



Alliant 3 Unrestricted GWAC
Solicitation Number: 47QTCB24R0009
ATTACHMENT J.P-11



A3 Contractor C-SCRM Responsibility Questionnaire

Offeror Information:

Name of the offeror (legal entity, company name):
Name of the primary Point-Of-Contact (POC) for the offeror:
E-mail Address of the primary POC for the offeror:
Phone number of the primary POC for the offeror:

Please put an "X" after each question to represent "Yes" or "No". All sections must be completed, and signature is required at bottom of form.

Basic Safeguarding of Covered Contractor Information Systems Responsibility Assessment (FAR 52.204-21):

Section 1: Access Control (NIST SP 800-53 Controls: AC-2, AC-3, AC-17, AC-20, AC-22)

- 1.1 Does your organization limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems)?
Yes ____ No ____
- 1.2 Does your organization limit information system access to the types of transactions and functions that authorized users are permitted to execute?
Yes ____ No ____
- 1.3 Does your organization verify and control/limit connections to and use of external information systems?
Yes ____ No ____
- 1.4 Does your organization control information posted or processed on publicly accessible information systems?
Yes ____ No ____

Section 2: Identification and Authentication (NIST SP 800-53 Controls: IA-2, IA-3, IA-5)

- 2.1 Does your organization identify information system users, processes acting on behalf of users, or devices?
Yes ____ No ____
- 2.2 Does your organization authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems?
Yes ____ No ____

Section 3: Media Protection (NIST SP 800-53 Controls: MP-2, MP-4, MP-6)

- 3.1 Does your organization sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse?
Yes ____ No ____

Section 4: Physical Protection (NIST SP 800-53 Controls: PE-2, PE-3, PE-4, PE-5, PE-6)

- 4.1 Does your organization limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals?
Yes ____ No ____
- 4.2 Does your organization escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices?
Yes ____ No ____

Section 5: System and Communications Protection (NIST SP 800-53 Controls: SC-7)

5.1 Does your organization monitor, control, and protect organizational communications (i.e., information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems?

Yes _____ No _____

5.2 Does your organization implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks?

Yes _____ No _____

Section 6: System and Information Integrity (NIST SP 800-53 Controls: SI-2, SI-3, SI-5)

6.1 Does your organization identify, report, and correct information and information system flaws in a timely manner?

Yes _____ No _____

6.2 Does your organization provide protection from malicious code at appropriate locations within organizational information systems?

Yes _____ No _____

6.3 Does your organization update malicious code protection mechanisms when new releases are available?

Yes _____ No _____

6.4 Does your organization perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed?

Yes _____ No _____

FAR 52.204-23, Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities**Section 7: (FAR 52.204-23)**

7.1 Does your organization certify it does not utilize hardware, software, and services developed or provided by Kaspersky Lab and other covered entities in accordance with FAR Clause 52.204-23?

Yes _____ No _____

Section 889 Compliance**Section 8: (FAR 52.204-25, FAR 52.204-26, FAR 52.204-24)**

8.1 Does your organization certify that it does not utilize certain telecommunications and video surveillance services or equipment in accordance with FAR Clause 52.204-25 by:

- 1) Completing the fill-in provision located at FAR 52.204-26?
- 2) Including the representation in Section K of your organization's Alliant 3 Proposal?

OR

Does your organization provide representation that it does not utilize certain telecommunications and video surveillance services or equipment in accordance with FAR Provision 52.204-24 by:

- 1) Completing the fill-in provision located at FAR 52.204-24?
- 2) Including the representation in Section K of your organization's Alliant 3 Proposal?

Yes _____ No _____

Federal Acquisition Supply Chain Security Act Orders

Section 9: (FAR 52.204-29, FAR 52.204-30, Alt 1)

9.1 Does your organization certify that it complies with the provision at FAR 52.204-29, Prohibition from providing or using as part of the performance of the contract any covered article, or any products or services produced or provided by a source, if the prohibition is set out in an applicable Federal Acquisition Supply Chain Security Act (FASCSA) order, as described in paragraph (b)(1) of FAR 52.204-30, Federal Acquisition Supply Chain Security Act Orders?

Yes _____ No _____

9.2 Does your organization certify that complies with the Clause at FAR 52.204-30, Federal Acquisition Supply Chain Security Act Orders—Prohibition, Alt. 1

Yes _____ No _____

Certification of Responses

I understand that a response of "no" to any of the items above disqualifies my organization from receiving an Alliant 3 GWAC Master Contract award. I understand that a separate risk assessment will be conducted by GSA and that an approval is required to be eligible for award. I hereby certify that, to the best of my knowledge, the provided information is true and accurate.

(Signature Required)

DATE: _____