

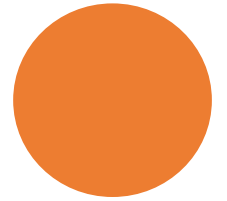
# CMMC Update in 2024

Dr. Jose Neto

- Certified CMMC Professional (CCP)
- Provisional CMMC Assessor



**PC-WARRIORS**

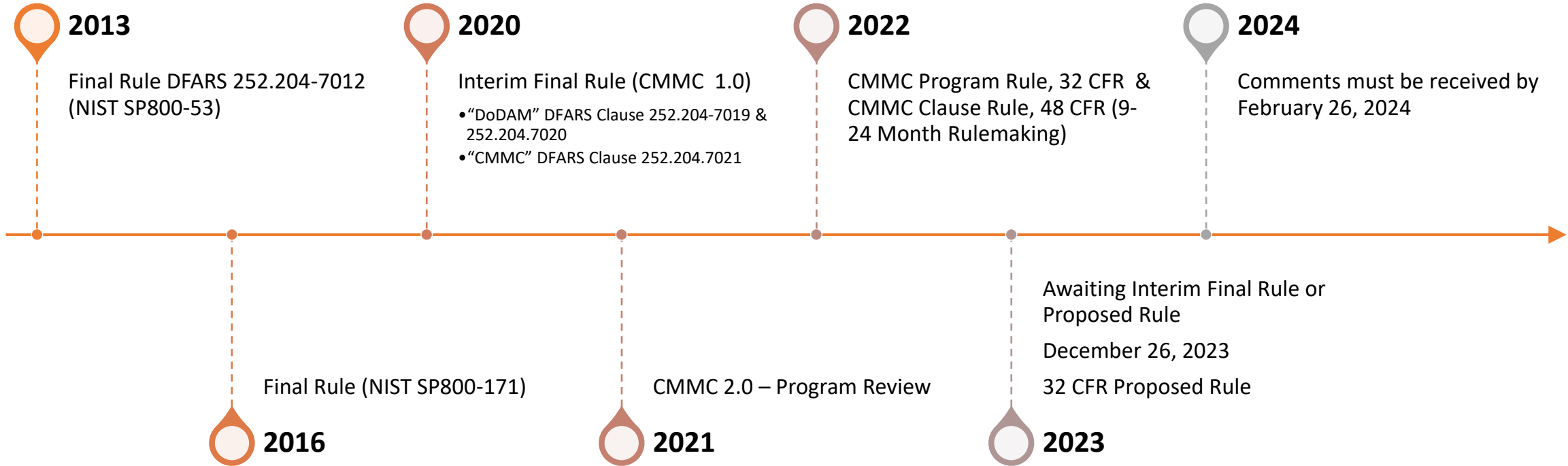


# Agenda



- CMMC Historical Timeline
- CMMC 2.0 update
- Current Challenges
  - Scoping
  - Timeframe
  - Cost
  - MSPs/Cloud Providers

# Cyber Compliance Historical Timeline



# Cybersecurity Maturity Model Certification

- The CMMC Program is designed to verify protection of sensitive unclassified information shared between the Department and its contractors and subcontractors or generated by the contractors and subcontractors
- Emphasis on Supply Chain Compliance




# CMMC 2.0



- The CMMC 2.0 framework consists of three levels of cybersecurity maturity, ranging from basic cyber hygiene to advanced cybersecurity practices.

- Each level builds upon the previous level and includes specific practices and processes that organizations must implement and demonstrate in order to achieve certification.

CMMC Model 2.0	Model	Assessment
<b>LEVEL 3</b> Expert	<b>110+</b> practices based on NIST SP 800-172	Triennial government-led assessments
<b>LEVEL 2</b> Advanced	<b>110</b> practices aligned with NIST SP 800-171	Triennial third-party assessments for critical national security information; Annual self-assess- ment for select programs
<b>LEVEL 1</b> Foundational	<b>17</b> practices	Annual self-assessment



# FAR clause 52.204-21

- Basic Safeguarding of Covered Contractor Information Systems.
- FAR clause 52.204-21 requires compliance with **15 security requirements** to achieve basic cybersecurity.

- **Affirmation Requirements (New)**

A senior official from the prime contractor and any applicable subcontractor will be required to annually affirm continuing compliance with the specified security requirements. Affirmations are entered electronically in SPRS (see § 170.22 for details on Affirmation requirements and procedures).

# **FAR clause 52.204-21**

## **15 security requirements**

- (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.

# 15 security requirements

Continued..

(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.



# DFARS clause 252.204-7012



Contractors shall include the clause in subcontracts involving covered defense information or operationally critical support.



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



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


Continued..

Provide adequate security on all covered contractor information systems by implementing the 110 security requirements specified in the National Institute of Standards and Technology (NIST) Special Publication (SP) 800–171

The DFARS clause 252.204–7012 includes additional requirements; for example, defense contractors must meet Federal Risk and Authorization Management Program (FedRAMP) standards by confirming that their Cloud Service Providers (CSP) have achieved the FedRAMP Baseline Moderate or Equivalent standard. The DFARS clause 252.204–7012 also requires defense contractors to flow down all the requirements to their subcontractors.

# In November 2020

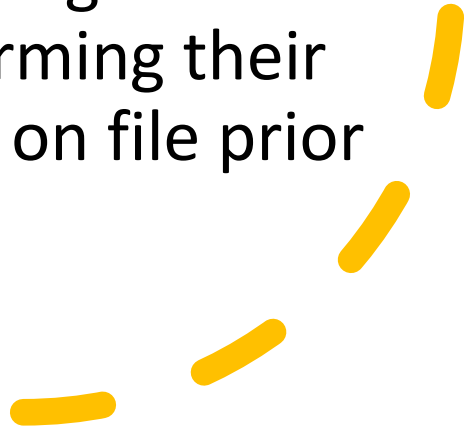
- DoD released its DFARS Interim Rule, the *Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements*
- This rule introduced three new clauses
  - DFARS clause 252.204–7019
  - DFARS clause 252.204–7020
  - DFARS clause 252.204–7021



# DFARS clause 252.204–7019

- DFARS clause 252.204–7019 strengthens DFARS clause 252.204–7012 by requiring contractors to conduct a NIST SP 800–171 self-assessment according to NIST SP 800–171 DoD Assessment Methodology.
- Self assessment scores must be reported to the Department via SPRS. SPRS scores must be submitted by the time of contract award and not be more than three years old.

# DFARS clause 252.204– 7020

- DFARS clause 252.204–7020 notifies contractors that DoD reserves the right to conduct a higher-level assessment of contractors' cybersecurity compliance, and contractors must give DoD assessors full access to their facilities, systems, and personnel.
  - Flow down requirements by holding contractors responsible for confirming their subcontractors have SPRS scores on file prior to awarding them contracts.
- 

# DFARS clause 252.204– 7021

- DFARS clause 252.204–7021 will be inserted in solicitations and contracts. It will guide the compliance level required for the organizations.
- Ensure adequate availability of assessors and C3PAOs.
- Exceptions for organizations only dealing with COTS.
- DFARS clause 252.204–7021 also stipulates contractors will be responsible for flowing down the CMMC requirements to their subcontractors.




- Scoping
- Timeframe
- Cost
- MSPs/Cloud Providers








# Remediation Timeframe

- 18 months – No formal SSP, third party support (MSP), unknown cyber posture, in-house self-assessment.
  - 12 months – Basic SSP, dedicated compliance person, in-house self-assessment.
  - 6 months - Mature security documentation, dedicated security team, neutral third-party compliance assessment.
- 

# Cost

Multiple commenters commented on the cost impact of CMMC to small businesses, suggesting that the cost to become and remain compliant is too high.



The Department currently has no plans for separate reimbursement of costs to acquire cybersecurity capabilities or a required cybersecurity certification that may be incurred by an offeror on a DoD contract. Costs may be recouped via competitively set prices, as companies see fit.

# MSPs/Cloud Providers

---

- If the Cloud Service Provider's (CSP) product or service offering is not FedRAMP Authorized at the FedRAMP Moderate (or higher) baseline but meets security requirements equivalent to those established by the FedRAMP Moderate (or higher) baseline.
- Equivalency is met if the CSP's System Security Plan (SSP) or other security documentation describes the system environment, system responsibilities, a Customer Responsibility Matrix (CRM) that summarizes how each control is MET and which party is responsible for maintaining that control that maps to the NIST SP 800–171 Rev 2 requirements.



## **Team Collaboration**

- A major success factor in your compliance journey is establishing a cohesive team of security ambassadors across the enterprise to work together in building and maintaining a secure resilient infrastructure.

# Cyber Compliance Best Practices



Plan accordingly based on the size of the organization and its mission



Allocate a realistic budget based on the value of your assets (Information)



Hire a competent cyber firm to conduct a "Gap Analysis"



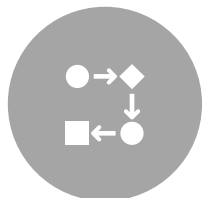
Establish a security team to formulate an effective deployment plan



Document all processes in tandem with the technical deployment



Re-test effectiveness of all controls at key milestone intervals



Once compliance is attained, sustain compliance through continuous monitoring



**PC-WARRIORS**

# Questions?

## Contact Information

Dr. Jose Neto

407-715-7392

JNeto@PC-Warriors.com

<https://PC-Warriors.com>



**PC-WARRIORS**

Leaders in Military-Grade Cybersecurity Compliance

We helped secured a **PERFECT 110** Compliance rating in an official **DoD DIBCAC** assessment for one of our valued clients.

CALL US for a **FREE** Consultation