Safeguarding Covered Defense Information – The Basics

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, is required in all contracts except for contracts solely for the acquisition of COTS items. In addition the Contractor shall include the clause in subcontracts for which performance will involve **covered defense information** or **operationally critical support.**

Covered defense information is used to describe information that requires protection under DFARS Clause 252.204-7012. It is defined as unclassified controlled technical information (CTI) or other information as described in the CUI Registry (http://www.archives.gov/cui/registry/category-list.html), that requires safeguarding/dissemination controls **AND IS EITHER** marked or otherwise identified in the contract and provided to the contractor by DoD in support of performance of the contract; **OR** collected/developed/received/transmitted/used/stored by the contractor in performance of contract.

Operationally critical support is defined as supplies/services designated by the Government as critical for airlift, sealift, intermodal transportation services, or logistical support that is essential to the mobilization, deployment, or sustainment of the Armed Forces in a contingency operation.

DFARS Clause 252.204-7012 requires contractors/subcontractors to:

1) **Safeguard covered defense information**
2) **Report cyber incidents**
3) **Submit malicious software**
4) **Facilitate damage assessment**

1) **To safeguard covered defense information** contractors/subcontractors must implement **NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations**, as soon as practical, but not later than Dec 31, 2017
   - For contracts awarded prior to 1 Oct 2017, contractors/subcontractors shall notify DoD CIO within 30 days of contract award of any NIST SP 800-171 security requirements not implemented at the time of contract award.
   - If the offeror proposes to vary from NIST SP 800-171, they shall submit to the CO a written explanation of why a security requirement is not applicable **OR** how an alternative security measure is used to achieve equivalent protection
2) **To report cyber incidents** that affect covered defense information or that affect the contractor's ability to perform requirements designated as operationally critical support, the Contractor shall conduct a review for evidence of compromise and rapidly report cyber incidents to DoD at https://dibnet.dod.mil via an incident collection form (ICF).
3) If discovered and isolated in connection with a reported cyber incident, the contractor/ subcontractor shall **submit the malicious software** to the DoD Cyber Crime Center (DC3).
4) If DoD elects to conduct a damage assessment, the Contracting Officer will be notified by the requiring activity to **request media and damage assessment information from the contractor**.

Safeguarding Covered Defense Information – The Questions and Concerns

Who is responsible for identifying and marking covered defense information?

The DoD requiring activity is responsible for identifying covered defense information (CDI) in accordance with DoD procedures for identification and protection of controlled unclassified information found in DoDM 5200.01 Vol 4, DoD Information Security Program: Controlled Unclassified Information (CUI). The requiring activity is also responsible for determining the appropriate marking for the CDI in accordance with the procedures for applying distribution statements on technical documents found in DoDM 5200.01 Vol 4 and DoDI 5230.24, Distribution Statements on Technical Documents. The requiring activity must document in the Statement of Work that CDI is required for performance of the contract, and specify requirements for the contractor to mark the CDI developed in the performance of the contract.

Why NIST SP 800-171, Protecting CUI in Nonfederal Information Systems and Organizations?

The NIST SP 800-171 was written using performance-based security requirements to enable contractors to use systems and practices they already have in place to process, store, or transmit CUI. It eliminates unnecessary specificity and includes only those security requirements necessary to provide adequate protection. Though most requirements in NIST SP 800-171 are about policy, process, and configuring IT securely, some require security-related software or additional hardware.

Will the DoD monitor contractors to ensure implementation of the required security requirements?

The DFARS rule does not add any unique/additional requirements for the DoD to monitor contractor implementation. Nor does the rule require "certification" of any kind, either by DoD or any other firm professing to provide compliance, assessment, or certification services for DoD or Federal contractors. The DoD will not recognize 3rd party assessments or certifications. By signing the contract, the contractor agrees to comply with the terms of the contract.

The contractor's system security plan (SSP) – required by NIST SP 800-171 - documents how the organization meets, or plans to meet, the NIST SP 800-171 requirements. When requested by the requiring activity, the SSP (or elements of the SSP) may be used to demonstrate implementation of NIST SP 800-171 or to inform a discussion of risk between the contractor and requiring activity.

When should DFARS clause 252.204-7012 flow down to subcontractors?

The clause flows down to subcontractors without alteration, except to identify the parties, when performance will involve operationally critical support or CDI. The contractor will determine, and may consult with the contracting officer if necessary, if the information required for subcontractor performance retains its identify as CDI, thus necessitating flow-down of the clause. Flow-down is a requirement of the terms of the contract, which should be enforced by the prime contractor as a result of compliance with these terms. If a subcontractor does not agree to comply with the clause, CDI should not be on that subcontractor's information system.