PR002256

Viasat Subcontractor/Supplier Cybersecurity 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 FAR 52.240-93, DFARS Clause 252.204-7012, 252.240-7997, and 252.204-7021 Cybersecurity Maturity Model Certification (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 52.240-93 – 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 252.240-7997 – Requires Supplier provide access to its facilities, systems, and personnel necessary for the Government to conduct a Medium or High NIST SP 800-171 DoD Assessment, using the methodology described at 32 CFR 170.24, if necessary. The results of Medium or High NIST SP 800-171 DoD Assessments, when conducted by DCMA, will take precedence over any other assessment, in accordance with 32 CFR 170.16(a)(1)(iv), 32 CFR 170.17(a)(1)(iv), and 32 CFR 170.18(a)(1)(iv).

DFARS 252.204-7021 – Requires Supplier have and maintain for the duration of the contract a current CMMC status at the following CMMC level, or higher: CMMC Level 1 (Self); CMMC Level 2 (Self); CMMC Level 2 (C3PAO); or CMMC Level 3 (DIBCAC) for all information systems used in performance of the contract, task order, or delivery order that process, store, or transmit FCI or CUI.

Note: Effective February 1, 2026, Department of Defense's (DoD) Revolutionary Federal Acquisition Regulation Overhaul (RFO) implemented Phase 1 class deviations and DFARS 252.204-7019 and 252.204-7020 have been retired.

Instructions

1) Please complete the questionnaire below for your entity referred to as "Seller". All responses should be specific to the performing site.

2) Inability to complete the Viasat Subcontractor/Supplier Cybersecurity Assessment may result in Viasat's inability to "flow-down" FCI or CUI to its supply chain partners.

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

Cybersecurity Assessment

	Question/Requirement	Yes	No
1	Is Seller ONLY providing true commercially available off-the-shelf (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 performing anything other than providing true COTS, please select 'No'.	☐	☐
2	Does Seller meet the requirements of FAR 52.240-93 "Basic Safeguarding of Covered Contractor Information Systems"? *"To be compliant, all 15 NIST FAR 52.204-21 controls must be fully implemented and cannot be met with a Plan of Action and Milestone (POAM).* *Meeting the requirement: Attestation in SPRS of CMMC Level 1 (Self) and CMMC Unique Identifier (UID).*	☐	☐
3	Does Seller currently hold a DoD-approved Medium Assurance Certificate for cyber incident reporting per DFARS 252.204-7012? Provide the name of the Issuer: _____ *Meeting the requirement: Seller holds the DoD approves Medium Assurance Certificate*	☐	☐
4	Does Seller meet the requirements of DFARS 252.204-7012 "Safeguarding Covered Defense Information and Cyber Incident Reporting"? *Meeting the requirement: A system security plan has been generated, a POAM if applicable has been generated, and a CMMC Level 2 SPRS score has been submitted.*	☐	☐
5	What is Seller's current CMMC status? Option 1: Final Level 1 (Self) Option 2: Conditional Level 2 (Self) Option 3: Final Level 2 (Self) Option 4: Conditional Level 2 (C3PAO) Option 5: Final Level 2 (C3PAO) Option 6: Conditional Level 3 (DIBCAC) Option 7: Final Level 3 (DIBCAC) *Meeting the requirement: Score must be inputted on CMMC tab in SPRS.*	Select CMMC Level	
6	Seller's CMMC Unique Identifier (UID) *Meeting the requirement: UID generated from SPRS website provided* If applicable: Level 2 CMMC Unique Identifier (UID): _____	Click or tap here to enter text.	

	Level 3 CMMC Unique Identifier (UID): _____		
7	Is Seller's CMMC assessment score in Supplier Performance Rating System (SPRS) 88 or greater?	Yes ☐	No ☐
8	Provide the date the score was submitted to SPRS:	Click or tap to enter a date.	
9	What is Seller's CMMC status expiration date?	Click or tap to enter a date.	

Company Name of Seller		
Name of Authorized Representative	**Title of Authorized Representative**	
E-Mail Address		**Phone**
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 (Rev 4)
https://dodprocurementtoolbox.com/uploads/Cyber_DFARS_FA_Qs_rev_4_6_13_24_4702075bf4.pdf

DOD Procurement Toolbox
http://dodprocurementtoolbox.com/site-pages/cybersecurity-policy-regulations

DoD Supplier Performance Risk System (SPRS)
https://www.sprs.csd.disa.mil/

Defense Industrial Base Network (DIBnet) – Medium Assurance Certificate
https://www.dc3.mil/Missions/DIB-Cybersecurity/DIB-Cybersecurity-DCISE/