

# CMMC and Cybersecurity for Government Contractors

The Current Landscape, What's Coming, and  
What You Should Be Doing To Prepare

---

PRESENTED BY:

**SheppardMullin**

**CHESS**  
CONSULTING LLC

**xerox** 

OCTOBER 14, 2021

# Nice To Meet You!

---



**Townsend Bourne**

Partner, Sheppard Mullin



**Nikki Snyder**

Associate, Sheppard Mullin



**Mike Tomaselli**

Senior Manager, Chess  
Consulting LLC



**Sharon Steele**

Senior Counsel, Xerox

# Today's Agenda

---

- 01 Current Regulatory Landscape
- 02 The Cybersecurity Maturity Model Certification Program
- 03 Cybersecurity in the Cloud
- 04 Biden Cybersecurity Executive Order
- 05 Proposed/Pending Legislation





# Current Regulatory Landscape

---

# Current Regulatory Landscape

---

## Basic Safeguarding of Covered Contractor Information Systems (FAR 52.204-21)

- Protects “**Federal Contract Information**” (FCI)
- Contractor information systems that process, store, or transmit FCI are subject to **15 basic security requirements** from NIST SP 800-171
- No incident reporting requirements
- Flow-down in all subcontracts (except solely COTS) involving FCI

## Safeguarding Covered Defense Information (DoD; DFARS 252.204-7012)

- DoD contractors must provide “adequate security” for “**covered defense information**” (CDI) (includes Controlled Unclassified Info (CUI))
- “**Adequate security**” (usually) means compliance with the NIST SP 800-171 standards
- Incident Reporting: “Rapidly report” (within 72 hours of discovery)
- Cyber incident requirements
- Flow-down in all subcontracts involving CDI or “operationally critical support”

# Current Regulatory Landscape

---

## Notice of NIST SP 800-171 DoD Assessment Requirements (DoD; DFARS 252.204-7019)

- If required to implement NIST 800-171, Offeror must have current assessment to be considered for award
- Current assessment (not more than 3 years old) must be posted in Supplier Performance Risk System (SPRS)

## NIST SP 800-171 DoD Assessment Requirements (DoD; DFARS 252.204-7020)

- Requires assessment for compliance with NIST SP 800-171 for covered contractor information systems
  - Contractor to conduct Basic assessment and self-report compliance score in SPRS
  - Medium or High assessment may be conducted by the government at its discretion
- Flow-down in all subcontracts (except solely COTS)
  - Contractor must ensure subcontractors have completed assessment



# Controlled Unclassified Information

---



- **NARA Federal Program (32 CFR 2002)**
  - Executive Branch CUI policy for designating, handling, and decontrolling information that qualifies as CUI
- **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”
- **Open FAR Case 2017-016 – Controlled Unclassified Information**
  - Will implement NARA CUI program and address breaches of PII
  - Requirements for designating, safeguarding, disseminating, marking, decontrolling, and disposing of CUI

# Discussion Topics

---

How can I distinguish between Federal Contract Information (FCI) and CUI?

#1

How do I know if I need to submit a NIST 800-171 Assessment score in SPRS?

#2

My Company sends/would like to send CUI via email. Is this OK?

#3

Do I need a CUI Policy?

#4





# The Cybersecurity Maturity Model Certification (“CMMC”) Program

---

# CMMC Overview

---



- Unified standards for DoD acquisitions to protect sensitive data, including Controlled Unclassified Information (CUI)
- Some early pilot programs, widespread by 2026
- 5 levels based on review by 3<sup>rd</sup> party assessor (C3PAO)
- CMMC Accreditation Body (AB) to manage ecosystem
- Some level to be required in all DoD contracts
  - Prime & subcontractors
  - COTS exception
- Reciprocity? – ex. ISO, FedRAMP
- DoD *only* (for now)
- Currently under government review and third-party certifications delayed; possible changes to framework

# CMMC: A Closer Look At Each Level

---

CMMC Level	Primary Focus Area	Total Practices	Underlying Requirements
<b>Level 1:</b> Basic Cyber Hygiene	Basic safeguarding of Federal Contract Information (FCI).	17	17 practices that comply with FAR 48 CFR 52.204-21.
<b>Level 2:</b> Intermediate Cyber Hygiene	Transition step to protecting Controlled Unclassified Information (CUI).	72	Level 1, plus 48 selected practices from NIST SP 800-171 r1, and an additional 7 practices.
<b>Level 3:</b> Good Cyber Hygiene	Protecting CUI.	130	Level 1 and Level 2, plus 58 additional practices (all NIST SP 800-171 r1, and others).
<b>Level 4:</b> Proactive	Protecting CUI and reducing the risk of Advanced Persistent Threats (APTs).	156	Levels 1-3, plus an additional 26 (from Draft NIST SP 800-171B and others).
<b>Level 5:</b> Advanced/Progressive	Protecting CUI and reducing the risk of APTs.	171	Levels 1-4, plus an additional 15 practices (from Draft NIST SP 800-171B and others).



# CMMC: Timing for Organizations Seeking Certification

---

- CMMC-AB will select and train C3PAOs
- Certification will be valid for 3 years
- Begin planning certification well in advance (timing depends on maturity)



# CMMC: Assistance for Organizations Seeking Certification

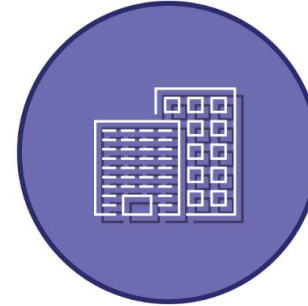
---



Certified Third Party  
Assessor Organization  
("C3PAO")



Registered Provider  
Organization  
("RPO")



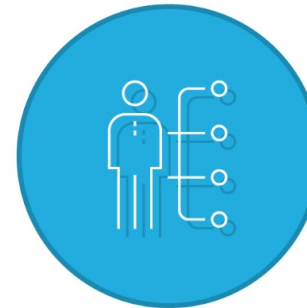
Licensed Training  
Provider  
("LTP")



Licensed Partner  
Publisher  
("LPP")



Certified Assessor  
("CA")



Registered Practitioner  
("RP")

# CMMC: Anticipated # of Contractors with Requirement

---

Total Number of <u>Contracts and Subcontracts</u> with CMMC Requirement				
Year 1	Year 2	Year 3	Year 4	Year 5
1,500	7,500	25,000	47,905	47,905

Total Number <u>Contractors and Subcontractors</u> with CMMC Requirement				
Level 1	Level 2	Level 3	Level 4	Level 5
28,709	4,785	14,355	28	28

All new DOD contracts to contain the CMMC requirement starting in FY26



# CMMC Regulatory Update – Interim Rule



- DFARS 252.204-7021 effective November 2020, BUT
  - CMMC planned to be **rolled out over the next 5 years**, with clause to be included in all solicitations and contracts by October 1, 2025
  - Prior to October 1, 2025, use of the clause **must be approved** by OUSD (A&S)
- Solicitations and contracts will specify required CMMC level (Levels 1-5)
  - Contractor must have and maintain CMMC certification for duration of contract (**renew every 3 years**)
- Flow-Down in all subcontracts (except solely COTS)
  - Contractor must ensure subcontractors have current CMMC certification at appropriate level
- Final Rule expected by the end of the year
- Interim Rule also included NIST SP 800-171 Assessment requirements (discussed above)

# CMMC Delays

---

**“Get on with it, don’t let the perfect be the enemy of the good.”**

– Ellen Lord, former Undersecretary for Defense for Acquisition & Sustainment, on CMMC implementation

# CMMC Discussion Topics

---

How long will it really take for my company to get CMMC certification? Level 3? Level 1?

#1

My company does not have contracts with DoD. Do I need to worry about this?

#2

Will a CMMC certification apply to my entire organization?

#3

How can I determine how much a CMMC assessment will cost my organization?

#4



# Cybersecurity in the Cloud

---

# FedRAMP

---

- Created out of the Federal Cloud Computing Initiative to remove barriers to adoption of cloud
- Stakeholders:
  - **Federal agencies** – conduct risk assessments, integrate FedRAMP requirements into Agency specific policies/procedures, deposit authorization documents in FedRAMP secure repository
  - **Cloud Service Providers** – submit documentation and testing in support of their FedRAMP application for offering(s)
  - **Third party assessment organizations (3PAOs)** – provide assessments, maintain independence as part of quality assurance process
- Four Security Baselines: High (400+ controls)
  - Medium (300+ controls)
  - Low (100+ controls)
  - Tailored for Low Impact SaaS (30+ controls)



# DoD and the Cloud

## Representation of Use of Cloud Computing (DoD; DFARS 252.239-7009)

- Offerors must represent whether they anticipate using cloud computing services “in the performance of any contract or subcontract” resulting from the solicitation

## Cloud Computing Services (DoD; DFARS 252.239-7010)

- Applies to DoD cloud service providers that process data ***on behalf of DoD***
- Requires compliance with DoD Cloud Computing Security Requirements Guide
- Contains requirements for cyber incident reporting, malicious software, data preservation and access, and cyber incident damage assessment
- Contractor must maintain all Government data within the US, unless written authorization to use another location
- Flow-down in all subcontracts that involve or may involve cloud services



# DoD and the Cloud

---

- Contractor use of external cloud service provider (see DFARS 252.204-7012, *Safeguarding Covered Defense Information*)
  - (b)(2)(ii)(D) – where contractor uses external Cloud Service Provider (CSP) to store, process, or transmit CDI
  - Contractor must require and ensure its CSP:
    - Is either approved by the FedRAMP program at the “moderate” baseline, or possesses equivalent security requirements
    - Complies with requirements regarding cyber incident reporting, malicious software, data preservation and access, and cyber incident damage assessment
  - This clause will normally not ‘flow down’ to the CSP; it is up to the contractor to ensure compliance with requirements
- Note (b)(1)(i) refers to DFARS 252.239-7010 for requirements for cloud computing services

# Cybersecurity in the Cloud Discussion Topics

---

What are some of the major differences in requirements when providing cloud services to DoD v. civilian agencies?

#1

My company uses cloud services in performance of government contracts. What are the security requirements for my cloud vendors?

#2

My company is a cloud provider to the government. What are the best resources for me under DoD contracts? Civilian agency contracts?

#3



# Biden Cybersecurity Executive Order


---

# Biden Executive Order: Improving Cybersecurity

(May 12, 2021)

---

- Sharing Threat Information (Sec. 2)
- Modernizing Federal Government Cybersecurity (Sec. 3)
- Enhancing Software Supply Chain Security (Sec. 4)
- Cyber Safety Review Board (Sec. 5)
- Government Playbook to Respond to Cyber Vulnerabilities and Threats (Sec. 6)
- Steps for the Government to Maximize Early Detection of Vulnerabilities & Incidents (Sec. 7)
- Government improvement of its Cyber Investigation and Remediation Capabilities (Sec. 8)
- Updates to Requirements for the National Security Systems (Sec. 9)



Most direct impact  
for Federal  
contractors



# Biden Executive Order: Improving Cybersecurity

(May 12, 2021)

---

- **Sharing Threat Information** – recognizes **IT and OT service providers, including cloud service providers**, have unique access and insight into cyber threat and incident information
  - The government will focus on removing contractual barriers to IT and OT service providers sharing threat information
- **New FAR Clause** –
  - Contract requirements and language for contracting with IT and OT service providers, including descriptions of contractors to be covered by the proposed contract language (Per EO, by mid-October 2021)

# Biden Executive Order: Improving Cybersecurity

(May 12, 2021)

---



**Sharing Threat Information** – It is policy that **information and communications technology (“ICT”) service providers must promptly report cyber incidents**

**New FAR Clause** - Contract language that relates to reporting of cyber incidents by ICT service providers (Per EO, by late September 2021)

# Biden Executive Order: Improving Cybersecurity

(May 12, 2021)

---

**Sharing Threat Information** – Focus on streamlining/standardizing cybersecurity contractual requirements across agencies

**New FAR Clause** - Standardized contract language for appropriate cybersecurity requirements, which include the scope of covered contractors and associated service providers (Per EO, by mid-September 2021)





# Biden Executive Order: Improving Cybersecurity

(May 12, 2021)

---

## Open FAR Cases: Sharing Threat Information

- **2021-019 – Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems**

- Standardizes common cybersecurity contractual requirements across Federal agencies for unclassified Federal information systems

- **2021-017 – Cyber Threat and Incident Reporting and Information Sharing**

- Consolidates IT/OT and ICT service provider reporting provisions
- Increases the sharing of information about cyber threats and incident information between the Government and certain providers
- Requires certain contractors to report cyber incidents to the Federal Government to facilitate effective cyber incident response and remediation



# Biden Executive Order: Improving Cybersecurity

(May 12, 2021)

---



- **Modernizing Federal Government Cybersecurity** – requires the government to modernize its approach to cybersecurity, to include prioritizing cloud solutions and Zero Trust Architecture
  - The government will begin to modernize FedRAMP
- Establishes a government **Cyber Safety Review Board** to review and assess significant cyber incidents

# Biden Executive Order: Improving Cybersecurity

(May 12, 2021)

---

## Enhancing Software Supply Chain Security – focus on “critical software”

Preliminary and updated guidance to be published relating to enhancing software supply chain security.

Identify existing and develop new standards, tools, and best practices for complying with practices that enhance the security of the software supply chain.

The government will identify IoT cybersecurity criteria for a consumer labeling program.

The government will identify secure software development practices or criteria for a consumer software labeling program.

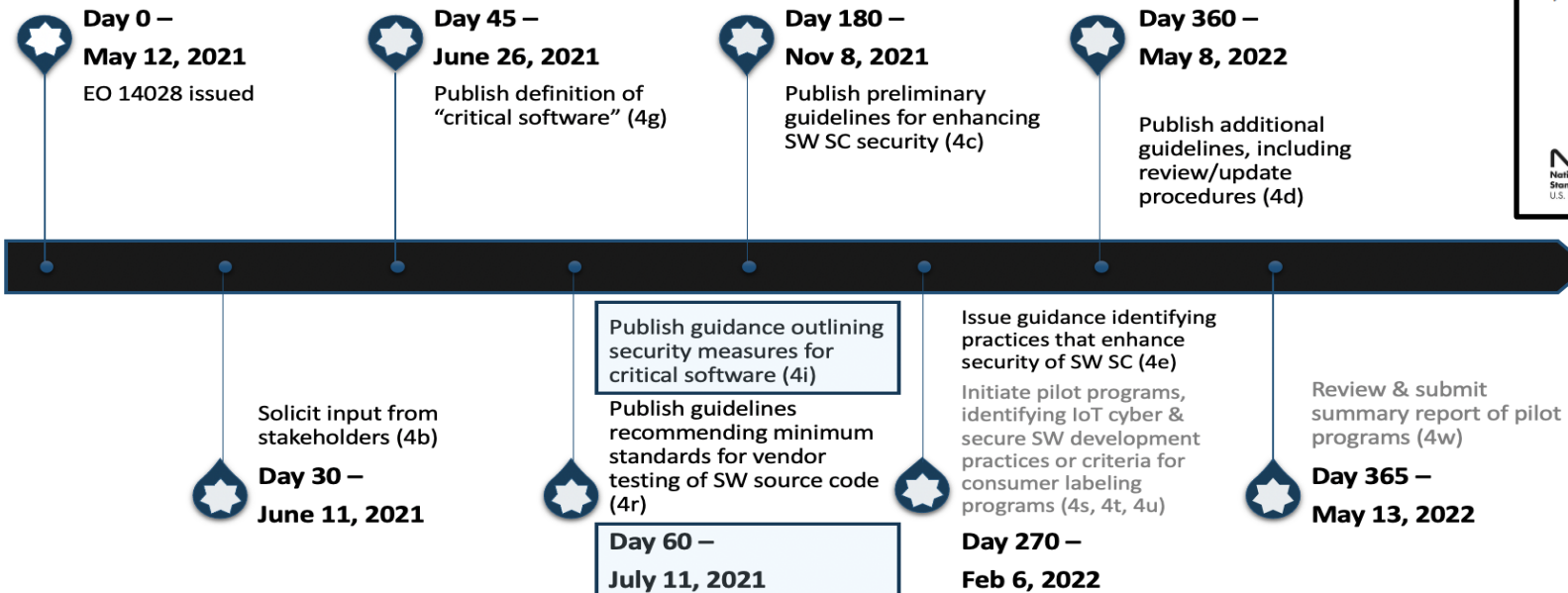
# Critical Software

EO-critical software is defined as any software that has, or has [direct software dependencies](#)

upon, one or more components with at least one of these attributes:

- is designed to run with elevated privilege or manage privileges;
- has direct or privileged access to networking or computing resources;
- is designed to control access to data or operational technology;
- performs a function [critical to trust](#); or,
- operates outside of normal trust boundaries with privileged access.

## NIST Timeline



## Guidelines on Minimum Standards for Developer Verification of Software

Paul E. Black  
Barbara Guttman  
Vadim Okun  
Software and Systems Division  
Information Technology Laboratory

July 2021

**NIST**  
National Institute of  
Standards and Technology  
U.S. Department of Commerce

# Cyber EO Discussion Topics

---

What should I be doing now to prepare for the new FAR rules?

#1

I am a cloud provider. How might the EO's modernization of FedRAMP impact me?

#2

What organizations may be impacted by an SBOM requirement?

#3

How does the move towards Zero Trust align with the CMMC framework requirements?

#4





# Proposed/Pending Legislation

---

# Proposed Legislation

---

- Cyber Incident Reporting Act – 72-hour mandatory reporting period for actual or potential “cyber intrusions”
  - Covered entities include Federal contractors
  - Failure to comply could result in monetary penalties
- FISMA Reform Bill – contractor to notify an agency “immediately” if it has a reasonable basis to conclude that an incident involving “federal information” has occurred
  - Additional reporting requirements if “major” incident occurs
- Ransom Payment Disclosure – 48 hour mandatory reporting period for covered entities after paying a ransom
  - Covered entities include any entity engaged in interstate commerce or an entity that receives federal funds

# Proposed Legislation Discussion Topics

---

How can my company best prepare now for new cyber incident reporting requirements?

01

What are the largest challenges in preparing for or meeting existing and proposed cybersecurity requirements?

02

What resources are available to assist businesses in meeting existing and proposed cybersecurity requirements?

03





# Major Takeaways/Best Practices

---



# Major Takeaways

---



- Upcoming additions to the landscape likely will require you to take action
  - CMMC
  - Accompanying clauses
  - Regulations stemming from new Executive Order
  - New legislation



- Applicability of requirements will depend on company's position in the supply chain



- Things are changing quickly – it's critical to stay updated



# Best Practices

---



## Assess required data and CMMC requirement

- Begin thinking about pre-assessment if haven't already



## Understand your supply chain and service providers

- CMMC requirement flows down
- Full reach of new Executive Order is unclear



Prepare to update vendor agreements as well as data security and incident response plans



Compliance ≠ Security

# Questions?

---



**Townsend Bourne**

tbourne@sheppardmullin.com  
202.747.2184



**Nikki Snyder**

nsnyder@sheppardmullin.com  
202.747.3218



**Mike Tomaselli**

mtomaselli@chessconsultingllc.com  
703.282.5077



**Sharon Steele**

Sharon.Steele@xerox.com  
202.414.1291



# Resources

---



# Helpful Resources

---

## CMMC Resources

- **CMMC Accreditation Body:** <https://www.cmmcab.org/>
- **DoD CMMC:** <https://www.acq.osd.mil/cmmc/>
- **DoD CMMC FAQs:** <https://www.acq.osd.mil/cmmc/faq.html>

## Small Business Cyber Resources

- **Small Business Administration:** <https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats>
- **NIST – Small Business Cybersecurity Fundamentals:** <https://nvlpubs.nist.gov/nistpubs/ir/2016/NIST.IR.7621r1.pdf>

## Cloud

- **FedRAMP:** [FedRAMP.gov](https://www.fedramp.gov/)
- **DoD Cloud Security Requirements Guide:** [https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/Cloud\\_Computing\\_SRG\\_v1r3.pdf](https://dl.dod.cyber.mil/wp-content/uploads/cloud/pdf/Cloud_Computing_SRG_v1r3.pdf)

# Helpful Resources

## Cybersecurity E.O. Resources

- **NIST Cyber EO Website** - <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/executive-order>
- **NIST & CISA, “Defending Against Software Supply Chain Attacks”** – <https://www.cisa.gov/publication/software-supply-chain-attacks>
- **NIST Security Measures for EO Critical Software Use** – <https://www.nist.gov/itl/executive-order-improving-nations-cybersecurity/security-measures-eo-critical-software-use>
- **NIST Recommended Minimum Standards for Verification of Software** – <https://nvlpubs.nist.gov/nistpubs/ir/2021/NIST.IR.8397.pdf>
- **Minimum Elements For a Software Bill of Materials (SBOM)** - [https://www.ntia.doc.gov/files/ntia/publications/sbom\\_minimum\\_elements\\_report.pdf](https://www.ntia.doc.gov/files/ntia/publications/sbom_minimum_elements_report.pdf)
- **OMB Memo: Protecting Critical Software** – <https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf>
- **NIST SP-800-207 Zero Trust Architecture** - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-207.pdf>
- **OMB Federal Zero Trust Strategy** - <https://zerotrust.cyber.gov/federal-zero-trust-strategy/>
- **CISA Zero Trust Maturity Model** - <https://zerotrust.cyber.gov/zero-trust-maturity-model/>
- **CISA Cloud Security Technical Reference Architecture (TRA)** – [Moving the U.S. Government Towards Zero Trust Cybersecurity Principles](#)
- **NIST Updated Secure Software Development Framework (NIST SP 800-218)** - <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-218-draft.pdf>



# Helpful Resources

## SMRH Blogs

- **Moving to Zero Trust – CISA and OMB Seek Comments on Zero Trust Publications and Cloud Security Technical Reference Architecture under Cybersecurity Executive Order** (Sept. 15, 2021) - <https://www.governmentcontractslawblog.com/2021/09/articles/cybersecurity/cisa-omb-seek-comments-on-zero-trust-publications/>
- **Watch Your Boundaries – FedRAMP Releases Draft Authorization Boundary Guidance for Public Comment** (July 28, 2021) - <https://www.governmentcontractslawblog.com/2021/07/articles/cybersecurity/fedramp-releases-draft-authorization-boundary-guidance/>
- **Right on Time – NIST Releases Definition of “Critical Software” Per Biden’s Cybersecurity Executive Order** (June 29, 2021) - <https://www.governmentcontractslawblog.com/2021/06/articles/cybersecurity/nist-releases-definition-of-critical-software/>
- **Biden’s Cybersecurity Executive Order** (May 17, 2021) - <https://www.governmentcontractslawblog.com/2021/05/articles/cybersecurity/bidens-cybersecurity-executive-order/>
- **CMMC Update** (May 28, 2020) – <https://www.governmentcontractslawblog.com/2020/05/articles/audits/dod-cmmc-update/>
- **CMMC Version 1.0** (February 27, 2020) – <https://www.governmentcontractslawblog.com/2020/02/articles/supply-chain/cmmc-level/>
- **The Pitfalls of Factoring in Security and CMMC Costs** (M. Tomaselli, June 8, 2021) - <https://www.nationaldefensemagazine.org/articles/2021/6/8/the-pitfalls-of-factoring-in-security-and-cmmc-costs>

## National Defense Article

# Cyber Requirements – FAR

FAR 52.204-21	<b>Basic Safeguarding of Covered Contractor Information Systems</b>	Protect Federal Contract Information – 15 basic security requirements No reporting requirement
Open FAR Case 2017-016	<b>Controlled Unclassified Information</b>	Will implement CUI program Will include requirements for protection of CUI (likely NIST SP 800-171 for contractor systems)
Open FAR Case 2021-017	<b>Cyber Threat &amp; Incident Reporting and Info Sharing</b>	Will include requirements for incident reporting and response for IT/OT/ICT service providers
Open FAR Case 2021-019	<b>Standardizing Cybersecurity Requirements for Unclassified Federal Information Systems</b>	Will standardize common cybersecurity contractual requirements across agencies



# Cyber Requirements – DFARS

DFARS 252.204-7012	<b>Safeguarding Covered Defense Information &amp; Cyber Incident Reporting</b>	Protect Covered Defense Information (CDI) and CUI in contractor systems per NIST 800-171 Report cyber incidents within 72 hours Includes incident response requirements
	<b>(b)(2)(ii)(D) – contractor use of external cloud service provider</b>	External cloud service provider must meet FedRAMP Moderate or equivalent and incident response requirements
DFARS 252.204-7019	<b>Notice of NIST SP 800-171 DoD Assessment Requirements</b>	If required to implement NIST SP 800-171, Offeror must have current assessment Assessment score must be posted in SPRS
DFARS 252.204-7020	<b>NIST SP 800-171 DoD Assessment Requirements</b>	Requirement for NIST SP 800-171 assessment and posting in SPRS
DFARS 252.204-7021	<b>Contractor Compliance with CMMC Level Requirement</b>	Requirement for current CMMC certificate at level required by contract Use of clause must be approved for use before Oct. 1, 2025

# Cyber Requirements – DFARS (Cloud)

DFARS 252.239-7009	<b>Representation of Use of Cloud Computing</b>	Offeror must represent whether contract will use cloud computing services
DFARS 252.239-7010	<b>Cloud Computing Services</b>	DoD cloud service providers must comply with DoD Cloud Security Requirements Guide  Includes incident response requirements