PR002256

Viasat Supply-Chain Information Security Assessment

# Purpose & Scope

The purpose of this questionnaire is to gain representation & certification from your organization as to its current profile and state-of-compliance regarding DFARS Clause 252.204-7012 / 7019 / 7020 and future CMMC requirements. This questionnaire is issued to Viasat Supply-Chain partners that provide products and services in support of government contracts and/or receive, store, process, and/or generate Federal Contract Information (FCI) or Controlled Unclassified Information (CUI).

Viasat is required to implement the U.S. Government’s cybersecurity requirements, including FAR and DFARS clauses, and in turn, these requirements must be flowed down to contractors and subcontractors (at all tiers) to provide adequate security to safeguard FCI and/or CUI in performance of the contract, or subcontract, as applicable.

FAR 52.204-21 – Requires supplier’s compliance prior to contract award with a select subset of NIST SP 800-171 “basic safeguarding” cybersecurity controls for internal systems with Federal Contract Information (FCI).

DFARS 252.204-7012 – Requires supplier’s implementation of NIST SP 800-171, prior to contract award, which includes cybersecurity controls for internal systems with “Controlled Unclassified Information” (CUI).

DFARS 252.204-7019 and DFARS 252.204-7020 – Prior to award, suppliers must conduct a basic self-assessment of the 110 NIST 800-171 controls for each information system that will handle Covered Defense Information (CDI) and submit resulting scores to the Department of Defense (DoD) Supplier Performance Rating System (SPRS). If the Government requests a medium or high-assurance assessment, supplier must give the Government access to its facilities, systems, and personnel to conduct said assessment.

DFARS 252.204-7021 - The CMMC DFARS Rule is supposed to be published in the Spring of 2024.

# Instructions

1) Please complete the questionnaire below for your entity referred to as “Seller”

2) Inability to complete the DFARS Information Security Assessment may result in Viasat’s inability to “flow-down” FCI or CUI to supply-chain partners.

3) If you have any questions about completing the form, please contact the following organization mailbox: [supplychainsecurity@viasat.com](mailto:supplychainsecurity@viasat.com).

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | Question / Requirement | | | YES | NO | |
| 1 | Is Seller providing only true COTS items without modifications and does not anticipate it will collect, develop, receive, transmit, use or store FCI or CUI as defined in DFARS Clause 252.204-7012? Note: If Seller is providing a mixture of true COTS items as well other products or services, that may be commercial in nature or non-commercial to Viasat, then Seller does not qualify for the COTS item exemption. | | |  |  | |
| 2 | Does Seller meet the requirements of FAR 52.204-21 “Basic Safeguarding of Covered Contractor Information Systems”?  To be compliant, all 15 NIST FAR 52.204-21 controls must be fully implemented.  The 15 requirements cannot be met with a Plan of Action and Milestone (POAM). | |  | |  | |
| 3 | Does Seller currently hold a DoD approved Medium Assurance Certificate for cyber incident reporting?  Please provide the name of the Issuer: \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ | |  | |  | |
| 4 | Does Seller meet the requirements of DFARS 252.204-7012 “Safeguarding Covered Defense Information and Cyber Incident Reporting”?  “*Meeting the requirements equals a system security plan has been generated, a POAM if applicable has been generated, and a SPRS score has been submitted.”* | | |  |  | |
| 5 | What is your current CMMC status?  “*Score must be inputted on CMMC tab in SPRS.*”  Option 1: CMMC Level 1 (Self-Assessment)  Option 2: CMMC Level 2 (Self-Assessment)  Option 3: CMMC Level 2 (C3PAO)  Option 4: CMMC Level 3 (DIBCAC) | Please select one option here | | | |  |
| 6 | (I) Is Seller’s CMMC assessment score in SPRS 88 or greater? :  (II) Provide the date the score was submitted to SPRS: \_\_\_\_\_\_\_\_  If “No” to question 5, Seller is operating under a Plan of Action and Milestones (POAM). If SPRS score is 110, write “N/A” on section (III) & (IV).    (III) Please provide the POAM closure date: \_\_\_\_\_\_\_\_    (IV) Which NIST 800-171 controls with a value of “5” in accordance with the NIST 800-171 Scoring Methodology are not implemented? (e.g., 3.5.3, 3.6.1, etc.) | | |  |  | |
|  |  | | |  |  | |
|  |  | | |  |  | |

|  |  |  |
| --- | --- | --- |
| Company Name of Seller-Offeror | | |
| Name of Authorized Representative (Type) | Title of Authorized Representative(Type) | |
| E-Mail Address (Type) | | Phone (Type) |
| Signature | | Date |

# Helpful References

# DFARS Procedures, Guidance, and Information (PGI)

# <https://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html>

Frequently Asked Questions (FAQs) regarding the implementation of DFARS Subpart 204.73 and PGI Subpart 204.73; DFARS Subpart 239.76 and PGI Subpart 239.76.

<https://dodprocurementtoolbox.com/cms/sites/default/files/resources/2021-11/Cyber%20DFARS%20FAQs%20rev%203%20%207.30.2020%20%2B%20correction%2011.23.2021.pdf>

DOD Procurement Toolbox

<http://dodprocurementtoolbox.com/site-pages/cybersecurity-policy-regulations>

DoD Supplier Performance Risk System (SPRS)

<https://www.sprs.csd.disa.mil/>