DFARS 252.204-7012

Supply-Chain Information Security Assessment

Overview

The protection of Covered Defense Information (CDI) within covered contractor information systems has become a top priority for the DoD in order to mitigate its risk in sharing CDI with federal contractors. As a result, the DoD has implemented DFARS Clause 252.204-7012, “Safeguarding Covered Defense Information and Cyber Incident Reporting” which requires that all federal contractors provide “adequate security” by implementing the security requirements of the NIST 800-171 security framework no later than 31 December, 2017, or establish a plan-of-action to remediate controls not implemented or document approved, alternative but equally effective security measures to achieve equivalent protection.

Purpose

The purpose of this questionnaire is to gain representation & certification from your organization as to its current profile and state-of-compliance in regards to DFARS Clause 252.204-7012. This assessment is being issued to Viasat Supply-Chain partners that support DoD contracts in order to allow Viasat to determine its ability to share CDI and sensitive Viasat information with its partners. In addition, DFARS Clause 252.204-7012 institutes a mandatory flow-down requirement to suppliers / subcontractors storing, processing, creating, and/or providing CDI in performance of the contract.

DFARS clause 252.204-7012 was structured to ensure that unclassified DoD information residing on a contractor’s internal information system is safeguarded from cyber incidents via the implementation of the NIST 800-171 security framework, and that any consequences associated with the loss of this information are assessed and minimized via the cyber incident reporting and damage assessment processes. To meet “adequate security” standards, covered contractor information systems with CDI must comply with the 110 security controls contained within the NIST 800-171 security framework.

Scope

The requirements in DFARS clause 252.204-7012 must be implemented when CDI is processed, stored, or transits through an information system that is owned, or operated by or for, the contractor (Viasat) and its suppliers/subcontractors, or when performance of the contract involves operationally critical support. Viasat will indicate in the solicitation/contract when performance of the contract will involve, or is expected to involve, CDI or operationally critical support.

Instructions

1) Please complete the attached DFARS Security Assessment

2) Please note that completing the DFARS Information Security Assessment does not relieve your company of any of the clause’s requirements for reporting of cyber incidents and/or requirements to submit a Systems Security Plan (SSP) or plan-of-action document(s) IAW DFARS 252.204-7012 (21 October, 2016) & PGI 204.7303 (01 December, 2017).

3) Failure to complete the DFARS Information Security Assessment will result in Viasat unable to "flow-down" CDI to defense-related supply-chain partners.

4) If you have any questions about completing the form, please contact Jeffrey Bauer, Information Security & Risk Management, jeffrey.bauer@viasat.com. Thank you for your attention in responding to this request.

Assessment

Viasat anticipates that its suppliers/subcontractors may collect, develop, receive, transmit, use, or store Covered Defense Information (CDI) on suppliers'/subcontractors' covered contract information systems in support of a bid and proposal and/or execution of a purchase order or subcontract with Viasat.

Unless Seller represents and certifies to one of the exceptions below, the Seller shall represent and certify to their current state of compliance to DFARS Clause 252.204-7012. The Seller shall make its representation and certification by selecting one of the following (1) through (3) below. *Offerors selecting options 2 or 3 will acquire and maintain a DoD-approved "Medium Assurance Certificate" (as defined in DFARS 252.204-7012) to access the reporting module to report cyber incidents. Information to obtain a DoD approved "Medium Assurance Certificate" is available at https://dl.dod.cyber.mil/wp-content/uploads/eca/pdf/unclass-eca_cp_v4-5_final_signed.pdf*

1) The Seller represents and certifies that it either:

___ Has not collected, developed, received, transmitted, used, stored or had access to Covered Defense Information (CDI) and does not anticipate that it will collect, develop, receive, transmit, use or store CDI as defined in DFARS Clause 252.204-7012 in support of a bid and proposal and/or execution of a purchase order or subcontract with Viasat. Seller asserts that in the event it receives CDI from Viasat, Seller will delete and/or destroy the CDI and notify Viasat that it received CDI.

Or

___ Does not comply with the requirements of DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" (21 October, 2016) and has not implemented the requirements of NIST 800-171r1, "Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations".

2) The Seller represents and certifies that it:

___ Complies with the requirements of DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" (21 October, 2016) and has implemented the requirements of

NIST 800-171r1, “Protecting Controlled Unclassified Information in Nonfederal Information Systems and Organizations”; and possesses a System Security Plan (SSP) and associated plan-of-action to correct deficiencies that is available upon request in accordance with PGI 204.7303 (01 December, 2017).

3) The Seller represents and certifies that it:

___ Has a control(s)/process that varies from NIST 800-171R1, as documented by positive adjudication of the DOD CIO per DFARS 252.204-7012(b)(2)(ii)(B). The Seller will provide the documented variation and approved adjudication documentation to Viasat, upon request.

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

DPAP Website http://www.acq.osd.mil/dpap/dars/dfarspgi/current/index.html for DFARs Clauses, Procedures, Guidance and Information (PGI), and Frequently Asked Questions

Network Penetration Reporting & Contracting for Cloud Services (DFARS Case 2013-D018) Frequently Asked Questions (FAQ); 27 January, 2017
http://www.acq.osd.mil/dpap/pdi/docs/FAQs_Network_Penetration_Reporting_and_Contracting_for_Cloud_Services_(01-27-2017).pdf

DFARS Implementation Memo to DoD Entities
http://www.acq.osd.mil/dpap/policy/policyvault/USA002829-17-DPAP.pdf

DOD Procurement Toolbox http://dodprocurementtoolbox.com/site-pages/cybersecurity-policy-regulations
NIST 800-171A, “Assessing Security Requirements for Controlled Unclassified Information” (Draft)
https://csrc.nist.gov/CSRC/media/Publications/sp/800-171a/draft/sp800-171A-draft.pdf

NIST Handbook 162, “NIST MEP Cybersecurity Self-Assessment Handbook”
https://doi.org/10.6028/NIST.HB.162