



Acquisition Letter MV-16-01

July 21, 2016

MEMORANDUM FOR THE GSA ACQUISITION WORKFORCE

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

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

SUBJECT: Contract Guidance on Information and Information Systems Security

1. Purpose. The purpose of this letter is to define guidance and establish consistent language for the management of contracts or orders involving access or use of information technology (IT) resources or sensitive data.

2. Background. In order to protect against cybersecurity threats, it is important to ensure that contracts that include handling of sensitive data are compliant with Federal security standards, policies, and reporting requirements. See Appendix A for a list of references.

GSA must provide security for the information and 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 assessment and authorization
- Protecting sensitive information
- Internet Protocol version 6 (IPv6) incorporation
- Cloud computing
- Security monitoring and alerting requirements
- Contractor systems oversight
- HSPD-12 compliance
- Contractor access to Government systems
- Compliance with Government policies
- IT security and privacy awareness training
- Government furnished equipment
- Secure technical implementation
- Use of social media
- Handling sensitive data while teleworking

This Acquisition Letter (AL) consolidates and updates guidance in AL MV-15-01 and AL MV-15-01 Supplement 1. The primary difference between this AL and MV-15-01 are the policies listed in Appendix D, which are now separated into various mandatory and optional categories.

3. Effective Date. Immediately.

4. Expiration Date. This Acquisition Letter expires upon incorporation of the changes into the General Services Administration Acquisition Manual (GSAM).

5. Cancellation. AL MV-15-01, including its Supplement 1, is hereby cancelled.

6. Applicability. This requirement applies to all contracts or orders awarded by GSA that may involve access or use of GSA IT resources or sensitive data to conduct business on behalf of, or with, GSA or GSA supported Government organizations, regardless of dollar value.

As other Federal agencies may place orders that are not applicable, this requirement does not apply to Federal Supply Schedules (FSS), Government-wide Acquisition Contracts (GWACs), or Multi-agency Contracts (MACs) at the master contract level.

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

7. Requirements. Except as provided in paragraph 8 of this Letter, contracting officers who are working with contracts determined to be applicable must ensure that the clauses listed in Appendix C and the language identified in Appendix D are incorporated into any new applicable contracts or orders, and incorporated into any existing applicable contracts or orders, if not previously modified to satisfy Acquisition Letter MV-15-01.

8. Waiver Process. In some instances it will not be prudent or cost effective to include the security clauses or policies in a contract, such as if a cost-benefit analysis demonstrates that the cost to include the requirements is unreasonably high. In such cases, the Head of Contracting Activity (HCA) may grant a waiver.

(a) Waiver Policy

To determine if a waiver is appropriate, contracting officers should first consider the feasibility of implementing the clause and policies contained in Appendix C and D. While most clauses and policies should not present cost or implementation issues to contractors, some likely will have a cost impact.

Each of the required clauses and policies should be considered on an individual basis for the waiver process. Contracting officers should limit the scope of waiver requests to only the clauses or policies for which clear and convincing rationale can be provided to demonstrate that incorporation and implementation of the clauses or policies into a contract is cost prohibitive or impracticable due to the unique circumstances of that particular contract.

(b) Waiver Instructions

The contracting officer should complete the *Waiver Request Template* identified in Appendix E, and provide it to their respective HCA for approval. The HCA should provide a response to the waiver request within 5 business days. The HCA must obtain concurrence from the Office of GSA IT to waive the requirements. Contracting officers must obtain approval for a waiver prior to issuing a solicitation and/or awarding a new contract. Contracting officers must include a copy of any waiver in the contract file.

HCAs may consider issuing blanket waivers for specific clauses or policies related to explicitly identified classes of contracts. Contracting officers must include a copy of the blanket waiver in the contract file, if utilized.

9. Point of Contact. Any questions regarding the content of this Letter may be directed to Mr. Kevin Funk, Procurement Analyst, General Services Acquisition Policy Division, by phone at 202-357-5805 or by email at kevin.funk@gsa.gov. CIO risk consultation requests may be directed to Mr. Kurt Garbars, GSA Chief Information Security Officer, by phone at 202-208-7485 or by email at kurt.garbars@gsa.gov.

| | |
|-------------|--------------------------------------|
| Attachments | Appendix A – References |
| | Appendix B – Product Service Codes |
| | Appendix C – Clause Checklist |
| | Appendix D – New Contract Language |
| | Appendix E – Waiver Request Template |

MV-16-01
Appendix A
References

The following documents are some of the statutes and regulations that govern information and information system security.

- 40 U.S.C. 11331, Responsibilities for Federal Information Systems Standards
<http://www.gpo.gov/fdsys/pkg/USCODE-2009-title40/pdf/USCODE-2009-title40-subtitleIII-chap113-subchapIII-sec11331.pdf>
- E-Government Act of 2002, Public Law 107-347
Federal Information Security Management Act of 2002 (FISMA), Public Law 107-347
<http://www.gpo.gov/fdsys/pkg/PLAW-107publ347/pdf/PLAW-107publ347.pdf>
- OMB Circular A-130, Management of Federal Information Resources
http://www.whitehouse.gov/omb/circulars_a130_a130trans4/
- OMB Memorandum M-14-03, Enhancing the Security of Federal Information and Information Systems
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-03.pdf>
- OMB Memorandum M-14-04, Fiscal Year 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2014/m-14-04.pdf>
- OMB Memorandum M-15-01, Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices
<http://www.whitehouse.gov/sites/default/files/omb/memoranda/2015/m-15-01.pdf>
- NIST Standard SP 800-137, Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations
<http://csrc.nist.gov/publications/nistpubs/800-137/SP800-137-Final.pdf>
- NIST Standard SP 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems
<http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf>

MV-16-01
Appendix 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 |
| B546 | SPECIAL STUDIES/ANALYSIS- SECURITY (PHYSICAL/PERSONAL) |
| 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 |
| D309 | IT AND TELECOM- INFORMATION AND DATA BROADCASTING OR DATA DISTRIBUTION |
| D310 | IT AND TELECOM- CYBER SECURITY AND DATA BACKUP |
| D311 | ADP DATA CONVERSION SERVICES |
| 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) |

MV-16-01
Appendix C
Clause Checklist

The following clauses must be included in all contracts or orders awarded by GSA that may involve access or use of GSA information technology (IT) resources or sensitive data.

- FAR Clause 52.204-2, Security Requirements
- FAR Clause 52.204-9, Personal Identity Verification of Contractor Personnel
- FAR Clause 52.224-1, Privacy Act Notification
- FAR Clause 52.224-2, Privacy Act
- FAR Clause 52.239-1, Privacy or Security Safeguards
- FAR Clause 52.204-21, Basic Safeguarding of Covered Contractor Information Systems
- GSAR Clause 552.204-9, Personal Identity Verification Requirements
- GSAR Clause 552.239-70, Information Technology Security Plan and Security Authorization
- GSAR Clause 552.239-71, Security Requirements for Unclassified Information Technology Resources

MV-16-01
Appendix D
New Contract Language

The following language must be included in the Statement of Work, or equivalent, for all contracts or orders awarded by GSA that may involve access or use of GSA information technology (IT) resources or sensitive data.

The program office should provide input and collaborate with the contracting officer on determining which policies, if any, in paragraph (f) of this section apply to a contract or order.

[Begin Section]
**Safeguarding Sensitive Data and
Information Technology Resources**

- (a) In accordance with FAR 39.105, this section is included in the contract.
- (b) This section applies to all who access or use GSA information technology (IT) resources or sensitive data, including awardees, contractors, subcontractors, lessors, suppliers and manufacturers.
- (c) The GSA policies as identified in paragraphs (d), (e) and (f) of this section are applicable to the contract. These policies can be found at <http://www.gsa.gov/directives> or <https://insite.gsa.gov/directives>.
- (d) All of the GSA policies listed in this paragraph must be followed.
- (1) CIO P 1878.2A Conducting Privacy Impact Assessments (PIAs) in GSA
 - (2) CIO P 2100.1 GSA Information Technology (IT) Security Policy
 - (3) CIO P 2180.1 GSA Rules of Behavior for Handling Personally Identifiable Information (PII)
 - (4) CIO 9297.1 GSA Data Release Policy
 - (5) CIO 9297.2B GSA Information Breach Notification Policy
- (e) All of the GSA policies listed in this paragraph must be followed, when inside a GSA building or inside a GSA firewall.
- (1) CIO P 2100.2B GSA Wireless Local Area Network (LAN) Security
 - (2) CIO 2100.3B Mandatory Information Technology (IT) Security Training Requirement for Agency and Contractor Employees with Significant Security Responsibilities
 - (3) CIO 2104.1A GSA Information Technology IT General Rules of Behavior
 - (4) CIO 2182.2 Mandatory Use of Personal Identity Verification (PIV) Credentials
 - (5) ADM P 9732.1D Suitability and Personnel Security

(f) The GSA policies listed in this paragraph must be followed, if applicable.
[Contracting Officer check all policies that apply.]

- (1) ___ CIO 2102.1 Information Technology (IT) Integration Policy
- (2) ___ CIO 2105.1C GSA Section 508: Managing Electronic and Information Technology for Individuals with Disabilities
- (3) ___ CIO 2106.1 GSA Social Media Policy
- (4) ___ CIO 2107.1 Implementation of the Online Resource Reservation Software
- (5) ___ CIO 2108.1 Software License Management
- (6) ___ CIO 2160.2B GSA Electronic Messaging and Related Services
- (7) ___ CIO 2160.4A Provisioning of Information Technology (IT) Devices
- (8) ___ CIO 2162.1 Digital Signatures
- (9) ___ CIO P 2165.2 GSA Telecommunications Policy

(g) The contractor and subcontractors must insert the substance of this section in all subcontracts.

[End Section]

MV-16-01
Appendix E
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.

Listing of clauses/policies requested for waiver. Please provide a concise, clear and convincing rationale of why a clause and/or a policy should be waived for this particular contract.

Example:

*GSAR Clause 552.239-71 - Security Requirements for Unclassified Information Technology Resources
 This clause was not incorporated into the previous contract. GSAR Clause 552.239-71(b), (c) and (d) require the contractor to develop both an IT security plan and a continuous monitoring plan, which were not submitted for the previous contract. Based on market research, there will be a sizeable cost impact for the development of such plans. The unclassified IT resources utilized by this contract consist solely of Government documents already in the public domain. As such, the cost of implementing GSAR Clause 552.239-71 for this contract will be disproportionate to the amount of risk actually mitigated.*

Summary of residual risk. Please describe any risks that GSA will encounter by not including the clauses and/or policies 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 HCA and/or CIO may want to consider.

| | | |
|------------------------------|-----------|------|
| Contracting Officer | Signature | Date |
| Head of Contracting Activity | Signature | Date |
| CIO Risk Analyst | Signature | Date |