AN OFFERING IN THE BLUE CYBER SERIES:

Safeguarding Federal Contract Information

Presented by
Mr. Chris Newborn
Professor, Defense Acquisition University
DAU Cybersecurity Enterprise Team

March 2022

#22 in the Blue Cyber Education Series

Safeguarding Government Sensitive Information per FAR 52.204-21 and DFARS Provision and Clauses (252.204-7012, 7019 & 7020)

Chris Newborn
DAU Cybersecurity Enterprise Team
March 2022

DFARS - Background

2016 - FAR 52.204-21: Basic Safeguarding of Covered Contract Information Systems; requires protection of Federal Contract Information (FCI); 15 basic cyber controls plus flow-down requirements.

2018 - DFARS 252.204-7012: Safeguarding Covered Defense Information and Cyber Incident Reporting; allowed self-attestation to implementation of the 110 security requirements in the NIST SP 800-171 framework; protects Controlled Unclassified Information (CUI) plus flow-down requirements, rapid reporting of cyber incidents (72 hours), submission of malicious software to the DoD, media preservation/protection, cloud service provider must meet FedRAMP moderate baseline; Plan of Action (POAs) allowed for unimplemented controls.

DFARS - Background

30 Nov 2020 – DFARS Interim Rule - Three new DFARS provision /clauses were added via the Interim Rule (DFARS Case 2019-D041).

- **DFARS 252.204-7019:** Requires a self-assessment (Basic) to the 110 security requirements in NIST SP 800-171 using the DoD Assessment Methodology (DoD AM) every 3 years; scores uploaded to the Supplier Performance Risk System (SPRS); and Contracting Officers verify SPRS score before awarding new or extending existing contracts.
- **DFARS 252.204-7020:** Requires contractors to allow the DoD to perform Medium or High assessments. DFARS 252.204-7012 still in effect.
- **DFARS 252.204-7021:** Introduced CMMC; 5-Level maturity model for cybersecurity; 3rd party assessments by C3PAOs every 3 years; rolled-out incrementally through September 30, 2025; added to 100% of DoD contracts by October 1, 2025 (excluded strictly COTS). POAs not allowed – 100% compliance.

Federal Registry Notice dated 17 Nov 2021

- As a result of receiving more than 850 public comments in response to the interim DFARS rule, DoD initiated an internal review March 2021 of CMMC. This review resulted in “CMMC 2.0,” which updates the program structure and the requirements to streamline and improve implementation of the CMMC program.
- Per the Federal Registry Notice dated 17 Nov 2021, the changes reflected in the CMMC 2.0 framework will be implemented through the rulemaking process. DoD will pursue rulemaking in both; (1) Title 32 of the Code of Federal Regulations (CFR), and (2) title 48 CFR, to establish CMMC 2.0 program requirements and implement any needed changes to the CMMC program content in 48 CFR.

What Does This Mean

"... Until the CMMC 2.0 changes become effective through both the title 32 CFR and title 48 CFR rulemaking processes, the Department will suspend the CMMC Piloting efforts, and will not approve inclusion of a CMMC requirement in DoD solicitations. The CMMC 2.0 program requirements will not be mandatory until the title 32 CFR rulemaking is complete, and the CMMC program requirements have been implemented as needed into acquisition regulation through title 48 rulemaking ..."

DFARS - Roles /Responsibilities

- **Requires the program office /requiring activity to:**
  - Mark or otherwise identify in the contract, task order, or delivery order controlled unclassified information provided to the contractor by or on behalf of, DoD in support of the performance of the contract
- **Requires the contractor /subcontractor to:**
  - Provide adequate security to safeguard controlled unclassified information that resides on or is transiting through a contractor's internal information system or network
  - Report cyber incidents that affect a covered contractor information system or the controlled unclassified information residing therein, or that affect the contractor's ability to perform requirements designated as operationally critical support
  - Submit malicious software discovered and isolated in connection with a reported cyber incident to the DoD Cyber Crime Center (DC3)
  - Submit media /information as requested to support damage assessment activities
  - Flow down the clause in subcontracts for operationally critical support, or for which subcontract performance will involve controlled unclassified information

Related Policy - Basic Safeguarding of Covered Contractor Information Systems

FAR 52.204-21, Basic Safeguarding of Covered Contractor Information Systems (CCIS):

- Covered contractor information system means an information system that is owned or operated by a contractor that processes, stores, or transmits FCI
- Supplier Requirements:
  - **Imposes 15 basic cybersecurity controls - CFR 52.204-21(b)**
    - **Limit Access, Authenticate, Sanitize, Monitor, Find/ Fix Flaws, Patch, Detect Malware, Scans, etc.**
  - **Flow down these controls to Subcontracts - CFR 52.204-21 (c)**

48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems

(a) Definitions As Used in this Clause:

- Covered contractor information system (CCIS) means an information system that is owned or operated by a contractor that processes, stores, or transmits Federal Contract Information (FCI).
- FCI means information, not intended for public release, that is provided by or generated for the Government under a contract to develop or deliver a product or service to the Government, but not including information provided by the Government to the public (such as on public Web sites) or simple transactional information, such as necessary to process payments.
- Information means any communication or representation of knowledge such as facts, data, or opinions, in any medium or form, including textual, numerical, graphic, cartographic, narrative, or audiovisual (Committee on National Security Systems Instruction (CNSSI) 4009).
- Information system means a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information (44 U.S.C. 3502).
- Safeguarding means measures or controls that are prescribed to protect information systems.

https://www.law.cornell.edu/cfr/text/48/52.204-21

NARA CUI Category: General Procurement and Acquisition

Category Description: Material and information relating to, or associated with, the acquisition and procurement of goods and services, including but not limited to, cost or pricing data, contract information, indirect costs and direct labor rates.

https://www.archives.gov/cui/registry/category-detail/procurement-acquisition.html

48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems.

(b) 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:

(i) Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

(ii) Limit information system access to the types of transactions and functions that authorized users are permitted to execute.

(iii) Verify and control/limit connections to and use of external information systems.

(iv) Control information posted or processed on publicly accessible information systems.

(v) Identify information system users, processes acting on behalf of users, or devices.

(vi) Authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

(vii) Sanitize or destroy information system media containing Federal Contract Information before disposal or release for reuse.

(viii) Limit physical access to organizational information systems, equipment, and the respective operating environments to authorized individuals.

(ix) Escort visitors and monitor visitor activity; maintain audit logs of physical access; and control and manage physical access devices.

(x) Monitor, control, and protect organizational communications (***i.e.,*** information transmitted or received by organizational information systems) at the external boundaries and key internal boundaries of the information systems.

(xi) Implement subnetworks for publicly accessible system components that are physically or logically separated from internal networks.

(xii) Identify, report, and correct information and information system flaws in a timely manner.

(xiii) Provide protection from malicious code at appropriate locations within organizational information systems.

(xiv) Update malicious code protection mechanisms when new releases are available.

(xv) Perform periodic scans of the information system and real-time scans of files from external sources as files are downloaded, opened, or executed.

https://www.law.cornell.edu/cfr/text/48/52.204-21

48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems.

(b) Safeguarding Requirements and Procedures.

(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.

https://www.law.cornell.edu/cfr/text/48/52.204-21

48 CFR § 52.204-21 - Basic Safeguarding of Covered Contractor Information Systems.

(c) Subcontracts. The Contractor shall include the substance of this clause, including this paragraph, in subcontracts under this contract (including subcontracts for the acquisition of commercial products or commercial services, 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.

https://www.law.cornell.edu/cfr/text/48/52.204-21

DFARS Implementation: FAR 21 Versus DFARS 7012

	FAR 21	DFARS 7012
Information Type:	FCI	CUI
Reference:	NIST SP 800-53	NIST SP 800-171
Compliancy:	15 Security Controls	110 Security Requirements
Deliverable:	N A	SSP & POA plus Artifacts
Validation:	N/A	3-Levels of Assessments (basic, medium, high) using NIST SP 800-171 v1.2, DoD AM
Governance:	N/A	7019, 7020

DFARS - Summary

- Contracting Officers are required to following the Interim Rule; Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041), that amends DFARS subpart 204.73, Safeguarding Covered Defense Information and Cyber Incident Reporting, and implements the NIST SP 800-171 DoD AM.
- The coverage in the subpart directs Contracting Officers to:
  - **Verify in Supplier Performance Risk System (SPRS)** that an offeror has a current NIST SP 800-171 DoD Assessment on record, prior to contract award or extending an existing contract, if the offeror is required to implement NIST SP 800-171 pursuant to DFARS clause 252.204-7012.
  - **Include DFARS provision 252.204-7019, Notice of NIST SP 800-171 DoD Assessment Requirements, DFARS clause 252.204-7020, and the NIST SP 800-171 DoD AM** in solicitations and contracts including solicitations using FAR part 12 procedures for the acquisition of commercial items, except for solicitations solely for the acquisition of COTS items.

For additional questions, please contact
Chris Newborn at
chris.newborn@dau.edu or
619-370-3076

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**, 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