AN OFFERING IN THE BLUE CYBER SERIES:

Following the Cybersecurity DFARS in your small business contract

Version 14 March 2022

#1 in the Blue Cyber Education Series

Federal Acquisition Regulation (FAR) and DFARS

Small Business contracts contains many FARS and DFARS, some are listed some are referenced and you have to look them up. These are not all, but some key security requirements.

What is a DFARS? The Defense Federal Acquisition Regulation Supplement (**DFARS**) contains requirements of **law**, DoD-wide policies, delegations of **FAR** authorities, deviations from **FAR** requirements, and policies/procedures that have a significant effect on the public.

- DFARS Clause 252.239-7010 Cloud Computing Services
- FAR Clause 252.204-21 Basic Safeguarding of Covered Contractor Information Systems
- DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting
- DFARS Clause 252.204-7008 Compliance with safeguarding covered defense information controls
- DFARS Clause 252.204-7019/20 NIST SP 800-171 DoD Assessment Requirements.
- DFARS Clause 252.204-7021 Cybersecurity Maturity Model Certification Requirement

DFARS Clause 252.239-7010 — Cloud Computing Services

Applies when a cloud solution is being used to process data on the DoD's behalf or DoD is contracting with Cloud Service Provider to host/process data in a cloud

Ensures that the cloud service provider:

- **Meets requirements of the DoD Cloud Computing Security Requirements Guide**
- **Use government-related data only to manage the operational environment that supports the Government data and for no other purpose**
- **Complies with requirements for cyber incident reporting and damage assessment**

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting, applies when a contractor intends to use an external cloud service provider to store, process, or transmit covered defense information in the performance of a contract. DFARS Clause 252.204-7012 requires the cloud service provider to meet security requirements equivalent to those established for the Federal Risk and Authorization Management Program (FedRAMP) Moderate baseline.

FAR Clause 52.204-21 Basic Safeguarding of Covered Contractor Information Systems

Safeguarding requirements and procedures

(1) The Contractor shall apply the following basic safeguarding requirements and procedures to protect covered contractor information systems. Requirements and procedures for basic safeguarding of covered contractor information systems shall include, at a minimum, the following security controls:

- The FAR lists 15 security controls, which correspond to 17 NIST SP 800-171 requirements

(2) *Other requirements.* This clause does not relieve the Contractor of any other specific safeguarding requirements specified by Federal agencies and departments relating to covered contractor information systems generally or other Federal safeguarding requirements for controlled unclassified information (CUI) as established by Executive Order 13556.

Flow-down the requirement

The Contractor shall include the substance of this clause, including this paragraph (c), in subcontracts under this contract (including subcontracts for the acquisition of commercial items, other than commercially available off-the-shelf items), in which the subcontractor may have Federal contract information residing in or transiting through its information system.

DFARS Clause 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

- Report cyber incidents
- Submit malicious software
- Facilitate damage assessment
- Safeguard covered defense information

Where to Report Cyber Incidents/Malware

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).

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). Also, https://dibnet.dod.mil

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

Safeguard Covered Defense Information (CDI)

CDI is defined as unclassified controlled technical information (CTI) or other information as described in the DOD CUI Registry

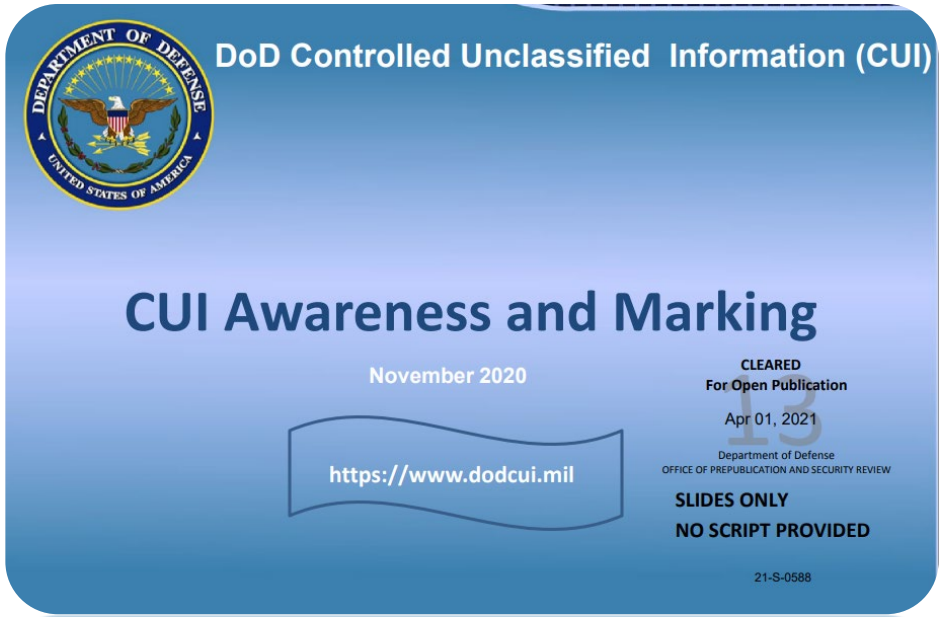
AND is marked as CDI

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.

Safeguard CDI: What is CUI?

Detailed training on what constitutes CUI is available from the DOD at this link: https://www.dodcui.mil



Safeguard CDI: What is CTI?

Controlled Technical Information (CTI) means technical information with military or space application that is subject to controls on the access, use, reproduction, modification, performance, display, release, disclosure, or dissemination.

Controlled technical information is to be marked.

The term does not include information that is lawfully publicly available without restrictions.

"Technical Information" means technical data or computer software, as those terms are defined in Defense Federal Acquisition Regulation Supplement clause 252.227-7013, "Rights in Technical Data - Noncommercial Items"

Examples of technical information include: research and engineering data, engineering drawings, and associated lists, specifications, standards, process sheets, manuals, technical reports, technical orders, catalog-item identifications, data sets, studies and analyses and related information, and computer software executable code and source code.

Safeguard CDI: Implementation of NIST SP 800-171

Implementation of the NIST SP 800-171 involves implementing and documenting the 110 security requirements listed in the document.

- **The implementation of security requirements is recorded in a System Security Plan (NIST SP 800-171 security requirement 3.12.4) and**
- **Any un-implemented security requirement and it's interim plan to provide alternative, but equally effective, security measure is recorded in a Plan of Action with Milestones, called a POAM (NIST SP 800-171 security requirement 3.13.2)**

Help with understanding the NIST SP 800-171 security requirements is found at this link: https://nvlpubs.nist.gov/nistpubs/hb/2017/NIST.HB.162.pdf

DFARS Clause 252.204-7008 Compliance with safeguarding covered defense information controls

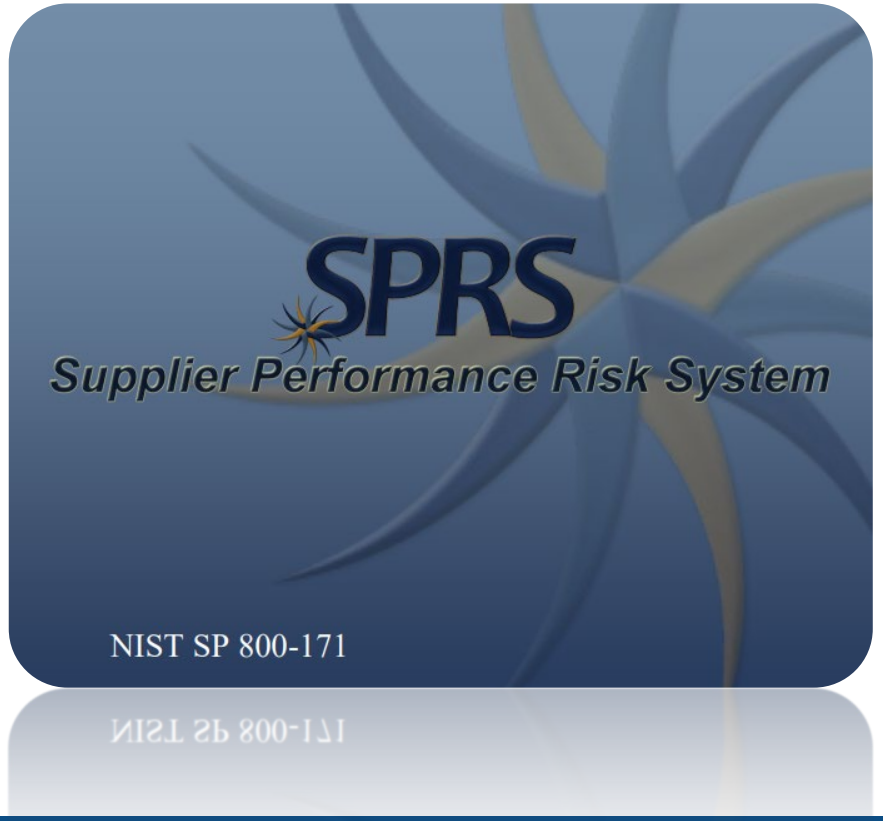
States "By submission of this offer, the Offeror represents that it will implement the security requirements specified by NIST SP 800-171, … not later than December 31, 2017.

If the Offeror proposes to vary from any of the security requirements specified by NIST SP 800-171 …, the Offeror shall submit to the Contracting Officer, for consideration by the DoD Chief Information Officer (CIO), a written explanation of:

- **Why a particular security requirement is not applicable**
- **How an alternative but equally effective**, security measure is used to compensate for the inability to satisfy a particular requirement and achieve equivalent protection.
- **An authorized representative of the DoD CIO** will adjudicate offeror requests to vary from NIST SP 800-171 requirements in writing **prior to contract award**. Any accepted variance from NIST SP 800-171 shall be incorporated into the resulting contract.

DFARS Clause 252.204-7019/20
NIST SP 800-171 DoD Assessment Requirements.

- Self-Assessment
- Submit information to SPRS.CSD.DISA.MIL
- Flow the Requirement Down
- Update your Self-Assessment



NIST SP 800-171 DoD Assessment Requirements

This clause applies to covered contractor information systems that are required to comply with the NIST(SP) 800-171, in accordance with DFARS clause at 252.204-7012, Safeguarding Covered Defense Information and Cyber Incident Reporting

Supplier Performance Risk System (SPRS) is a sophisticated website is ready to record your Self-Assessment https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf

The Contractor shall not award a subcontract or other contractual instrument, that is subject to the implementation of NIST SP 800-171 security requirements, in accordance with DFARS clause 252.204-7012 of this contract, unless the subcontractor has completed, within the last 3 years, at least a Basic NIST SP 800-171 DoD Assessment

DFARS Clause 252.204-7021
Cybersecurity Maturity Model Certification Requirement

This DFARS is under review and it's status will not be known until late 2022 at the earliest.

Until then, compliance with and full implementation of DFARS Clause 252.204-7012, "Safeguarding Covered Defense Information and Cyber Incident Reporting" is sufficient.

For more information on the new version of CMMC, see this great webinar by the DCMA Director John Ellis.
https://www.preveil.com/resources/webinar-john-ellis-on-cmmc-2-0/

Stay up-to-date at www.acq.osd.mil/cmmc/

Prohibition on Contracting for some items

SBIR/STTR contract contains many requirements. Many talk to not contracting with certain entities for certain items.

FAR 52.204-23
Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities

FAR 52.204-25
Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

52.204-23 Prohibition on Contracting for Hardware, Software, and Services Developed or Provided by Kaspersky Lab and Other Covered Entities.

Section 1634 of Division A of the National Defense Authorization Act for Fiscal Year 2018 (Pub. L. 115-91) prohibits Government use of any covered article. The Contractor is prohibited from—

(1) Providing

(2) Using

You must report exceptions

In the event the Contractor identifies a covered article provided to the Government during contract performance, or the Contractor is notified of such by a subcontractor at any tier or any other source, the Contractor shall report, in writing, to the Contracting Officer or, in the case of the Department of Defense, to the website at https://dibnet.dod.mil.

You must Flow the requirement down to subcontractors

All of these DFARS have many facets; this briefing is a high-level look

Covered article means any hardware, software, or service that–

(1) Is developed or provided by a covered entity;

(2) Includes any hardware, software, or service developed or provided In whole or in part by a covered entity; or

(3) Contains components using any hardware or software developed I in whole or in part by a covered entity.

Covered entity means–

(1) Kaspersky Lab;

(2) Any successor entity to Kaspersky Lab;

(3) Any entity that controls, is controlled by, or is under common control with Kaspersky Lab; or

(4) Any entity of which Kaspersky Lab has a majority ownership.

FAR 52.204-25 Prohibition on Contracting for Certain Telecommunications and Video Surveillance Services or Equipment

Prohibition

Prohibits the head of an executive agency, from procuring or obtaining, or extending or renewing a contract to procure or obtain, any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system. The Contractor is prohibited from providing to the Government any equipment, system, or service that uses covered telecommunications equipment or services as a substantial or essential component of any system, or as critical technology as part of any system, unless an exception has been granted

- Nor may you enter into a contract, or extend or renew a contract, with a *Covered foreign country, which* means The People's Republic of China

Reporting requirement

In the event the Contractor identifies covered telecommunications equipment or services used as a substantial or essential component of any system, or as critical technology as part of any system, during contract performance, or the Contractor is notified of such by a subcontractor at any tier or by any other source, the Contractor shall report the information to the Contracting Officer, in the case of the Department of Defense, the Contractor shall report to the website at https://dibnet.dod.mil.

Any Questions?

- This briefing is not a substitute for reading the FAR and DFARS in your contract.
- This presentation and other presentations in the DAF CISO Blue Cyber Educational Series and be found on the DAF CISO webpage: https://www.safcn.af.mil/CISO/Small-Business-Cybersecurity-Information/
- Please provide questions, feedback or if you just want to talk about your cyber security /data protection questions to Kelley.Kiernan@us.af.mil
  - Daily Office Hours for answering/researching **your** questions about DAF Small Business cybersecurity and data protection!

Every Tuesday, 1pm Eastern, dial in for the DAF CISO Small Business Cybersecurity Ask-Me-Anything. Register in advance for this Zoom Webinar: https://www.zoomgov.com/webinar/register/WN_6Gz84TQGRvm6YHMSVyE0Qg