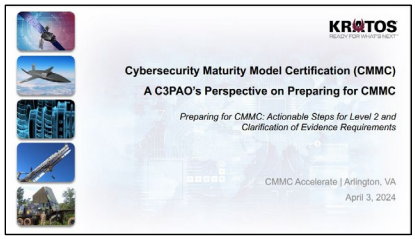



# A C3PAO's Perspective on Preparing for CMMC

## Preparing for CMMC: Actionable Steps for Level 2 and Clarification of Evidence

Thank you for downloading this Hypori presentation. Carahsoft is the distributor for Hypori CMMC solutions available via GSA 2GIT, NASA SWEP V, ITES-SW2 and other contract vehicles.

To learn how to take the next step toward acquiring Hypori's solutions, please check out the following resources and information:

For additional resources:
carah.io/HyporiResources

For upcoming events:
carah.io/HyporiEvents

For additional Hypori solutions:
carah.io/HyporiSolutions

For additional CMMC solutions:
carah.io/CMMC

To set up a meeting:
Hypori@carahsoft.com
703-871-8505

To purchase, check out the contract vehicles available for procurement:
carah.io/HyporiContracts





KRATOS
READY FOR WHAT'S NEXT™

# Cybersecurity Maturity Model Certification (CMMC)

# A C3PAO's Perspective on Preparing for CMMC

*Preparing for CMMC: Actionable Steps for Level 2 and Clarification of Evidence Requirements*

CMMC Accelerate | Arlington, VA

April 3, 2024

# Agenda

- Background
- Preparing for an Assessment
  - Actionable Steps
  - Evidence Requirements

KRATOS
READY FOR WHAT'S NEXT™

# Background

Who is Kratos? What's our perspective on the C3PAO audit process?

# Kratos

- Kratos builds technology and other products supporting strategic and transformational national security programs
  - Unmanned systems
  - Assured aerospace communications
  - Cybersecurity
  - Strategic programs
  - Microwave electronics
  - Training and simulation

# What We've Learned

- Documentation, documentation, documentation
- Asset inventory
- Multi-factor authentication
- Centralized auditing
- Software/application approved/deny lists
- Patching and vulnerability remediation
- CUI handling and marking

KRATOS
READY FOR WHAT'S NEXT™

# Preparing for Assessment

What are actionable steps? What are the evidence requirements?

# Actionable Steps – Documentation

- Documentation requirements have been relaxed in CMMC 2.0
- Documentation is still required (e.g., AC.L2-3.1.21 requires that portable storage devices be identified *and documented*)
- Consistency of documentation is key
- Where documentation is provided, there is an expectation that what is documented can be corroborated or demonstrated
- Complete and thorough documentation is a foundation for assessment success

# Actionable Steps – Asset Inventory

- A simple inventory of assets is not sufficient
- Assets, in the context of CMMC, include
  - Endpoints and Servers
  - Users
  - Elevated privileges (tied in with the User inventory)
  - Applications/software
  - Sites
- Inventories for each of the above are needed

# Actionable Steps – Multi-Factor Authentication

- CMMC requires multi-factor authentication (MFA) in the following scenarios
  - Network access to non-privileged accounts
  - Local and network access to privileged accounts
- MFA is a technical configuration that presents challenges
  - Cost and scope
  - Technical implementation and integration
  - System compatibility (e.g., network devices)
  - Change in daily operations that effects many users

# Actionable Steps – Centralized Auditing

- Auditing is key component of protecting CUI
- Key considerations
  - Standardized network time protocol for correlation
  - Need to capture from a potentially wide-range of endpoint types
  - **Defined audit events for capture**
  - Detection and notification of logging failures (prove the negative)
  - **Reporting, correlation, and reduction capabilities**
  - Audit log reviews and analysis
  - Audit record protection

# Actionable Steps – Software Control

- A technical mechanism to prevent the use of unauthorized software is required
- Either deny-by-exception (deny list) or permit-by-exception (approved list)
- Deny list is an easier implementation and can be used as a bridge to permit-by-exception
- Permit-by-exception is a more difficult implementation and can cause disruptions to users, particularly administrators who leverage software that is privileged in nature (e.g., PowerShell)
- Documentation is necessary to support the implementation
- As an auditor, it's just as important to understand how the list is defined as it is to see the implementation

# Actionable Steps – Patching and Vulnerability Remediation

- The maturity of patching has a direct correlation to vulnerabilities
- Vulnerability remediation must be driven by a solid process
- **Remediation timeframes are necessary**
- Evaluation of vulnerability management is directly correlated to meeting remediation timeframes
- Processes are needed for addressing vulnerabilities outside of the remediation timeframes
- Patching and vulnerability scanning are similar, but there are differences
  - Patching: enumerating flaws that are associated with vulnerabilities
  - Scanning: enumerating vulnerabilities associated with missing patches or improper configuration

# Actionable Steps – CUI Handling and Marking

- Understanding the data flow throughout the organization
- What is CUI? When does it need to be marked and by whom?
- Proper and consistent markings with distribution limitation
- Required for paper and electronic media
- Identification of where CUI is stored
- Physical and digital protection of CUI
- Consistency of handling and marking procedures
- Depending on the organization, it is possible that procedures are documented in multiple places
- In such cases, recommend creation of a standard or roadmap that provides a single point of reference for CUI handling and marking

KRATOS
READY FOR WHAT'S NEXT™

# Evidence Requirements

What are the evidence requirements? How do I know what kinds of evidence to prepare?

# What Are the Evidence Requirements?

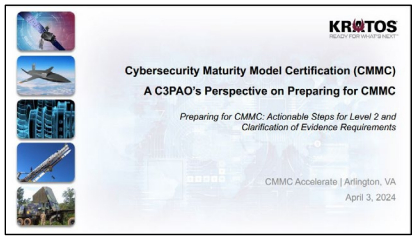
- Affirmation: must verifiably correlate to implementation, performance, or support of a practice
- Artifact: demonstrate the extent of implementing, performing, or supporting a practice
- Demonstration/Test: observed by an assessor and performed on the production system being assessed

# Common Requirements that Can Confuse

- Identified
  - AC.L1-3.1.1 requires that authorized users are identified
  - A list of authorized users in any form is sufficient, as the list satisfies the requirement that authorized users are identified
  - Distinction: what is *being* identified (authorized users) versus what *is* identified (an authorized user)
- Specified
  - AU.L2-3.3.7 requires that an authoritative source with which to compare and synchronize internal system clocks is specified
  - A tool configuration showing the source is sufficient on its own; documentation that specifies the source along with the tool configuration is preferred
  - Distinction: specific and/or for a specific purpose (time.gov for clock synchronization)

# Common Requirements that Can Confuse (cont.)

- Defined
  - AU.L2-3.3.1 requires that audit records are retained as defined
  - The log retention configuration in a tool or a policy enumerating the definition are each sufficient, preferably both
  - Distinction: general, agnostic, and sets a firm baseline (logs must be retained for at least 90 days)
- Documented
  - CM.L2-3.4.5 requires that physical and logical access restrictions associated with changes are documented
  - A document (policy, procedure, work instruction) depicting the restrictions is sufficient
  - Distinction: static document separate from a tool configuration




# A C3PAO's Perspective on Preparing for CMMC

## Preparing for CMMC: Actionable Steps for Level 2 and Clarification of Evidence

Thank you for downloading this Hypori presentation. Carahsoft is the distributor for Hypori CMMC solutions available via GSA 2GIT, NASA SWEP V, ITES-SW2 and other contract vehicles.

To learn how to take the next step toward acquiring Hypori's solutions, please check out the following resources and information:

For additional resources:
carah.io/HyporiResources

For upcoming events:
carah.io/HyporiEvents

For additional Hypori solutions:
carah.io/HyporiSolutions

For additional CMMC solutions:
carah.io/CMMC

To set up a meeting:
Hypori@carahsoft.com
703-871-8505

To purchase, check out the contract vehicles available for procurement:
carah.io/HyporiContracts