

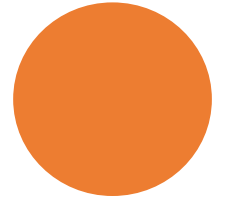
# CMMC Planning in 2023

Dr. Jose Neto

- Certified CMMC Professional (CCP)
- Provisional CMMC Assessor



**PC-WARRIORS**



# Agenda



- What is the current cyber threat landscape and its significance
- CMMC 2.0 update
- Scoping
- Collaboration
- Best Practices

# What is the current cyber threat landscape

- According to the Cybersecurity and Infrastructure Security Agency (CISA), there were over 100,000 cyber incidents reported to the agency in 2021.
1. Ransomware
  2. Phishing - Business Email Compromise
  3. Supply Chain Attacks
  4. Zero-Day Exploits
  5. Nation-State Threats
  6. Internet of Things (IoT) Threats



# Ransomware

- In May 2021, the Colonial Pipeline, a major U.S. fuel pipeline operator, was hit by a ransomware attack
- In July 2021, a ransomware attack targeting software provider Kaseya resulted in the compromise of hundreds of businesses and organizations around the world.

# Phishing

- This attack typically involves an email that appears to be from a legitimate source, such as a bank or other financial institution, asking the recipient to click on a link or provide sensitive information.



## GPT-4 is now live



OpenAI Announcement <donotreply@jgu.edu.in>  
To [redacted]@outlook.com



Hi There,

Chat GPT-4 is now only available for people with the OpenAI token

Don't miss the time-limited OpenAI DEFI token airdrop to get access to gpt4 chat.

[Get Started](#)

Our partnership resulted in the creation of a cryptocurrency which will serve as a gateway to our ecosystem such as access to GPT-4 Chat, it will also offer access our next concepts based on DEFI.

We are excited to announce that our token airdrop will be begins Wednesday **April 2 at 12:00 p.m.** and ends **Saturday at 4 p.m.**

If you encounter any issues with our airdrop, please visit our [help center](#) for assistance.

Action Required: Password Expiration Notice 3/18/2023



Pc-warriors.com Portal <itsupport=pc-warriors.com@herita>  
To Dr. Jose Neto



# Office 365

Hello user,

Password for your Account will be expiring today,  
to continue using the same password, proceed below accordingly.

[Keep Same Password](#)

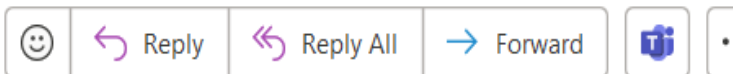
**⚠ Complete the above task to avoid Email disconnection**

©2023 Microsoft Password Expiration Notice

+14023095815 Mailbox – Kevin M. Easton Called at 05:05PM



Easton, Kevin M. <kmeaston@co.pg.md.us>  
To Easton, Kevin M.



Mon 10/31/2022 6:03

Mailbox – 2.1.1 Kevin M. Easton Cell Phone  
Message Length – 00:25 secs

+14023095815 Called you at 05:05PM CST

[Listen to VoiceMail Here](#)

**Kevin M. Easton**

Acting Assistant Division Chief, Community Corrections Division

Prince George's County Department of Corrections

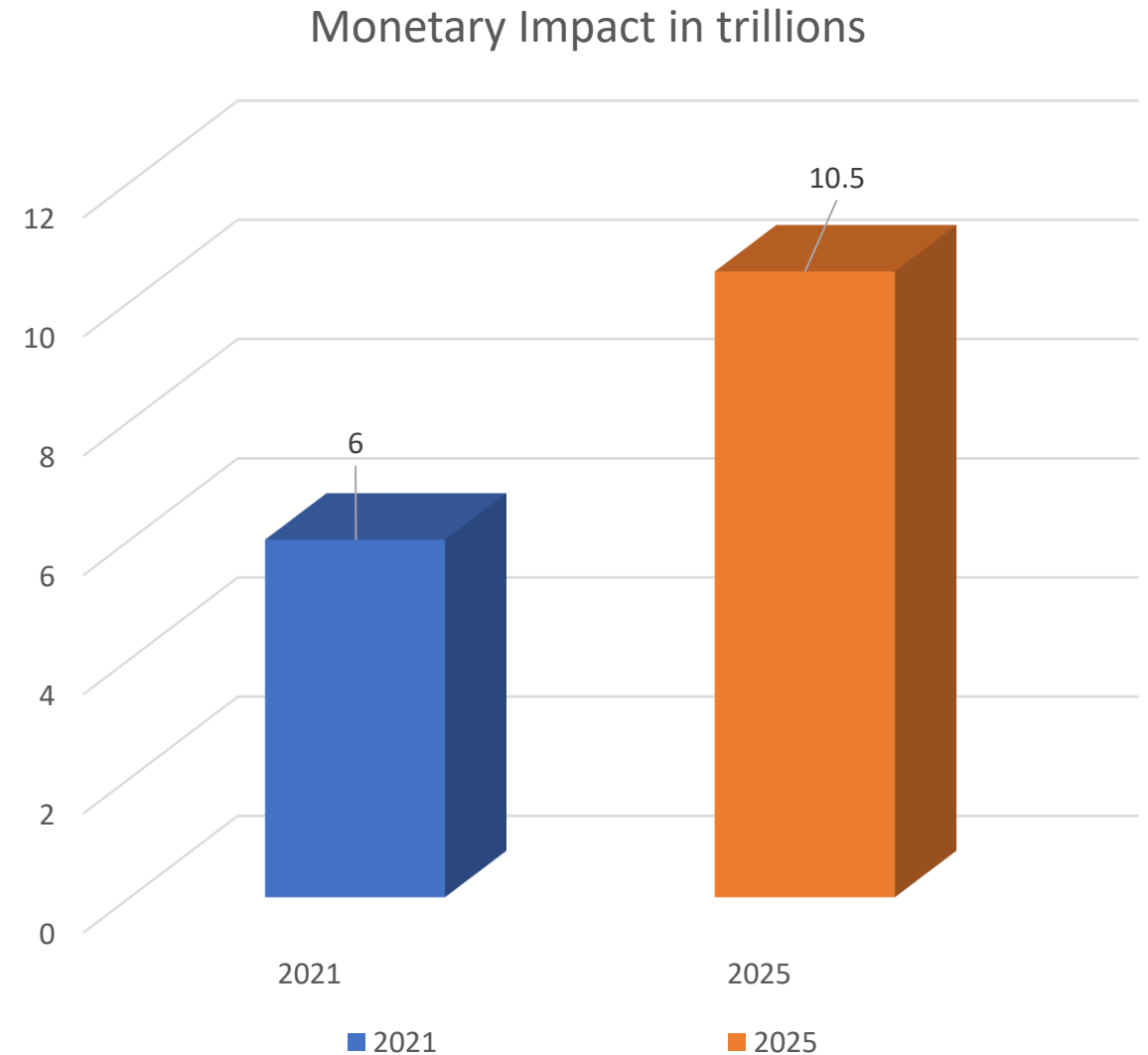
Email: [kmeaston@co.pg.md.us](mailto:kmeaston@co.pg.md.us)

---

This E-mail and any of its attachments may contain Prince George's County Government or Prince George's County 7th Judicial Circuit Court proprietary information or Protected Health Information, which is privileged and confidential. This E-mail is intended solely for the use of the individual or entity to which it is addressed. If you are not the intended recipient of this E-mail, you are hereby notified that any dissemination, distribution, copying, or action taken in relation to the contents of and attachments to this E-mail is strictly prohibited by federal law and may expose you to civil and/or criminal penalties. If you have received this E-mail in error, please notify the sender immediately and permanently delete the original and any copy of this E-mail and any printout.

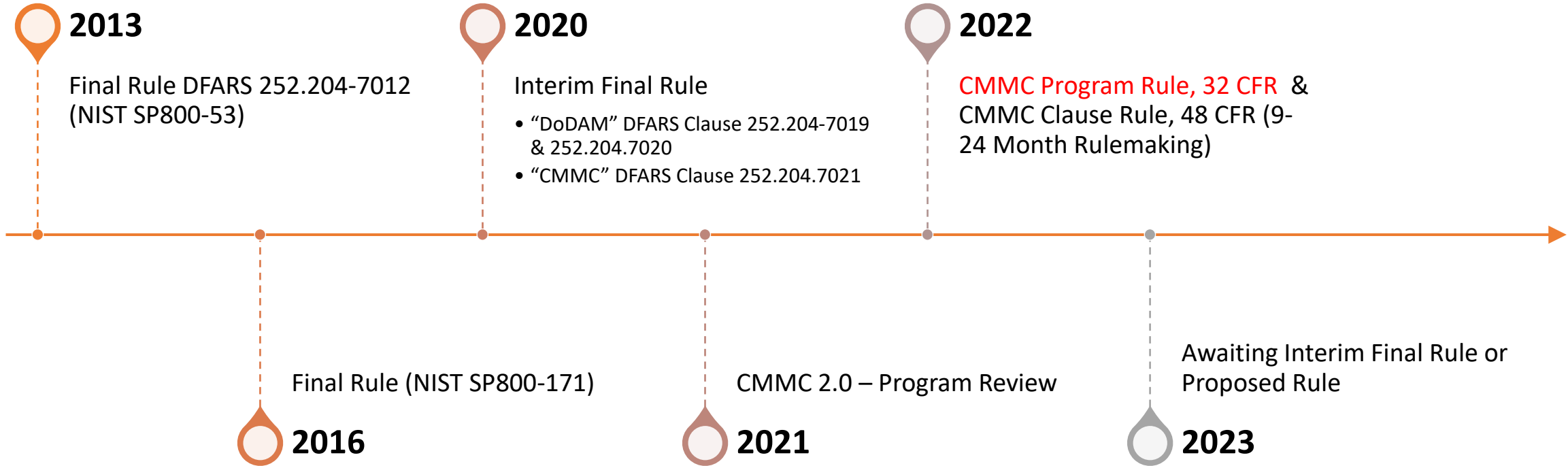
# Significance and Monetary Impact

- According to a report by the National Small Business Association, 50% of small businesses in the United States have been the victim of a cyber attack
- Small businesses are particularly vulnerable to cyber attacks and are often targeted because they have less robust cybersecurity measures in place.





# Cyber Compliance Historical Timeline



# 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

# LEVEL 1

## **17 basic security controls divided into two categories:**

Basic Cyber Hygiene: This includes implementing basic security practices such as maintaining an inventory of authorized and unauthorized devices, using antivirus software, and training employees in cybersecurity awareness.

Protecting Federal Contract Information (FCI): This includes implementing security controls such as access controls, incident response, and system and communications protection, among others.

# LEVEL 2



## Challenges

- Scoping
- Deployment/Collaboration
- Ongoing validation
- Documentation in tandem



# Scoping









- Controlled Unclassified Information (CUI) Assets **Will Process CUI**
- Security Protection Assets
- Contractor Risk Managed Assets **Can process CUI**
- Specialized Assets (IOT) **May or may not**
- Out-of-Scope Assets **Will not process**



## **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.
- The ideal formula relies on using strategic tools to create, track, review and monitor effectiveness.
- Assessors will also appreciate a consolidated library that organizes all the relevant security artifacts.



-  Dashboard
-  Customers >
-  Projects >
-  **Tasks**
-  Messages
-  Support
-  Knowledgebase
-  Other >

### Incomplete


**3.1.3** 

**Normal**

Project: Comprehensive Readiness Review #1  
Client: Defense Contractor 2  
Created: 03-02-2023  
Start Date: ---  
Due: ---


 

### In-Progress

**3.1.1** 

**Normal**

Project: Comprehensive Readiness Review #2  
Client: PC-Warriors LLC  
Created: 03-01-2023  
Start Date: 06-30-2022  
Due: ---



### Complete

**3.1.1** 

**High**

Project: Comprehensive Readiness Review #1  
Client: Defense Contractor 2  
Created: 03-01-2023  
Start Date: 03-01-2023  
Due: ---



### Validated by Assessor

**3.1.2** 

**Normal**

Project: Comprehensive Readiness Review #1  
Client: Defense Contractor 2  
Created: 03-01-2023  
Start Date: 03-01-2023  
Due: ---



### 3.2.1

Project: Comprehensive Readiness Review #1

Milestone: Development

#### Description

##### 3.2.1 SECURITY REQUIREMENT

Ensure that managers, systems administrators, and users of organizational systems are made aware of the security risks associated with their activities and of the applicable policies, standards, and procedures related to the security of those systems.

##### ASSESSMENT OBJECTIVE

Determine if:  
3.2.1[a] security risks associated with organizational activities involving CUI are identified.

Deployment/Testing -

3.2.1[b] policies, standards, and procedures related to the security of the system are identified.

Deployment/Testing -

3.2.1[c] managers, systems administrators, and users of the system are made aware of the security risks associated with their activities.

Deployment/Testing -

3.2.1[d] managers, systems administrators, and users of the system are made aware of the applicable policies, standards, and procedures related to the security of the system.

Deployment/Testing -

[Edit Description](#)

Assigned Users ✕

My Timer ⓘ

00:00 ▶

#### Settings

- Start Date: ---
- Due Date: ---
- Status: **Incomplete**
- Priority: **Normal**
- Client: **Visible**
- [Add A Reminder](#)

#### Tags

[Edit Tags](#)

#### Dependencies

[Add A Dependency](#)

#### Actions

- [Change Milestone](#)
- [Stop All Timers](#)
- [Archive](#)
- [Delete](#)

#### Information

Task ID	#6
Created By	Joe Neto
Date Created	03-02-2023

#### Checklist 0/4

- 3.2.1[d]
- 3.2.1[c]
- 3.2.1[b]
- 3.2.1[a]

[Create A New Item](#)

#### File Attachments

[Add a file attachment](#)

#### Comments

Post a comment...

Total Time	00:00
Time Invoiced	00:00
Project	#2



# 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”



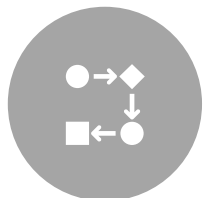
Establish a security team to formulate an effective deployment plan



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**