GSA Office of Government-wide Policy

5/14/2024

Acquisition Letter MV-2023-02
Supplement 2

MEMORANDUM FOR THE GSA ACQUISITION WORKFORCE

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

DocuSigned by:
Jeff Koses
21BD80B9E8AC4A0...

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

DocuSigned by:
David Shive
A3AE4284A2754F9...

SUBJECT: Supplement 2 to MV-2023-02; Ensuring Only Approved Software is Acquired and Used at GSA

On January 11, 2023, we issued Acquisition Letter MV-2023-02 to explain that Office of Management and Budget (OMB) Memo (M-22-18) required Federal agencies to use only software that complies with Government-specified secure software development practices.

While GSAM 511.170(d) already had a requirement for GSA IT to approve software before it could be acquired and used, the OMB memo necessitates GSA IT updating how it collects, reviews, retains, and monitors industry attestation information.

On May 24, 2023, we updated this Acquisition Letter to explain that GSA was extending the deadlines, including for collecting software attestations, while the Cybersecurity & Infrastructure Security Agency (CISA) and OMB finalized the Secure Software Development Attestation Common Form (hereafter referred to as the “Common Form”) and their Common Form repository.

On March 11, 2024, CISA and OMB released the Common Form and, on March 18, 2024, CISA’s repository went live.

These actions set a June 8, 2024, effective date for the OMB Policy.

Timeline for Collection & Updates to Associated GSA IT Policy

Starting June 8, 2024, GSA will begin collecting Common Forms for new contracts (including micro-purchases) and the exercise of contract options, that include the use of software, regardless of whether or not the software is considered critical.

GSA IT will update its policy (or policies) **by June 8, 2024**, in accordance with OMB M-22-18 and this AL, to help GSA's workforce and to reflect, among other updates, GSA's process for collecting, reviewing, retaining, and monitoring attestation information.

Process for Collecting & Using the CISA Repository

The Common Form for GSA's use can be found on both the GSA Acquisition Portal Cyber-Supply Chain Risk Management (C-SCRM) page and GSA.gov's Acquisition Policy Library and Resources page.

GSA will collect Common Forms directly from offerors and contractors, as needed. If a valid form has already been posted in the CISA's repository, there is no need to obtain a separate attestation.[1]

Generally, as outlined in MV-2023-02, for GSA-funded acquisitions, Common Forms and Plans of Action & Milestones (POA&Ms) will be collected and reviewed, as necessary, through GSA's existing IT Standards process.

With the exception of the changed date, paragraphs 3 through 7 MV-2023-02 (including Supplement 1) remain unchanged. Frequently Asked Questions (FAQs) will be posted to the C-SCRM Topic Page on the GSA Acquisition Portal.

Training

Mandatory Training

As part of the C-SCRM course training curriculum, *FCS 103 - Security Exclusions and Prohibitions*, is now available in FAI CSOD. Completion of this course is mandatory for all acquisition certification holders.

All mandatory acquisition training, including additional C-SCRM courses, can be found on the GSA Acquisition Portal.

Helpful Training

GSA's Office of Government-wide Policy (OGP) has created a "Knowledge Check" course for this Acquisition Letter in FAI CSOD (search using "FCL-GSA-OGP0029"). This course is worth 1 continuous learning point (CLP). While the "Knowledge Check" course is not required, it is helpful to reinforce understanding.

[1] The existence of the CISA repository nullifies MV-2023-02's requirement for GSA to "update GSA-administered indefinite delivery vehicles (IDVs) . . . to allow . . . contractors to provide attestations . . . at the base IDV contract level and make such information available to ordering activities" as industry may now submit forms to, and ordering agencies may access forms from, CISA's repository directly.

GSA Office of Government-wide Policy

5/24/2023

Acquisition Letter MV-2023-02
Supplement 1

MEMORANDUM FOR THE GSA ACQUISITION WORKFORCE

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

DocuSigned by:
Jeffrey A. Koses
21BD80B9E8AC4A0...

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

DocuSigned by:
David Shive
A3AE4284A2754F9...

SUBJECT: Supplement 1 to MV-2023-02; Ensuring Only Approved Software is Acquired and Used at GSA

On May 2, 2023, GSA was notified that the Office of Management and Budget (OMB) is working on a process to extend the deadlines, including for collecting software attestations, contained in OMB Memo M-22-18[1].

Accordingly, the dates reflected in GSA Acquisition Letter MV-2023-02[2], related to the updating of GSA IT policies and GSA's collection of software attestations, are no longer applicable.

A second Supplement to MV-2023-02, including new deadlines, will be issued once OMB has issued additional information.

Questions regarding this supplement may be directed to GSARPolicy@gsa.gov.

[1] OMB M-22-18
[2] GSA Acquisition Letter MV-2023-02

U.S. General Services Administration
1800 F Street, NW
Washington, DC 20405
www.gsa.gov

GSA Office of Governmentwide Policy

1/11/2023

Acquisition Letter MV-2023-02

MEMORANDUM FOR THE GSA ACQUISITION WORKFORCE

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

DocuSigned by:
Jeffrey A. Koses
21BD80B9E8AC4A0...

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

DocuSigned by:
David Shive
A3AE4284A2754F9...

SUBJECT: Ensuring Only Approved Software is Acquired and Used at GSA

1. What is the purpose of this Acquisition Letter (AL)?

The purpose is to highlight how current GSA acquisition policy and current GSA information technology policy work together to ensure only approved software (including products containing software) is acquired and used at GSA.

The combination of these policies allow GSA to respond to recent guidance issued by the Office of Management and Budget (OMB) as GSA, and other Federal agencies, wait for future Federal Acquisition Regulation (FAR) guidance.

2. What is the background of recent Federal policy?

Executive Order (EO) 14028, Improving the Nation's Cybersecurity, directed the National Institute of Standards and Technology (NIST) to publish guidance on practices for software supply chain security. Additionally, the EO directed OMB to require agencies to comply with NIST's applicable published guidance[1] .

In response to this direction, OMB issued M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices. In short, OMB M-22-18 states that Federal agencies must only use software that complies with Government-specified secure software development practices.

3. What is the background of GSA policy?

[1] The NIST Secure Software Development Framework (SSDF), SP 800-218 and the NIST Software Supply Chain Security Guidance

The General Services Acquisition Manual (GSAM) 511.170(d) already states that GSA information technology, including software, must be approved for use pursuant to GSA Order CIO 2160.1, GSA Information Technology (IT) Standards Profile (hereafter referred to as the "GSA Order").

Specifically, the GSA Order states that no software[2] can be acquired (or used) until it has been through the IT Standards process and has been approved by the GSA Chief Technology Officer (CTO). Approved software is listed in GSA's Enterprise Architecture Analytics & Reporting (GEAR) platform.

In order for software to become approved for GSA use, it must comply with the processes described in the GSA Order. Information Technology Coordination and Standards requirements are communicated to GSA acquisition teams and prospective offerors at General Services Administration Acquisition Regulation (GSAR) 511.170.

In accordance with OMB M-22-18 and this AL, GSA IT will update its policy (or polices), including the GSA Order, by June 12, 2023 to reflect, among other updates, GSA's process for collecting, reviewing, retaining, and monitoring attestation information.

4. What should you expect from upcoming federal acquisition policy?

The FAR Council has opened a proposed rule (FAR case 2023-002[3]) to implement section 4(n) of EO 14028. This rule will also focus on requirements outlined in OMB M-22-18.

Once the rule is finalized, relevant GSA acquisition policy, and the referenced GSA Order, may be updated to further implement the FAR rule.

5. How should you utilize current GSA policy for GSA-funded acquisitions?

As GSA waits for the referenced FAR rule to be issued, all GSA contracting activities, including lease contracting activities, are reminded of the requirements for the procurement and use of approved and unapproved software.

Existing Contracts that Include the use of Software

For existing contracts (including applicable micro-purchases and leases) that include the use of software, GSA IT will provide an internally accessible list of those softwares

[2] The GSA Order further explains and defines the information technologies within scope of the policy, including applicable software, cloud services, and products containing software.

[3] Open FAR Cases Report

and will start collecting attestations by June 12, 2023, working with the appropriate contracting officers, as necessary, as part of their IT Standards Process that will be clarified in the GSA Order, and in accordance with OMB M-22-18.

If GSA IT previously approved a software, but no longer approves the software (due to an expired pilot, or newer federal prohibitions, for example), any future period of performance (e.g., option year, extension, task order) cannot be exercised or issued and the requirement must be re-procured.

New Contracts that Include the use of Software

For any GSA contract[4] with requirements (or that may include requirements) for the use of software, acquisition teams must incorporate planning that includes the following in their applicable acquisition activities.

- If the solicitation or contract (including micro-purchases) is for the procurement or use of software in performance of a contract of a Federal Risk and Authorization Management Program (FedRAMP) authorized service provider, product, or solution[5], award may be made and the contract may start after ensuring the GSA IT Standards Process has been followed.

- If the apparently successful offeror offers software that is already approved in accordance with the IT Standards Process, award may continue and the contract start may be effective immediately (subject to other acquisition regulations and policies).

- If the apparently successful offeror offers software that is not already approved in accordance with the IT Standards Process, award may be made, however, the period of performance cannot begin (or the software cannot be used) until the offered software has been approved in accordance with the IT Standards Process.

    - Acquisition teams must consider during milestone planning that the GSA IT Standards Process and associated security review may take significant time to adjudicate.[6]

[4] Including applicable micro-purchases and leases

[5] Review the FedRAMP Marketplace for a list of FedRAMP authorized products, solutions, and providers.

[6] The GSA IT Standards process and associated security review will include collecting applicable attestations responsive to the requirements of OMB M-22-18.

- If GSA IT does approve the software, GSA IT will provide the acquisition team documentation, including attestation, to include in the official contract file.
- If GSA IT does not approve the software, the period of performance cannot commence (or the software cannot be used) and the requirement must be re-solicited if the acquisition team determines it's not in the best interest of the Government to award to the next best-suited offeror.

Communicating with Industry

For requirements covered by the GSA Order, acquisition teams must do the following as early in the acquisition process as possible:

- Communicate the requirements of GSAM 511.170 to potential and interested offerors.
- Communicate the requirements of the GSA IT Standards Profile and ensure potential and interested offerors understand that if the offered software has not previously been through the IT Standards Process, the offered software will need to undergo the IT Standards Process before the contract can start.
- Communicate that the attestation form, as part of the GSA IT Standards Process, will be collected as part of a contract deliverable.
- Notify potential and interested offerors that GSA IT may not approve the offered software (if the software doesn't follow applicable NIST guidance or for any other reasons as outlined in the GSA IT Standards Profile). If this happens, the requirement will need to be re-solicited.

Acquisition teams are also encouraged to recommend potential and interested cloud vendors to pursue FedRAMP compliance when possible.

6. What is the impact on GSA-administered Governmentwide Vehicles and Assisted Acquisitions?

GSA contracting activities must update GSA-administered indefinite delivery vehicles (IDVs) (e.g., Federal Supply Schedule, Government-wide Acquisition Contracts, Multi-Agency Contracts (MACs)) to allow, but not require, contractors to provide attestations[7], responsive to the requirements of OMB M-22-18, at the base IDV contract level and make such information available to ordering activities to the extent possible.

[7] Attestations at the IDV level must utilize the forthcoming Cybersecurity & Infrastructure Security Agency (CISA) attestation common form (if not already publicly posted) and must not include Plan of Action & Milestones (POA&M) or Software Bill of Material (SBOM) information. The ordering agency is responsible for complying with OMB M-22-18.

As previously discussed, once the FAR rule is finalized, relevant GSA acquisition policy specific to GSA-administered IDVs may be updated to further implement the FAR rule.

For assisted acquisitions, GSA contracting activities must follow the policy of the requesting agency.

7. What is the impact on micro-purchases and the use of GSA Purchase Cards?

The requirements of the GSA Order are applicable to micro-purchases and the use of the GSA Purchase Card.

8. Will there be training?

GSA's Office of Government-wide Policy (OGP), with help from GSA's Office of the Chief Information Security Officer (CISO), is designing and developing training on ensuring understanding and compliance with the GSA policies outlined in this AL.

Once the requirements of OMB M-22-18 are incorporated into the FAR, GSA's associated training will be adapted to the final FAR rule as applicable and made available to the workforce via FAI CSOD.

9. Points of Contact.

- For any general policy questions regarding this AL, questions may be directed to GSARPolicy@gsa.gov.
- For any specific questions regarding GSA IT Information Standards, questions must be directed to it-standards@gsa.gov.

ATTACHMENT A – MESSAGE SENT TO INDUSTRY

On January 11, 2023, GSA's Senior Procurement Executive Jeff Koses and GSA's Chief Information Officer David Shive jointly signed Acquisition Letter MV-23-02, *Ensuring Only Approved Software is Acquired and Used at GSA*.

What does the policy say?

MV-23-02 reminds GSA contracting activities of current GSA acquisition policy and current GSA information technology policy that must be followed to ensure only approved software is procured and used at GSA.

GSA's acquisition regulations (GSAM 511.170(d)) require GSA's Information Technology (IT) Office to approve new software before its use at GSA. To comply with Executive Order 14028 and OMB Memorandum M-22-18, which require federal agencies to only use software that complies with Government-specified secure software development practices, GSA IT will update its processes to approve software including requiring vendor attestations. GSA IT anticipates issuing an updated attestation process by June 12, 2023.

What does this mean for you?

Under GSA's implementation, GSA will begin collecting attestation letters as part of pre-award and post-award contract deliverables in mid-June 2023 for all impacted software, regardless of whether or not the software is considered critical. When collecting attestations, GSA anticipates using the Cybersecurity & Infrastructure Secure Agency (CISA) Common Form once the form is provided for agency use. GSA expects the form to be ready before June 2023, and GSA will help to communicate and distribute the form when it is available. When available, GSA will provide a link to the CISA form from the Acquisition Policy Library and Resources page on GSA.gov under the "Resources" section.

Contractors providing GSA with a cloud-based solution are encouraged to work with the Federal Risk and Authorization Management Program (FedRAMP). The FedRAMP approval process will streamline the GSA IT Standards Process allowing for a timely contract start. GSA also anticipates that leveraging FedRAMP will ensure and streamline compliance with requirements of OMB Memo M-22-18 in the future.

Contractors supporting GSA on-premises (non-cloud) Federal Information Systems will also be impacted. Once the CISA Common Form is issued, contractors should complete the form in accordance with any further CISA/OMB instructions or the pending instructions from GSA IT.

If you use a GSA contract vehicle to sell to other agencies, (such as a Federal Supply Schedule, GWAC, OASIS, etc), for now GSA will allow, but not require, you to attest at the contract level so you don't have to do so, repetitively, for each and every order. GSA anticipates that a forthcoming FAR rule will provide definitive instructions for the requirements of the attestation at the contract level.