How to Comply with DFAR 252-204-7012, -7019 & -7020 & NIST SP 800-171 Rev. 2

CROSS TIMBERS

Procurement Technical Assistance Center

Webinar Guidelines

All attendees are muted.

Use Chat box for questions.

Presentation available in Hand Out box or at www.uta.edu/crosstimbers/webinars.

Purpose

The purpose of this webinar is to create awareness of the current cybersecurity regulations, the DFAR 252.204-7012, -7019, -7020 and to help you understand what is expected as it relates to the new CMMC 2.0 cybersecurity requirements.

It is in the interest of National Security that ALL of the companies doing business with DoD will have to comply immediately with DFARS 252.204-7012 ,-7019, -7020 and have a Cybersecurity Maturation Model Certification (CMMC 2.0) level 1-3.

Agenda

1. DFAR 252.204-7012 ,-7019, -7020 Compliance Steps

2. Cybersecurity Maturation Model Certification (CMMC 2.0)

3. NIST SP 800-171: Control Families

CROSS TIMBERS

It’s the Law

DFAR 252.204-7012, -7019, -7020: By signing a DoD contract, the contractor agrees to comply with the terms of the contract and all requirements of the DFARS Clause 252.204-7012, -7019, -7020. The deadline for compliance was Dec 31, 2017. The deadline for compliance with -7019 & 7020 was November 30, 2020.

The regulations apply to ANY current DoD contractor with the DFARS 252.204-7012, -7019, -7020 clause within the contract.

False Claim Act: False Claims Act (FCA), 31 U.S.C. §§ 3729 - 3733, is a federal statute originally enacted in 1863 in response to defense contractor fraud during the American Civil War.

Cybersecurity Maturation Model Certification (CMMC 2.0): The intent is to incorporate CMMC 2.0 into Defense Federal Acquisition Regulation Supplement (DFARS) and use it as a requirement for contract award. Contractors are subject to third Party Assessment Organizations (C3PAOs) certification auditors.

It’s the Law

Current contracts including the DFARS 252.204-7012 will likely not be amended until the re-compete. Expect requirements to be more aggressively enforced through the Contracting Officer, Service investigative agencies, such as NCIS, DCMA, and referred to the Federal False Claims Act.

Enforcement of the current requirements is aggressively expanding through Defense Contact Management Agency (DCMA) audit, Federal False Claims Act referrals, and the individual military services authorization for criminal enforcement.

The regulations apply to ANY current DoD contractor with the DFARS 252.204-7012, -7019, -7020 clause within their contract. Those corporate (non-federal contractor information systems) that create, receive, share, store, or transmit CUI data... **globally**.

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting. | Acquisition.GOV

Types of Unclassified Information

Federal Contract Information (FCI): FCI is information provided by or generated for the Government under contract not intended for public release.

[OUSD A&S - Cybersecurity Maturity Model Certification (CMMC) (osd.mil)]

Controlled Unclassified Information: CUI is information the Government creates or possesses, or that an entity creates or possesses for or on behalf of the Government, that a law, regulation, or Government-wide policy requires or permits an agency to handle using safeguarding or dissemination controls.

CUI is technical in nature and could include drawings, specifications and other pertinent information that requires protection from unauthorized sources.

https://www.archives.gov/cui   https://youtu.be/egbAZ1f5r8g

1. DFAR 252.204-7012 , -7019, -7020 Compliance Steps

https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012

1.1 NIST SP 800-171 Self Assessment

1.2 Plan of Action and Milestones (POAMS)

1.3 Risk Assessment

1.4 System Security Plan

1.5 Incident Response Plan and Reporting

1.6 Subcontractor Flow Down Requirements

NOTE: SAVE DOCUMENTS FOR CMMC AUDITORS

1. DFAR 252.204-7012 , -7019, -7020 Compliance

1.1 NIST SP 800-171 Self-Assessment

Complete questionnaire. Ask about Cross Timber’s Self Assessment Tool.

Review total scores to know and understand the weaknesses.

Develop plan and budget to fix the weaknesses. Hire professional company to help if needed.

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements

https://doi.org/10.6028/NIST.SP.800-171A

Save Self Assessment results for CMMC auditors

1. DFAR 252.204-7012, -7019, -7020 Compliance Steps

1.2 Plan of Action and Milestones (POAMS) Template

Weaknesses

Responsible Office/ Organization

Resource Estimate (funded/ unfunded/ reallocation)

Scheduled Completion Date

Milestones with Interim Completion Dates

Changes to Milestones

How was the weakness identified?

Status *(Ongoing or Complete)*

CUI-Plan-of-Action-Template-final.docx (live.com)

Save POAM results for CMMC Auditor.

CROSS TIMBERS

1. DFAR 252.204-7012 , -7019, -7020 Compliance Steps

1.3 Risk Assessment

- Test and validate current information security measures
- Identify vulnerabilities to data loss
- Analyze safeguards to mitigate threats
- Build remediation plan
- Establish risk management plan

Save results for CMMC auditors

1. DFAR 252.204-7012 , -7019, -7020 Compliance Steps

1.4 System Security Plan (SSP) Template

3.1 Access Control: 22 sections	3.8 Media Protection: 9 sections
3.2 Awareness and Training: 3 sections	3.9 Personnel Security: 2 sections
3.3 Audit and Accountability: 9 sections	3.10 Physical Protection: 6 sections
3.4 Configuration Management: 9 sections	3.11 Risk Assessment: 3 sections
3.5 Identification and Authentication: 11 sections	3.12 Security Assessment: 4 sections
3.6 Incident Response: 3 sections	3.13 System and Communications Protection: 16 sections
3.7 Maintenance: 6 sections	3.14 System and Information Integrity: 7 sections

https://csrc.nist.gov/publications/detail/sp/800-171/rev-1/final

Save SSP for CMMC Auditor

1. DFAR 252.204-7012 , -7019, -7020 Compliance Steps

1.5 Incident Response Plan and Reporting

A “Cyber incident” is an action(s) taken through the use of computer networks that result in a compromise or an actual or potentially adverse effect on an information system and/or the information residing therein.

“Compromise” means disclosure of information to unauthorized persons, or a violation of the security policy of a system, in which unauthorized intentional or unintentional disclosure, modification, destruction, or loss of an object, or the copying of information to unauthorized media may have occurred.

Submit Incident to DoD DIB portal:

https://dibnet.dod.mil/portal/intranet/

1. DFAR 252.204-7012 , -7019, -7020 Compliance Steps

1.5 Incident Response Plan and Reporting

The incident response plan should include the following elements:

Mission.

Strategies and goals.

Senior management approval.

Organizational approach to incident response.

How the incident response team will communicate with the rest of the organization and with other organizations.

Metrics for measuring the incident response capability and its effectiveness.

Roadmap for maturing the incident response capability.

How the program fits into the overall organization.

https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Save IRPR for CMMC Auditor

1. DFAR 252.204-7012 , -7019, -7020 Compliance Steps

1.6 Subcontractor Flow Down Requirements

When should DFARS Clause 252.204-7012, -7019, -7020 flow down to subcontractors?

- The clause is required to flow down to subcontractors only when performance will involve operationally critical support or CUI.

- The contractor shall determine if the information required for subcontractor performance is or retains its' identity as CUI and requires safeguarding.

- Flow down is a requirement of the terms of the contract with the Government, which must be enforced by the prime contractor as a result of compliance with these terms.

–If a subcontractor does not agree to comply with the terms of DFARS Clause 252.204–7012, then CUI shall not be shared with the subcontractor or otherwise reside on its' information system.

https://www.navsea.navy.mil/Portals/103/Documents/Small_Business_Forum/SBID-CybersecurityChallenges.pdf

Selection Criteria for Third Party Providers (TPP's)

Regan Edens reganedens@dtcglobal.us CMMC AB Director

Third Party Providers (TPP'S) MUST meet CURRENT DFARS 252.204-7012 requirements if they receive, store, and transmit CUI data under DFARS 252.204-7012,-7019, -7020.

Those TPP's that only provide services such as "maintenance", "consulting services", etc.. and only require "access", but do not require receiving, transmitting, or storing FCI/CUI from an OSC's environment, could then be included as any other "1099 subcontractor" with remote or direct system access.

TPP's Should have a deep knowledge of DFARS 7008,7009, 7012, NIST 800-171r2, DoDi 5200,48, 32CFR, part 2002, FAR 52.204-21, CUI Registry; CUI determination and marking; DFARS 7012 2(ii)(D) compliant cloud solutions architecture, and CUI Supply Chain Risk Management.

Selection Criteria for Third Party Providers (TPP's)

Regan Edens reganedens@dtcglobal.us CMMC AB Director

Choose Consultants or Firms that engage you with best practices AND a variety of appropriate "turn-key solutions" often through trusted partners to address gaps (big and small). "Frankensteining" by piecing together disparate solutions is often FAR MORE EXPENSIVE and TIME INTENSIVE than needed. The importance of trusted relationships is worth emphasizing.

If you do not trust them to recommend MORE THAN THEIR SOLUTIONS, do not use them. Their strategy should best optimize WHAT YOU HAVE and ONLY THEN RECOMMEND WHAT YOU NEED. Compliance is THE objective, not getting you to buy "more stuff" or worse "more of their stuff".

Recap

Types of Unclassified Information

It’s The Law

1. DFAR 252.204-7012, -7019, -7020 Compliance Steps:

1.1 NIST SP 800-171 Self-Assessment

1.2 POAMS

1.3 Risk Assessment

1.4 System Security Plan (SSP)

1.5 Incident Response Plan and Reporting

1.6 Sub Contractor Flow Down Requirements

Selection Criteria for help from IT companies

Save Compliance Steps documents for CMMC Auditor

2. CMMC 2.0 - Cybersecurity Maturation Model Certification

The CMMC encompass multiple maturity levels that ranges from “Basic Cybersecurity Hygiene” to “Expert”. Contracting Officers will mark solicitation and award contracts with each level. Contractors will only be able to bid on their level issued by CMMC auditors. https://www.acq.osd.mil/cmmc/faq.html

- **Level 1 – Basic Cyber Hygiene:** Includes basic cybersecurity appropriate for small companies utilizing a subset of universally accepted common practices. This level has 35 security controls that must be successfully implemented.

- **Level 2 – Advanced Cyber Hygiene:** Includes universally accepted cybersecurity best practices, coverage of all NIST SP 800-171 Rev. 1 controls and additional practices beyond the scope of current CUI protection. Includes advanced and sophisticated cybersecurity practices. This level has 301 controls beyond the first Level.

- **Level 3 – Expert:** Includes highly advanced cybersecurity practices**.** This level requires an additional 35 controls.

2. CMMC 2.0 - Cybersecurity Maturation Model Certification

You Should Know:

- The CMMC 2.0 Rule committee expects to finalize the rules March 2023
- Requirements included in contracts expected to start March-June 2023
- Achieving CMMC 2.0 regulations generally takes about 12 months

(suggest starting immediately)

3. NIST SP 800-171: Control Families

3.1 Access Control: 22 sections	3.8 Media Protection: 9 sections
3.2 Awareness and Training: 3 sections	3.9 Personnel Security: 2 sections
3.3 Audit and Accountability: 9 sections	3.10 Physical Protection: 6 sections
3.4 Configuration Management: 9 sections	3.11 Risk Assessment: 3 sections
3.5 Identification and Authentication: 11 sections	3.12 Security Assessment: 4 sections
3.6 Incident Response: 3 sections	3.13 System and Communications Protection: 16 sections
3.7 Maintenance: 6 sections	3.14 System and Information Integrity: 7 sections

NIST MEP Cybersecurity Self-Assessment Handbook For Assessing NIST SP 800-171 Security Requirements in Response to DFARS Cybersecurity Requirements.

https://doi.org/10.6028/NIST.SP.800-171A

3. NIST SP 800-171: Control Families
Access Control (3.1)

Access is the ability to make use of any system resource. Access control is the process of granting or denying requests to use information, use information processing services, and enter company facilities.

This family contains 22 sections and 2+ questions. Selected sample questions include:

Does the company use passwords? 3.1.1

Does the company have an authentication mechanism? 3.1.1

Do applications used to remotely access the system use approved encryption methods? 3.1.13

ALL questions will need to be addressed and written into a DETAILED SSP.

CROSS TIMBERS

3. NIST SP 800-171: Control Families
Awareness & Training (3.2)

Users of a system can be viewed as the weakest link in securing systems. Often users are not aware of how their actions may impact the security of a system. Making system users aware of their security responsibilities and teaching them correct practices helps change their behavior.

This family contains 3 sections and 12+ questions. Selected sample questions include:

Is basic security awareness training provided to all system users before authorizing access to the system when required by system changes and at least annually thereafter? 3.2.1

Do all users, managers, and system administrators receive initial and annual training commensurate with their roles and responsibilities? 3.2.1

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families
Audit and Accountability (3.3)

An audit is an independent review and examination of records and activities to assess the adequacy of system requirements and ensure compliance with established policies and operational procedures. An audit trail is a record of individuals who have accessed a system as well as what operations the user has performed during a given period.

This family contains 9 sections and 25+ questions. Selected sample questions include:

Can the company uniquely trace and hold accountable users responsible for unauthorized actions? 3.3.2

Does the company review and update audited events annually or in the event of substantial system changes or as needed. 3.3.3

Does the system maintain audit records on host servers until log delivery to central repositories can be re-established? 3.3.4

ALL questions will need to be addressed and written into a DETAILED SSP.

CROSS TIMBERS

3. NIST SP 800-171: Control Families
Configuration Management (3.4)

Configuration management is a collection of activities focused on establishing and maintaining the integrity of information technology products and systems through the control of processes for initializing, changing, and monitoring the configurations of those products and systems throughout the System Development Life Cycle (SDLC).

This family contains 9 sections and 34+ questions. Selected sample questions include:

Are baseline configurations developed, documented, and maintained for each information system type? 3.4.1

Are changes to the system authorized by company management and documented? 3.4.4

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families
Identification & Authentication (3.5)

For most systems, identification and authentication is often the first line of defense. Identification is the means of verifying the identity of a user, process, or device, typically as a prerequisite for granting access to resources in a system.

This family contains 11 sections and 40+ questions. Selected sample questions include:

Do all passwords follow best practice of at least 12 characters, and require a mix of upper and lower case letters, numbers, and special characters? 3.5.2

Is multifactor authentication used for local access to privileged accounts? 3.5.3
Are accounts uniquely assigned to employees, contractors, and subcontractors? 3.5.5

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families

Incident Response (3.6)

Systems are subject to a wide range of threat events, from corrupted data files to viruses to natural disasters. Vulnerability to some threat events can be lessened by having standard operating procedures that can be followed in the event of an incident.

This family contains 3 sections and 19+ questions. Selected sample questions include:

Is there a company incident response policy which specifically outlines requirements for handling of incidents involving CUI? 3.6.2

Is cybersecurity incident information promptly reported to company management and authorities? 3.6.2

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families
Maintenance (3.7)

Controlled maintenance of a system deals with maintenance that is scheduled and performed in accordance with the manufacturer’s specifications.

This family contains 6 sections and 15+ questions. Selected Sample questions include:

Does the company perform maintenance on the information system? 3.7.1

Is there a company media sanitization policy? 3.7.3

Are all activities of maintenance personnel (who do not normally have access to a system) monitored? 3.7.6

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families

Media Protection (3.8)

Media protections can restrict access and make media available to authorized personnel only, apply security labels to sensitive information, and provide instructions on how to remove information from media so that the information cannot be retrieved or reconstructed.

This family contains 9 sections and 35+ questions. Selected sample questions include:

Do only approved individuals have access to media from CUI systems? 3.8.1

Are all CUI data on media encrypted or physically locked prior to transport outside of the company's secure locations? 3.8.3

Are all CUI systems identified with an asset control identifier, for example, does each company laptop have an asset id tag with a unique number? 3.8.4

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families
Personnel Security (3.9)

Almost no system can be secured without properly addressing these aspects of personnel security. Personnel security seeks to minimize the risk that staff (permanent, temporary, or contractor) pose to company assets through the malicious use or exploitation of their legitimate access to the company's resources.

This family contains 2 sections and 7+ questions. Selected samples questions include:

Are individuals requiring access screened before access is granted? 3.9.1

Are electronic and physical access permissions reviewed when employees are reassigned or transferred? 3.9.2

Does the company disable information system access prior to employee termination or transfer? 3.9.2

ALL questions will need to be addressed and written into a DETAILED SSP.

CROSS TIMBERS

3. NIST SP 800-171: Control Families
Physical Protection (3.10)

The term physical and environmental security refers to measures taken to protect systems, buildings, and related supporting infrastructure against threats associated with their physical environment.

This family contains 6 sections and 15+ questions. Selected sample questions contain:

Are all visitors to sensitive areas always escorted by an authorized employee? 3.10.3

Are keys, combinations, and other physical access devices secured? 3.10.5

Are logs of physical access to sensitive areas maintained per retention policies? (This includes authorized access as well as visitor access.) 3.10.4

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families
Risk Assessment (3.11)

Risk assessments identify and prioritize risks to company operations, assets, employees, and other organizations that may result from the operation of a system.

This family contains 3 sections and 14+ questions. Selected sample questions include:

Does the company have a risk management policy? 3.11.1

Is vulnerability scanning performed? 3.11.2

Are reports regarding the scans made available to system owners and company management in a timely manner? 3.11.2

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families
Security Assessment (3.12)

A security requirement assessment is the testing and/or evaluation of the management, operational, and technical security requirements on a system to determine the extent to which the requirements are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.

This family contains 4 sections and 23+ questions. Selected sample questions include:

Has a periodic (e.g., annual) security assessment been conducted to ensure that security controls are implemented correctly and meet the security requirements? 3.12.1

Is the assessment conducted by an independent security auditor/consultant? 3.12.1

ALL questions will need to be addressed and written into a DETAILED SSP.

3. NIST SP 800-171: Control Families

System and Communications Protection (3.13)

System and communications protection requirements provide an array of safeguards for the system. Some of the requirements in this family address the confidentiality of information at rest and in transit.

This family contains 16 sections and 35+questions. Selected sample questions include:
Does the system monitor and manage communications at the system boundary and at key internal boundaries within the system? 3.13.1

Are processes and automated mechanisms used to provide encryption of CUI during transmission? Are processes and automated mechanisms used to provide encryption of CUI during transmission? 3.13.8

ALL questions will need to be addressed **and written into a DETAILED SSP.**

3. NIST SP 800-171: Control Families
System and Information Integrity (3.14)

Integrity is defined as guarding against improper information modification or destruction and includes ensuring information non-repudiation and authenticity.

This family contains 7 sections and 22+ questions. Selected sample questions include:

Does the system automatically update malicious code protection mechanisms? 3.14.2

Does the company receive security alerts, advisories, and directives from reputable external organizations? 3.14.3

Does the company perform real-time scans of files from external sources as the files are downloaded, opened, or executed? 3.14.5

ALL questions will need to be addressed and written into a DETAILED SSP.

Recap

DFAR 252.204-7012 Compliance Steps

- **1.1 NIST SP 800-171 Self Assessment**
- **1.2 Plan of Action and Milestones (POAMS)**
- **1.3 Risk Assessment**
- **1.4 System Security Plan (SSP)**
- **1.5 Incident Response Plan and Reporting**
- **1.6 Sub Contractor Flow Down Requirements**

Cybersecurity Maturation Model Certification (CMMC 2.0)

NIST SP 800-171: Control Families

Key Websites

252.204-7012 Safeguarding Covered Defense Information and Cyber Incident Reporting: https://www.acq.osd.mil/dpap/dars/dfars/html/current/252204.htm#252.204-7012:

National Archives CUI Registry: https://www.archives.gov/cui:

Cybersecurity ChallengesUnclassified1NAVSEA Small Business Industry DayAugust 8, 2017 Protecting DoD’s Unclassified Information: https://www.navsea.navy.mil/Portals/103/Documents/Small_Business_Forum/SBID-CybersecurityChallenges.pdf

NIST 800-171 Hand Book: https://doi.org/10.6028/NIST.SP.800-171A

SP 800-171 Rev. 2 Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. See templates for SSP, POEMS and the SP 800-171 Rev. 2 (DOI) https://csrc.nist.gov/publications/detail/sp/800-171/rev-2/final

Computer Security Incident Handling Guide: https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-61r2.pdf

Key Websites

DOD INSTRUCTION 5200.48 CONTROLLED UNCLASSIFIED INFORMATION (CUI): https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF
32 CFR Part 2002 - CONTROLLED UNCLASSIFIED INFORMATION (CUI): https://www.law.cornell.edu/cfr/text/32/part-2002
CYBERSECURITY MATURITY MODEL CERTIFICATION (CMMC) https://www.acq.osd.mil/cmmc/
Determining Authorized Holders of CUI: https://youtu.be/egbAZ1f5r8g
DFARS & NIST 800-171 Compliance 101: https://youtu.be/2g4sm7rVqjM

CROSS TIMBERS

Key Websites

TMAC/MEP: https://tmac.org/additional-services/
DIB SCC CyberAssist: https://ndisac.org/dibscc/cyberassist/
CMMC Accreditation Body: https://www.cmmcab.org/
Info Defense: https://www.infodefense.com/
DTC Global: https://dtcglobal.us/contact-us
CUI Program Blog: https://isoo.blogs.archives.gov/

Contact

Cross Timbers Procurement Technical Assistance Center
University of Texas at Arlington
202 East Border St, #323
Arlington Texas 76010
www.uta.edu/crosstimbers

Shelia Birdow shelia.birdow@uta 817-272-2081

Gregory James gjames@uta.edu 817-272-5978

The University of Texas at Arlington/Cross Timbers Procurement Technical Assistance Center is Funded in part through a cooperative agreement with the Department of Defense.

- https://www.dla.mil/SmallBusiness/PTAPFeedback/

CROSS TIMBERS

Additional Assistance

Darold Tippey
Darold.Tippey@tmac.org
(817) 789-9249 | TMACdfw.org
The University of Texas at Arlington

Work Smart. Grow Smart.™

PART OF THE MEP National Network™