

# CMMC Assessments Lessons Learned from the Front Lines



# FERNANDO MACHADO

## CISO, CYBERSEC INVESTMENTS

### ■ Cybersecurity Consulting:

- 15 years DoD cybersecurity experience
- NIST 800-171: Controlled Unclassified Information (CUI) / Cybersecurity Maturity Model Certification (CMMC)
- Army, Navy, Air Force customer experience

### ■ Certified:

- Lead Certified CMMC Assessor (Lead CCA)
- Certified CMMC Professional (CCP)
- Authorized CMMC 3<sup>rd</sup> Party Assessment Organization (C3PAO)

### ■ Awards:

- President's Volunteer Service Award



1900 S Harbor City Blvd. Suite 340  
Melbourne, Florida 32901

[info@cybersecinvestments.com](mailto:info@cybersecinvestments.com)

1-800-960-8802



PUBLIC

Public Release Authorized

# CARTER SCHOENBERG

## VICE PRESIDENT, ASSESSMENT & COMPLIANCE

- 32 years' experience in cybersecurity, board level cyber risk management, ATOs, compliance, cyber law, criminal & Civil investigations.
- Lead CCA (L-CCA), CISSP, QTE
- Head of an Authorized C3PAO

### Office Sites

- *Anchorage*
- *Atlanta*
- *Minneapolis*
- *Washington, D.C.*



[cschoenberg@koniagcyber.com](mailto:cschoenberg@koniagcyber.com)



# AGENDA

- *Software Assurance*
- *CMMC Preparation and Assessment Challenges*
- *From Joint Surveillance Voluntary Assessments (JSVA) to CMMC Assessments: Lessons Learned*
- *External Service Providers (ESP's)*
- *Enclaves*
- *Significant Change*

# SOFTWARE ASSURANCE

## ■ Secure Software Development

### Revision 2

#### SC.L2-3.13.2 – SECURITY ENGINEERING

Employ architectural designs, software development techniques, and systems engineering principles that promote effective information security within organizational systems.

#### ASSESSMENT OBJECTIVES [NIST SP 800-171A]<sup>189</sup>

Determine if:

- [a] architectural designs that promote effective information security are identified;
- [b] software development techniques that promote effective information security are identified;
- [c] systems engineering principles that promote effective information security are identified;
- [d] identified architectural designs that promote effective information security are employed;
- [e] identified software development techniques that promote effective information security are employed; and
- [f] identified systems engineering principles that promote effective information security are employed.

### Revision 3

#### 03.16.01 Systems Security Engineering Principles

##### ASSESSMENT OBJECTIVE

*Determine if:*

**A.03.16.01.ODP[01]:** *systems security engineering principles to be applied to the development or modification of the system and system components are defined.*

**A.03.16.01: <A.03.16.01.ODP[01]: systems security engineering principles>** are applied to the development or modification of the system and system components.

##### ASSESSMENT METHODS AND OBJECTS

###### Examine

[SELECT FROM: system and services acquisition policy; system and services acquisition procedures; procedures addressing security engineering principles used in the development and modification of the system; system design documentation; security requirements and specifications for the system; system security plan; other relevant documents or records]

###### Interview

[SELECT FROM: personnel with acquisition/contracting responsibilities; personnel with information security responsibilities; personnel with system development and modification responsibilities; system developers]

###### Test

[SELECT FROM: processes for applying security engineering principles in system development and modification; mechanisms supporting the application of security engineering principles in system development and modification]

# ***CMMC PREPARATION AND ASSESSMENT CHALLENGES***

- *“Network” vs. “System” (i.e. Scoping)*
- *Availability of Evidence*
- *Right People at the Right Time*
- *ESP’s*

# ***FROM JOINT SURVEILLANCE VOLUNTARY ASSESSMENTS (JSVA) TO CMMC ASSESSMENTS: LESSONS LEARNED***

- *Joint Surveillance Voluntary Assessments (JSVA) Explained:*
  - *Defense Contract Management Agency (DCMA) Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) Involvement*
  - *CMMC Conversion*
- *CMMC Assessments Explained:*
  - *C3PAO Involvement*
  - *Conditional versus Final CMMC Level 2 Certificate of Status*

## ***EXTERNAL SERVICE PROVIDERS (ESP'S)***

- *Certified at Level 2 vs. Non-Certified at CMMC Level 2*
- *Sampling to include the ESP*
- *Rules of Behavior for the Organization Seeking Certification (OSC)*
- *Customer Responsibility Matrix (CRM) versus Service-Level Agreement (SLA)*

# ENCLAVES

## Eutopia vs Dystopia

### ■ Pros

- *Easier to implement*
- *Potential to “inherit” large number of requirements*

### ■ Cons

- *One size does not fit all*
- *Azure Virtual Desktop (AVD) (Friend of Foe)*
- *Risk of missing elements that can only be identified, validated and resolved with onsite inspection*

## **SIGNIFICANT CHANGE**

- Cyber-AB Committees working
- *The following types of Major Changes require pre-notification and acknowledgement by the GSA ISSO, ISSM and CO/COR prior to their implementation. These changes may require re-assessment:*
  - *Changes to the CUI data types and retention by the system.*
  - *Changes to the encryption used to protect GSA CUI data at rest or in transit.*
  - *Re-hosting or re-platforming the system including migrations to different data centers, to the cloud, or between cloud providers.*
  - *Addition of any External Service that may store, process or transmit CUI.*
  - *Removal of security components used to protect and monitor the information system.*
  - *Removal of MFA requirements for administrative access to the system or GSA CUI data.*

# QUESTIONS?

*Fernando Machado*

[info@cybersecinvestments.com](mailto:info@cybersecinvestments.com)



*Carter Schoenberg*

[cschoenberg@koniagcyber.com](mailto:cschoenberg@koniagcyber.com)

