bring long-standing GSA information system practices into the GSAR, consolidating policy into one area. Because of that consolidation, contractors may need less time and

fewer resources to read and understand all the requirements relevant to their contract.

GSA is proposing to amend the GSAR to revise sections of GSAR part 511, Describing Agency Needs, part 539, Acquisition Information Technology, and other related parts; to maintain consistency with the Federal Acquisition Regulation (FAR); and to incorporate and consolidate existing cybersecurity and other information technology requirements previously implemented through various Office of the Chief Information Officer (OCIO) or agency policies.

**II. Authority for This Rulemaking**

Title 40 of the United States Code (U.S.C.) Section 121 authorizes GSA to issue regulations, including the GSAR, to control the relationship between GSA and contractors.

**III. Discussion and Analysis**

The proposed rule changes fall into three categories: (1) streamlining existing agency information technology (IT) security policies previously issued through the OCIO into one consolidated cybersecurity requirements policy titled CIO IT Security Procedural Guide 09-48: *Security and Privacy Requirements for IT Acquisition Efforts*; (2) consolidating existing agency non-security IT policies previously issued through the OCIO into one streamlined requirements policy titled *CIO 12-2018: IT Policy Requirements Guide*; and (3) eliminating the GSAR provision

552.239-70, *Information Technology Security Plan and Security Authorization*, and GSAR clause 552.239-71, *Security Requirements for Unclassified Information Technology Resources.* The changes to the GSAR included in this proposed rule are summarized below:

1. Streamlining IT Security Policies into CIO IT Security Procedural Guide 09-48: Security and Privacy Requirements for IT Acquisition Efforts

GSA's internal information systems policies will be incorporated into subpart 511.171, Requirements for GSA Information Systems, requiring GSA contracting officers to:

- Incorporate the applicable sections or complete version of the CIO IT Security Procedural Guide 09-48: *Security and Privacy Requirements for IT Acquisition Efforts, and CIO 12-2018, IT Policy Requirements Guide*, into GSA solicitations (i.e., Statement of Work, or equivalent); and
- Coordinate with the GSA OCIO for applicable procurements.

The new guidance will also establish a waiver process for cases where it is not effective from a cost or timing standpoint or where it is unreasonably burdensome.

The streamlining of the policy into subpart 511.171 will also replace the general instruction found in GSAR 511.102, Security of Information Data, with more detailed

instruction, and better aligns the GSAR with language in the FAR.

The streamlining of security IT policies into CIO IT Security Procedural Guide 09-48: *Security and Privacy Requirements for IT Acquisition Efforts* means the:

- Requirements outlined in the numerous OCIO security, privacy, and other information system policies are succinctly stated in a centralized policy.
- Burden on contractors for understanding and implementing the applicable requirements for GSA information systems will be significantly reduced due to the elimination of outdated policies.
- Contract administration will be simplified by consolidating the IT security requirements in one location.

2. Consolidating Non-Security IT Policies into *CIO 12-2018 IT Policy Requirements Guide*

The consolidating of OCIO non-security IT policies into CIO 12-2018 IT Policy Requirements Guide, will reduce the burden for GSA contractors and ensure contractors understand and can easily comply with GSA's OCIO non-security requirements. In addition, the creation of one central acquisition policy guide covering applicable non-security information technology requirements will save time

and effort for both contractors and the Government to understand and implement these requirements.

3. Eliminating GSAR Provision and Clause

The analysis of GSA's IT and relevant policies will lead to the elimination of GSAR provision 552.239-70, *Information Technology Security Plan and Security Authorization*, and GSAR clause 552.239-71, *Security Requirements for Unclassified Information Technology Resources.* The elimination of the provision and clause means duplicative, outdated, and complex requirements imposed by them will be deleted from the GSAR and incorporated into the two policies. This new approach provides a more detailed explanation of the requirements for the Government and the public.

## IV. Regulatory Cost Analysis

The current GSAR coverage does not clearly include all GSA information system requirements contained in existing OCIO policies. This rule will bring long standing GSA information system practices into the GSAR and consolidate all relevant policies into one area. As a result, contractors can expend less time and fewer resources reading and understanding all the requirements relevant to their contract in order to fully comply with the requirements.

In addition, streamlining existing requirements for GSA information systems into two contractor focused

policies, CIO 09-48 and CIO 12-2018, will reduce the number of requirements that contractors must implement, and the Government must validate through contract administration, saving time and effort for both contractors and the Government.

The costs and impacts to streamline and consolidate IT security and non-security policies are discussed in the analysis below. The analysis was developed in consultation with the GSA Office of the Chief Information Officer (OCIO).

Explanation of Data Source and Cost Calculation

The associated costs were calculated by analyzing data from the beta.SAM formerly known as the Federal Procurement Data System New Generation (FPDS-NG) for GSA information system contracts completed in Fiscal Years 2017-2020. The report provides information on GSA contracts and task orders valued at $25,000 or more awarded using the Product Service Code (PSC) "D – ADP and Telecommunication Services" from beta.SAM. According to beta.SAM, the average number of new contract actions involving access to GSA's information system was 132, of which 48 percent, or 63 entities, were small business entities. The following paragraphs detail activities which are required by this rule for contractors using GSA's internal information systems:

1. Familiarize Business Staff with CIO 09-48: Security and Privacy Requirements for IT Acquisition Efforts

GSA estimates that contractors having to access GSA's internal information systems will take 2 hours to familiarize themselves with CIO 09-48 IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts. The 2 hours estimation is based on research findings which indicate that the requirements listed in CIO IT Security Procedural Guide 09-48: Security and Privacy Requirements for IT Acquisition Efforts are: 1) similar to those imposed by other Federal agencies, 2) required by Federal laws and guidance such as the Federal Information Security Modernization Act (FISMA), Office of Management and Budget Circulars, and NIST publications, and 3) outlined in the original CIO 09-48 policy and its supplements before the updates. The consistency with the majority of the requirements reduces the time industry will need to familiarize themselves with the updated policy. GSA estimates the regulatory cost for this part of the rule to be $26,422 (= 2 hours × $100.08 × 132 (rounded)).[1]

2. Familiarize Business Staff with CIO 12-2018: GSA IT Policy Requirements Guide

GSA estimates that contractors having to access GSA's internal information systems will take 2 hours to familiarize themselves with CIO 12-2018 IT Policy Requirements. The 2 hours estimation is based on research

[1] The $100.08 hourly is the 2021 GS rate for a GS-13 Step 5 (using the rate for the rest of the United States) burdened by 100% for fringe benefits.

findings which indicate that the non-security IT requirements are similar to those implemented by other federal agencies and was part of GSA many policy requirements in previous years. GSA estimates the total regulatory cost for this part of the rule to be $26,422 (= 2 hours × $100.08 × 132 (rounded)).[2]

3. Develop Business Procedures to Comply with CIO 09-48

Under GSA's IT policies, new contract actions may need to develop an IT plan and supplements to comply with GSA internal information systems security requirements. GSA estimates that it will take 1 hour to fully develop the policies as required by CIO 09-48 GSA IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts. The 1 hour estimation is based on the GSA's provision that allows contractors to use GSA's policies to develop contractor-specific policies. Developing the IT plan and supplement documents will result in a total estimated cost for this part of the rule of 13,211 (= 1 hour × $100.08 × 132 (rounded)).[3]

4. Develop Business Procedures to Comply with CIO 12-2018

Under GSA's IT policies new contract actions may need to develop, at a minimum, an IT Plan which includes non-security IT. GSA estimates that it will take 1 hour to comply with CIO 12-2018 GSA IT Policy Requirements Guide. The 1 hour estimate is based on the contractor's ability to

[2] See footnote 1.
[3] See footnote 1.

use GSA's policies to develop their own policies and procedures to comply with the requirements of FISMA as incorporated in the GSA's IT policies. The total estimated cost for this part of the rule is $13,211 (= 1 hour × $100.08 × 132 (rounded)).[4]

5. Recordkeeping to Comply with CIO 09-48

GSA estimates that contractors accessing GSA's internal information systems will take 1 hour to maintain records including the updating IT Plans and procedures, as needed. GSA estimated the total regulatory cost for this part of the rule to be $13,211(= 1 hour × $100.08 × 132(rounded)).[5]

6. Recordkeeping to Comply with CIO 12-2018

GSA estimates that contractor's accessing GSA's internal information systems will take 1 hour to maintain records. GSA calculated the total estimated cost for this part of the rule to be $13,211(= 1 hour × $100.08 × 132(rounded)).[6]

Total Regulatory Cost

The total cost of the above Cost Estimate is $72,000 in the first year after publication.

The total cost of the above Cost Estimate in subsequent years is $18,000 annually.

[4] See footnote 1.
[5] See footnote 1.
[6] See footnote 1.

The following is a summary of the estimated total regulatory cost calculated into perpetuity at a 7-percent discount rate:

| | |
|---|---|
| Present Value Costs | $451,536 |
| Annualized Costs | $31,608 |

## V. Executive Orders 12866 and 13563

Executive Orders (E.O.s) 12866 and 13563 direct agencies to assess all costs and benefits of available regulatory alternatives and, if regulation is necessary, to select regulatory approaches that maximize net benefits (including potential economic, environmental, public health and safety effects, distributive impacts, and equity). E.O. 13563 emphasizes the importance of quantifying both costs and benefits, of reducing costs, of harmonizing rules, and of promoting flexibility. The Office of Management and Budget (OMB) anticipates that this will not be a significant regulatory action and, therefore, will not be subject to review under section 6(b) of E.O. 12866, Regulatory Planning and Review, dated September 30, 1993.

## VI. Congressional Review Act

The Congressional Review Act, 5 U.S.C. 801 et seq., as amended by the Small Business Regulatory Enforcement Fairness Act of 1996, generally provides that before a "major rule" may take effect, the agency promulgating the rule must submit a rule report, which includes a copy of

the rule, to each House of the Congress and to the Comptroller General of the United States. OMB anticipates that this will not be a major rule under 5 U.S.C. 804.

**VII. Regulatory Flexibility Act**

GSA does not expect this rule to have a significant economic impact on a substantial number of small business entities within the meaning of the Regulatory Flexibility Act, at 5 U.S.C. 601, et seq., because the rule will incorporate the minimum requirements consistent with applicable laws, Executive orders, and prudent business practices for securing Government information systems. In addition, the requirements are similar to those currently in use in GSA information systems solicitations and contracts, and contractors are familiar with and are currently complying with these requirements. The Initial Regulatory Flexibility Analysis (IRFA) has been performed, and is summarized as follows:

GSA is proposing to amend the General Services Administration Acquisition Regulation (GSAR) to codify the proposed streamlined and consolidated requirements for contract actions that involve accessing GSA's information systems. GSA’s policies on cybersecurity and other information technology requirements have been previously implemented through various Office of the Chief Information Officer (OCIO) policies separately disseminated to the

workforce. Contractors have already been performing the majority of the requirements.

The objective of the rule is to formalize the proposed changes to the existing guidance for contracts involving GSA information systems. The rule also allows GSA to vet these existing information technology requirements to the public for comment.

The rule requires contractors to comply with applicable requirements contained in *CIO 09-48 GSA IT Security Procedural Guide: Security and Privacy Requirements for IT Acquisition Efforts* and *CIO 12-2018, IT Policy Requirements Guide*. The legal basis for the rule is 40 U.S.C. 121(c), 10 U.S.C. chapter 137, and 51 U.S.C. 20113.

The rule applies to large and small businesses, which are awarded contracts involving GSA information systems. Information generated from the beta.SAM, formerly FPDS, for Fiscal Years 2017-2020 has been used as the basis for estimating the number of contractors that may involve GSA information systems as a requirement of their contract. The analysis focused on contracts in the Product Service Code (PSC) category D-Information and Technology and Telecommunications.

Examination of this data revealed there was an average of 132 new contracts awarded in the targeted PSC for fiscal year (FY) 2017-2020. Of these contract actions, 63 or 48 percent were small businesses. The number of potential

subcontractors in the selected PSC to which the requirements would flow down was calculated by using a ratio of 0.3:1, subcontractors to prime contractors (including other than small businesses), which equates to 44 annual subcontractors, of which GSA estimates that 75 percent would be small businesses (i.e., 33). Therefore, the total number of small businesses, including prime contractors and subcontractors, impacted annually would be 96.

This rule will consolidate requirements currently used in solicitations and contracts involving GSA information systems and does not implement new requirements. In addition, the rule establishes a waiver process for cases where it is not cost effective or where it is unreasonably burdensome.

The rule involves reporting and recordkeeping that are currently covered under OMB Control Number 3090-0300. This rule does not include any new reporting, recordkeeping, or other compliance requirements for small businesses.

The rule does not duplicate, overlap, or conflict with any other Federal rules.

There are no known alternatives to this rule which would accomplish the stated objectives. This rule does not initiate or impose any new administrative or performance requirements on small business contractors because the policies are already being followed and comply with all

applicable Federal laws regarding Federal IT systems. The rule will allow the policies to be codified.

The Regulatory Secretariat Division will be submitting a copy of the IRFA to the Chief Counsel for Advocacy of the Small Business Administration. A copy of the IRFA may be obtained from the Regulatory Secretariat Division. GSA invites comments from small business concerns and other interested parties on the expected impact of this rule on small business entities.

GSA will also consider comments from small business entities concerning the existing regulations in subparts affected by the rule in accordance with 5 U.S.C. 610. Interested parties must submit such comments separately and should cite 5 U.S.C. 610 (FAR Case 2016-G511), in correspondence.

**VIII. Paperwork Reduction Act**

The Paperwork Reduction Act (44 U.S.C. Chapter 35) does apply because the rule contains procedures with information collection requirements. However, these procedures do not impose additional information collection requirements to the paperwork burden previously approved under an existing OMB Control Number 3090-0300.

Requesters may obtain a copy of the information collection documents from the GSA Regulatory Secretariat Division, by calling 202-501-4755 or emailing *GSARegSec@gsa.gov*. Please cite OMB Control No. 3090-0300,

Implementation of Information Technology Security Provision, in all correspondence.

**List of Subjects in 48 CFR Parts 501, 502, 511, 539, 552, and 570**

Government procurement.

Jeffrey A. Koses,
Senior Procurement Executive,
Office of Acquisition Policy,
Office of Government-wide Policy,
General Services Administration.

Therefore, GSA proposes amending 48 CFR parts 501, 502, 511, 539, 552, and 570 as set forth below:

**PART 501—GENERAL SERVICES ADMINISTRATION ACQUISITION REGULATION SYSTEM**

1. The authority citation for 48 CFR part 501 continues to read as follows:

**AUTHORITY:** 40 U.S.C. 121(c).

2. In section 501.106, amend table 1 by—

a. Adding an entry for "511.171" in numerical order; and

b. Removing the entry for "552.239-71".

The addition reads as follows:

**501.106 OMB approval under the Paperwork Reduction Act.**

* * * * *

**Table 1 to 501.106**

| GSAR Reference | OMB control No. |
|---|---|
| * * * | * * * * |
| 511.171 | 3090-0300 |
| * * * | * * * * |

**PART 502—DEFINITIONS OF WORDS AND TERMS**

3. The authority citation for 48 CFR part 502 continues to read as follows:

**AUTHORITY:** 40 U.S.C. 121(c).

4. Amend section 502.101 by adding, in alphabetical order, the definitions of "GSA Information System" and "Information System" to read as follows:

**502.101 Definitions.**

* * * * *

*GSA Information System* means an information system used or operated by the U.S. General Services Administration (GSA) 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 if breached.

(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**

5. The authority citation for 48 CFR part 511 continues to read as follows:

**AUTHORITY:** 40 U.S.C. 121(c).

6. Add section 511.171 to read as follows:

**511.171 Requirements for GSA Information Systems.**

(a) *General Service Administration (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 applicable sections of the following policies in the Statement of Work, or equivalent:

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

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

(b) *CIO (Chief Information Officer) coordination.* The contracting officer shall coordinate with GSA's information technology (IT) point of contact to identify possible CIO policy inclusions prior to publication of a Statement of Work, or equivalent. In addition, contracting officers shall review the Security Considerations section of the acquisition plan to identify 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.

(1) The contracting officer will be responsible for documenting the date of request for GSA IT coordination.

(2) If no response is received within 10 business days of the request, the contracting officer will document that fact in the contract file and proceed with the publication of the Statement of Work or equivalent.

(3) The contracting officer may grant an extension of this time period, if requested by GSA IT.

(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 as identified in 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-

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

(ii) Identification of requirement requested for waiver;

(iii) Sufficient justification for why the requirement should be waived; and

(iv) Any residual risks posed by waiving the requirement.

(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—[REMOVED AND RESERVED]**

7. Under the authority of 40 U.S.C. 121(c), remove and reserve part 539.

**PART 552—SOLICITATION PROVISIONS AND CONTRACT CLAUSES**

8. The authority citation for 48 CFR part 552 continues to read as follows:

**AUTHORITY:** 40 U.S.C. 121(c).

**Section 552.239-70 [Removed and Reserved]**

9. Remove and reserve section 552.239-70

**PART 570—ACQUIRING LEASEHOLD INTERESTS IN REAL PROPERTY**

10. The authority citation for 48 CFR part 570 continues to read as follows:

**AUTHORITY:** 40 U.S.C. 121(c).

11. In section 570.101, revise the table in paragraph (b) to read as follows:

**570.101 Applicability.**

* * * * *

(b) * * *

**Table 1 to Paragraph (b)--GSAR Rules Applicable to Acquisitions of Leasehold Interests in Real Property**

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

* * * * *

[FR Doc. 2021-18866 Filed: 9/9/2021 8:45 am; Publication Date: 9/10/2021]