Redspin
A Division of Clearwater

NAVIGATING THE POST-CERTIFICATION LANDSCAPE

WHAT HAPPENS AFTER THE ASSESSMENT?

CUI CON, 2024

REDSPIN

POINTS OF CONTACT

Thomas Graham, Ph.D., CISSP, MBA

VICE PRESIDENT, CISO, CCA, AND CMMC PROVISIONAL INSTRUCTOR AT REDSPIN

- Chief architect of Redspin becoming the first authorized CMMC C3PAO
- Previous experience supporting the Defense Health Agency (DHA) where his team received a FedHealthIT award for innovation, Naval Commendations, and the Captain Joan Dooling Award
- Prior Information Assurance Officer (IAO) supporting DISA and MARCORSYSCOM
- Lead Assessor for Aero-Glen International (First OSC to pass Joint Surveillance) and Microsoft Federal

Thomas.graham@redspin.com

Find me on LinkedIn!

TABLE OF CONTENTS

AGENDA

PROPOSED RULE REQUIREMENTS

- Artifact Retention & Integrity
- Affirmation
- CMMC Level 3
- CMMC Status Revocation

MAINTAINING COMPLIANCE

- Training
- POA&M
- Third-Party Management

QUESTIONS

- Q&A

Redspin
A Division of Clearwater

NAVIGATING THE POST-CERTIFICATION LANDSCAPE

PROPOSED RULE REQUIREMENTS

CUI-CON 2024

§ 170.17 (4) ARTIFACT RETENTION & INTEGRITY

- (4) Artifact Retention and Integrity. The artifacts used as evidence for the assessment must
- be retained by the OSC for the duration of the validity period of the certificate of assessment, and
- at minimum, for six (6) years from the date of certification assessment.

- To ensure that the artifacts have not been altered, the OSC must hash the artifact files using a NIST-approved hashing algorithm.

- The OSC must provide the C3PAO with a list of the artifact names, the return values of the hashing algorithm, and the hashing algorithm for upload into the CMMC instantiation of eMASS.

- Additional guidance for hashing artifacts can be found in the guidance document listed in paragraph (h) of appendix A.

§ 170.22 AFFIRMATION

(a) General. The OSA must affirm continuing compliance with the appropriate level CMMC Self-Assessment or CMMC Certification Assessment. The affirmation shall be submitted in accordance with the following requirements:

1. Affirming official. All CMMC affirmations shall be submitted by the OSA senior official who is responsible for ensuring OSA compliance with CMMC Program requirements.
2. Affirmation content. Each CMMC affirmation shall include the following information: Name, title, and contact information for the affirming official; and
    i. Affirmation statement attesting that the OSA has implemented and will maintain implementation of all applicable CMMC security requirements for all information systems within the relevant CMMC Assessment Scope at the applicable CMMC Level.
3. Affirmation submission. The affirming official shall submit a CMMC affirmation in the following instances:
    i. Upon completion of the assessment (conditional or final);
    ii. Annually thereafter; and
    iii. Following a POA&M closeout assessment, as applicable.

(b) Submission procedures. All affirmations shall be completed in SPRS. The Department will verify submission of the affirmation in SPRS to ensure compliance with CMMC solicitation or contract requirements.

§ 170.18 CMMC LEVEL 3

(a) Level 3 Certification Assessment Requirements. To comply with CMMC Level 3 Certification Assessment requirements, the OSC must meet the requirements set forth in paragraphs (a)(1) and (2) of this section. Receipt of a CMMC Level 2 Final Certification Assessment for information systems within the Level 3 CMMC Assessment Scope is a prerequisite for a CMMC Level 3 Certification Assessment.

(1) Level 3 Certification Assessment. The OSC must achieve a CMMC Level 2 Final Certification Assessment on the Level 3 CMMC Assessment Scope, as defined in § 170.19(c) and complete and implement all Level 3 security requirements specified in table 1 to § 170.14(c)(4) CMMC Level 3 Requirements prior to initiating a CMMC Level 3 Certification Assessment, which will be performed by DCMA DIBCAC1 on behalf of the DoD.

To achieve and maintain CMMC Level 3 Certification Assessment, OSCs must achieve both a CMMC Level 2 Final Certification Assessment in accordance with § 170.17 and a CMMC Level 3 Final Certification Assessment in accordance with this section on a triennial basis for all information systems within the Level 3 CMMC Assessment Scope. DCMA DIBCAC will submit the assessment results into the CMMC instantiation of eMASS, which then provides automated transmission to SPRS.

§ 170.17 CMMC STATUS REVOCATION

(iv) CMMC Status Revocation. If the CMMC PMO determines that the provisions of Level 1 or Level 2 of this rule have not been achieved or maintained, as addressed in § 170.6, a revocation of the validity status of the CMMC Level 2 Final Certification Assessment may occur.

At that time, standard contractual remedies will apply and the OSC will be ineligible for additional awards with CMMC Level 2 Certification Assessment or higher requirements for the information system within the CMMC Assessment Scope until such time as a valid CMMC Level 2 Certification Assessment is achieved.

The revocation of a CMMC Level 2 Final Certification Assessment will automatically cause the revocation of any CMMC Level 3 Certification Assessments that were dependent upon that CMMC Level 2 Final Certification Assessment.

Redspin
A Division of Clearwater

NAVIGATING THE POST-CERTIFICATION LANDSCAPE

MAINTAINING COMPLIANCE

CUI-CON 2024

TRAINING

Redspin®
A Division of Clearwater

Problem
OSCs must maintain CMMC assessment certification for the three-year duration

Solution
Recommend sending personnel to the CCP course to gain a better understanding of the CMMC program

Result
Personnel have a full understanding of how to manage and maintain compliance for the duration of the certification period

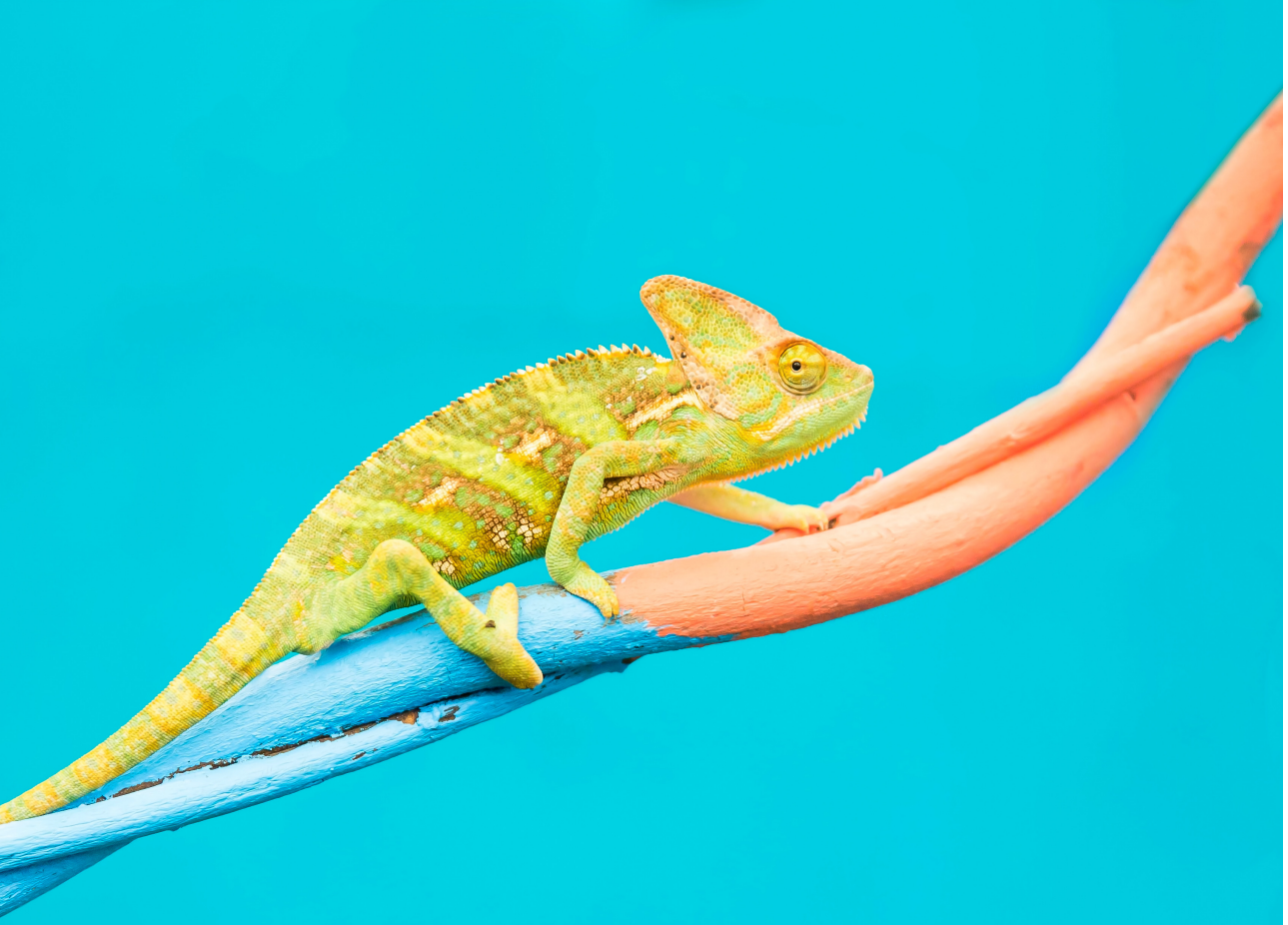
Redspin
A Division of Clearwater

POA&M

Problem
Changes to the environment will affect compliance with CMMC Level 2 during the certification period

Solution
PAO&Ms should be utilized to address changes to the environment and be closed out prior to the recertification

Result
OSCs are fully managing changes within the environment to ensure security requirements are being maintained



Redspin
A Division of Clearwater

NIST SP 800-171 REV3

Problem
NIST SP 800-171 Revision 3 will be ingested into the CMMC program sometime over the next couple of years

Solution
Review the requirements for the updated version and begin implementing those requirements

Result
By implementing changes now, the OSC will be better postured for recertification

We are here to help.

Moving federal contractors to a more secure, compliant, and resilient state in order to better validate the security of the federal supply chain.

Redspin®

A Division of Clearwater

www.Redspin.com

CMMC Resources >

888.907.3335

info@Redspin.com

LinkedIn.com/company/redspin-inc

Redspin®
A Division of Clearwater

Legal Disclaimer

Although the information provided by Redspin, a division of Clearwater may be helpful in informing customers & others who have an interest in data privacy & security issues, it does not constitute legal advice. This information may be based in part on current federal law & is subject to change based on changes in federal law or subsequent interpretative guidance. Where this information is based on federal law, it must be modified to reflect state law where that state law is more stringent than the federal law or other state law exceptions apply. This information is intended to be a general information resource & should not be relied upon as a substitute for competent legal advice specific to your circumstances. YOU SHOULD EVALUATE ALL INFORMATION, OPINIONS & RECOMMENDATIONS PROVIDED BY REDSPIN, A DIVISION OF CLEARWATER IN CONSULTATION WITH YOUR LEGAL OR OTHER ADVISOR, AS APPROPRIATE.

Copyright Notice

*The existence of a link or organizational reference in any of the following materials should not be assumed as an endorsement by Clearwater Compliance LLC.