GSA Office of Government-wide Policy

9/16/2022

Acquisition Letter MV-22-06

MEMORANDUM FOR PBS LEASING CONTRACTING ACTIVITIES

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

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

SUBJECT: Cyber-Supply Chain Risk Management (C-SCRM) Requirements for Leasing

1. Purpose.

The purpose of this acquisition letter (AL) is to clarify the C-SCRM requirements, including provisions and clauses, that must be considered for inclusion in the acquisition of leasehold interests in real property[1] (lease acquisitions).

2. Background.

Almost all of GSA's procurements, including lease acquisitions, can introduce cybersecurity risks to the Government. For example, Federally leased-facilities may contain building and access control systems--computers that monitor and control building operations such as elevators, electrical power, and heating, ventilation, and air conditioning--that are increasingly being connected to other information systems and the Internet.

Further, the adoption and integration of Internet of Things (IoT) and Industrial Internet of Things (IIoT) devices have led to an increasingly interconnected mesh of systems–not just building and access control systems–which expands the attack surface and blurs the once clear functions of cybersecurity and physical security.[2]

The increased connectivity heightens PBS-leased facilities' vulnerability to cyber attacks, which could compromise security measures, hamper our Federal tenant agencies' ability to carry out their missions, or cause physical harm to the facilities or their occupants.

[1] Except as noted at GSAR 570.101

[2] Cybersecurity and Physical Security Convergence, Cybersecurity & Infrastructure Security Agency (CISA)

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

Additionally, as noted in previous GSA Orders[3], a series of recent Government-wide and GSA-specific policy changes have highlighted the importance of the Federal Government's goal to improve its focus on C-SCRM acquisition and considerations.

This AL supplements those policies by addressing the growing nature of cyber-supply chain risks that must be considered during the pre-award and post-award phases by the lease contracting officer and any other members of the leasing acquisition team.

3. Effective Date.

This AL is effective immediately and remains in effect until rescinded or incorporated into the General Services Acquisition Regulation (GSAR).

GSA is also aware of C-SCRM-related cases on the Regulatory Agenda[4] that will impact GSA, and may be applicable to lease acquisitions. This AL, or the GSAR, may be updated in the future to account for C-SCRM rules impacting lease acquisitions.

4. Applicability.

New Lease Contracting Actions

Beginning on 10/01/2022, the provisions and clauses listed in Attachment A, as well as the requirement considerations in Attachment B, are required, as applicable, to all new lease contracting actions (including leasing activities delegated by GSA to other Federal agencies). Specifically:

- For any open solicitation, the solicitation must be either amended prior to close or the clauses incorporated into the award prior to signature.
- For any future solicitation, the solicitation must be amended prior to award.

Existing Leases

- Existing FBI leases
  - By 05/01/2023, existing Federal Bureau of Investigation (FBI) leases must be bilaterally modified to include the required clauses and requirements listed in Attachment A and Attachment B.
- Existing leases for all other agencies
  - The modification of existing leases for all agencies other than the FBI will be addressed in a future supplement to this AL.

[3] GSAM Case 2021-G511 and GSAM Case 2021-G512

[4] Unified Agenda of Regulatory and Deregulatory Actions (Agenda) reports on the actions administrative agencies plan to issue in the near and long term. Released by the Office of Information and Regulatory Affairs, the Agenda provides important public notice and transparency about proposed regulatory and deregulatory actions within the Executive Branch.

Updating Leasing Templates

Beginning 10/01/2022, the following leasing templates (as well as any future relevant documents) must be updated to reflect the provisions, clauses, and requirements listed in Attachment A and Attachment B.

- General Clauses Template 3517A and 3517B
- Lease Contract Templates
- Request for Lease Proposal Templates

The templates must be further updated as additional C-SCRM related laws, statutes, regulations and/or policies are issued to meet deadline dates listed throughout this AL.

In addition, the Office of Leasing shall work expeditiously to revise appropriate policy and templates relevant to the requirements listed under Attachment B, as well as update its policy (e.g., Leasing Alerts (LA), Leasing Desk Guide (LDG)) and templates to reflect any new applicable C-SCRM related laws, statutes, regulations issued, or best practices and recommendations as issued by other GSA offices or agencies.

5. Requirements.

Acquisition Planning

- When the lease involves or may involve information technology or connected building systems (e.g., connected systems listed in Attachment C) the customer agency is responsible for the required information technology coordination and approval. As the servicing agency, GSA should ensure the CIO coordination is appropriately documented. It may be documented in the tenant occupancy agreement or a separate document, such as the Client Project Agreement. The Office of Leasing will work with relevant PBS offices (e.g., Office of Portfolio and Customer Engagement) to communicate such requirements.
- Future acquisition plans for new leases must include discussion of the reasoning when any C-SCRM-related provision or clause listed in Attachment A will not be included in the planned solicitation and resultant lease award. Such determinations shall be provided to the National Office of Leasing.
- Lease acquisition team members, including the HCA of the leasing contracting activity, must review General Services Acquisition Manual (GSAM) 504.470 for acquisitions involving classified information before accepting a reimbursable agreement for a requirement involving classified information.
- Though not required, leasing acquisition team members are not precluded from using the C-SCRM considerations outlined at GSAM 504.7004.
- Lease acquisition team members may review additional resources highlighted in Section 6 of this AL.

Solicitation and Contract Award

- Lease contracting officers must ensure that all C-SCRM-related provisions and clauses listed in Attachment A and the requirements and considerations of Attachment B are incorporated into solicitations and awards for new lease contracts when required by the prescription and as documented in the acquisition plan. Any C-SCRM-related representation clause requiring review (e.g., "FAR 52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment") must be completed as a condition for award.
- Lease acquisition team members should communicate and highlight the applicable provisions, clauses, and requirements to potential offerors as part of the market outreach/survey process.
- In collaboration with the customer agency, lease acquisition teams should consider utilizing a C-SCRM related evaluation factor as part of the source selection process including for low-priced technically acceptable offers. For example, a factor could consider the cyber protection measures used to safeguard facilities and occupants by the lessors. Depending on the requirements and mission of the customer agency, this type of factor may be helpful in supporting a trade-off between lessors prioritizing cyber-hygiene and lessors that are not.

Pre and Post-Award

- For any potential cyber-supply chain event, including occurrence of an IT security incident, discovery of a prohibited article or source (e.g., an affirmative response under FAR 52.204-24 or 52.204-26), or identification of supply chain risk information, the lease contracting officer or another acquisition team member must contact the GSA IT Service Desk by phone at 866-450-5250 or by email at ITServiceDesk@gsa.gov[5].
- The lease contracting officer must review C-SCRM related representations and certifications prior to exercising options, or extensions or renewals, or at least annually when applicable (e.g. GSAR 552.270-33, Foreign Ownership and Financing Representation for High-Security Leased Space).

The FAR or GSAR provisions or clauses must not include any deviations unless an approved deviation specific to the relevant provision or clause is signed by the GSA Senior Procurement Executive. Active deviations can be found on GSA InSite's Acquisition Policy Library.

6. Additional References, Resources, and Guidance.

- GSA's C-SCRM Insite page (insite.gsa.gov/cscrm)

[5] GSAM 504.7005

7. Points of Contact.

- For any general policy questions regarding this AL, questions may be directed to GSARPolicy@gsa.gov.
- For any specific questions regarding implementing the requirements of this AL, questions should be directed to ASKPR@gsa.gov.

Attachments

- Attachment A – C-SCRM Provisions and Clauses for Leasing Contracts
- Attachment B – GSA Policies and Requirements Related to C-SCRM
- Attachment C – Examples of Connected Systems in Buildings

ACQUISITION LETTER MV-22-06
ATTACHMENT A
C-SCRM Provisions and Clauses for Leasing Contracts

The following provisions and clauses, as applicable, must be included in leasing solicitations and/or contracts. The list below does not reflect the representations and certifications captured through FAR provision 52.204-7, System for Award Management, FAR provision 52.204-8, Annual Representations and Certifications, or FAR clause 52.204-19, Incorporation by Reference of Representations and Certifications.

FAR Provisions and Clauses		
Title	**Provision/Clause**	**Where Prescribed**
52.204-2, Security Requirements	Clause	4.404(a)
52.204-9, Personal Identity Verification of Contractor Personnel	Clause	4.1303
52.204-21, Basic Safeguarding of Covered Contractor Information Systems	Clause	4.1903
52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities	Clause	4.2004
52.204-24, Representation Regarding Certain Telecommunications and Video Surveillance Services or Equipment	Provision	4.2105(a) (see also LA-20-11)
52.204-25, Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment	Clause	4.2105(b) (see also LA-20-11)
52.204-26, Covered Telecommunications Equipment or Services-Representation	Provision	4.2105(c) (see also LA-20-11)
GSAM/R Provisions and Clauses		
Title	**Provision/Clause**	**Where Prescribed**
552.204-9, Personal Identity Verification Requirements	Clause	504.1303

552.270-33, Foreign Ownership and Financing Representation for High-Security Leased Space	Clause	570.703(c)
552.270-34, Access Limitations for High-Security Leased Space	Clause	570.703(d)

ACQUISITION LETTER MV-22-06
ATTACHMENT B
GSA Policies and Requirements Related to C-SCRM

Policy/Reference	**GSA Order PBS 3490.3 CHGE 1**
Title	**Security for Sensitive Building Information Related to Federal Buildings, Grounds, or Property**
Notes	This Order applies to all entities that handle, receive, and store CUI building information related to GSA-controlled space, as well as to the access to and generation, dissemination, storage, transfer, and disposal of all such information. It also applies to procurements to acquire, alter, or manage space, either Government-owned or leased, including GSA space that is delegated to other Federal agencies. **Appendix C (within the Order) includes CUI language for all solicitations containing CUI information (including Requests for Lease Proposals)**
See also	**GSA Order CIO 2103.2**, Controlled Unclassified Information (CUI) Policy
Policy/Reference	**LA-18-05**
Title	**Cybersecurity Measures for Leased Facilities**
Notes	This leasing alert provides required and recommended measures for lessors related to cybersecurity protections and precautions in leased facilities. **Section 2 (within the LA) provides required measures and recommended guidance, and Attachment 1 provides cybersecurity language that was added to Federal Security Level (FSL) templates.**

ACQUISITION LETTER MV-22-06
ATTACHMENT C
Examples of Connected Systems in Buildings[6]

PBS-leased facilities may include various types of connected systems, such as parts, equipment, services, and technologies that can be a target for cyber-events. Below is a sample list of some of those connected systems. Understanding the needs and mission of your customer agency, as well as any Office of the Chief Information Officer (OCIO) (or similar office) policy the customer may have, can help mitigate C-SCRM risk.

Common Systems in Federal Facilities	Connected Systems
Closed Circuit Camera Systems	Cameras, televisions or monitors, and recording equipment, and provide video surveillance capabilities
Access Control Systems	Card readers, control panels, access control servers, and infrastructure such as door actuators and communications lines, which restrict access to authorized persons
Fire Annunciation and Suppression Systems	Fire alarms, emergency communication equipment, and water-based or nonwater-based suppression systems, designed to prevent, extinguish, or control a fire or other life safety event
Building Automation Systems (commonly manages the HVAC)	Also known as energy management control systems, provide centralized control—through the use of software and hardware (e.g., computer, modems, sensors, controllers, and printers)—to monitor and adjust building systems (e.g., temperature settings and schedules for running equipment)—such as a building's cooling systems.
Power and Lighting Control Systems	Lighting devices and their controls, advanced-metering controls, power distribution systems, and emergency power or lighting systems, which are also often managed through a building automation system

[6] Table and graphic in Attachment C are adapted from GAO-15-6

Elevator Control Systems	Operating machinery, safety systems, and a control system or panel