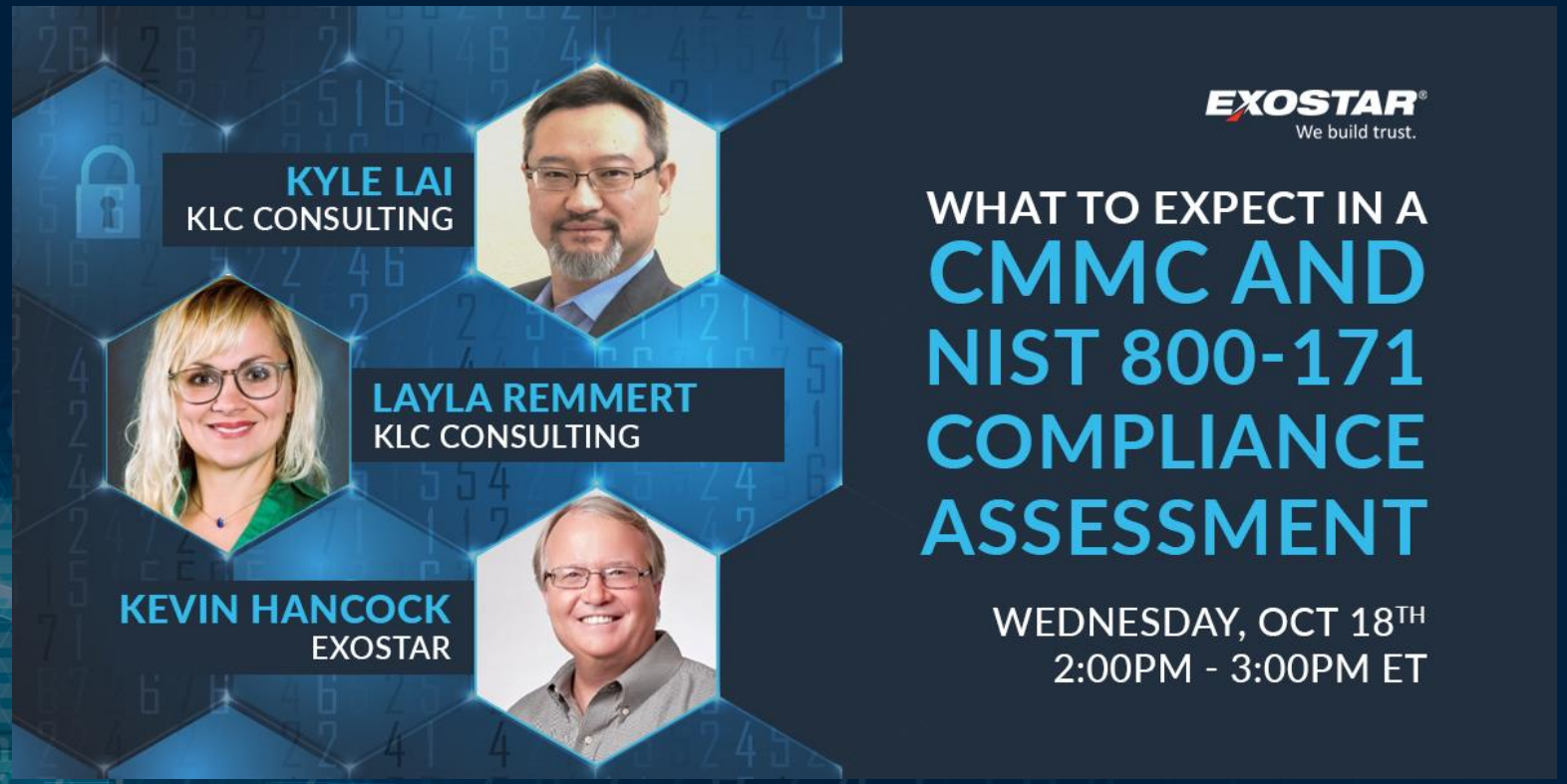
EXOSTAR®
We build trust.



October 19, 2023

Housekeeping

- Today's webinar is scheduled to last 45 minutes to one hour, including Q&A.
- All participants will be muted to enable the speakers to present without interruption.
- A portion of today's event is dedicated to answering pressing questions from the audience. Speakers will be answering questions that have been submitted prior to today's event.
- In case of outage, please wait for a minute and refresh the page.
- For your convenience, there is a link in the YouTube description to a glossary of commonly used terms, acronyms and initializations that will be referenced during today's webinar.
- This webinar is being recorded and will be available on-demand via the Exostar Resource Library (www.Exostar.com/Resources) post-event, as well as at this same YouTube link.
- To speak with one of our industry experts or request a copy of this slide deck, please reach out to us at cmmc-team@Exostar.com or use the live chat feature at www.Exostar.com.

Agenda

EXOSTAR®
We build trust.

Purpose

Understand your obligations under current DFARS Clauses, how to ensure your compliance with these clauses, mitigate risks, ensure investments are maintained when CMMC Rulemaking takes effect.

- **Housekeeping**
- **Introductions**
- **NIST SP 800-171/CMMC Update**
- **Mock Assessment**
- **Joint Surveillance Voluntary Assessment**
- **Question and Answer**

Speakers

Kyle Lai is the President and CISO at KLC Consulting, a U.S. Dept. of Defense (DoD) authorized CMMC Third-Party Assessment Organization (C3PAO), which provides advisory, conducts assessments, and enhances the cybersecurity of the Defense industry supply chain. Kyle also serves on the board of the C3PAO Forum. With over 25 years of cybersecurity expertise, Kyle has served as an advisor to renowned organizations such as ExxonMobil, Zoom, DISA (U.S. DoD), Boeing, HP, and Microsoft. His qualifications include CMMC Certified Professional (CCP) and Certified Assessor (CCA) certifications and CISSP, CSSLP, CISA, CIPP/US/G, and ISO 27001 Lead Auditor credentials.

Layla Remmerrt leads the delivery of KLC Consulting's cybersecurity & compliance services for our U.S. Defense Industrial Base clients. She developed top-shelf expertise over 16 years of progressive experience, including five years with Booz Allen Hamilton as the team lead of 17 assessors. Her subject matter expertise, collaborative spirit, and superior communication skills make her a highly sought-after cyber DFARS compliance expert. Layla's qualifications include Certified CMMC Assessor (CCA), Certified CMMC Professional (CCP), PMP, and CASP.

Copyright 2023 Exostar LLC | All Rights Reserved

EXOSTAR®
We build trust.

CMMC Update

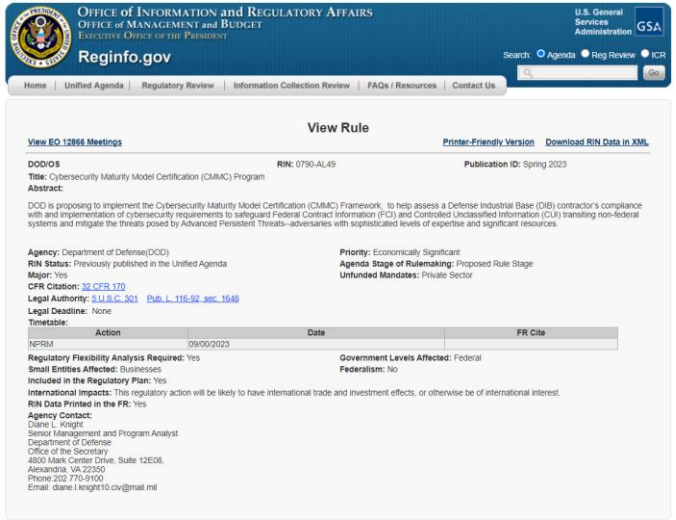
Latest CMMC Timeline

DOD Submits CMMC Rule to OIRA July 24, 2023

OIRA Review ~ 60 business days

Notice of Proposed Rulemaking (NPRM) ~ 280 Businsse Days

Rule is published in the Federal Registry



Office of Information and Regulatory Affairs
Office of Management and Budget
Executive Office of the President

U.S. General Services Administration

Reginfo.gov

Search: Agenda Reg Review ICR

Home | Unified Agenda | Regulatory Review | Information Collection Review | FAQs / Resources | Contact Us

View Rule

View EO 12866 Meetings | Printer-Friendly Version | Download RIN Data in XML

DOD/OS | RIN: 0790-AL49 | Publication ID: Spring 2023

Title: Cybersecurity Maturity Model Certification (CMMC) Program

Abstract:

DOD is proposing to implement the Cybersecurity Maturity Model Certification (CMMC) Framework, to help assess a Defense Industrial Base (DIB) contractor's compliance with and implementation of cybersecurity requirements to safeguard Federal Contract Information (FCI) and Controlled Unclassified Information (CUI) transiting non-federal systems and mitigate the threats posed by Advanced Persistent Threats--adversaries with sophisticated levels of expertise and significant resources.

Agency: Department of Defense(DOD)
RIN Status: Previously published in the Unified Agenda
Major: Yes
CFR Citation: 32 CFR 170
Legal Authority: 5 U.S.C. 301 | Pub. L. 116-92, sec. 1648
Legal Deadline: None
Priority: Economically Significant
Agenda Stage of Rulemaking: Proposed Rule Stage
Unfunded Mandates: Private Sector

Timetable:

Action	Date	FR Cite
NPRM	09/00/2023	

Regulatory Flexibility Analysis Required: Yes
Small Entities Affected: Businesses
Included in the Regulatory Plan: Yes
Government Levels Affected: Federal
Federalism: No
International Impacts: This regulatory action will be likely to have international trade and investment effects, or otherwise be of international interest.
RIN Data Printed in the FR: Yes

Agency Contact:
Diane L. Knight
Senior Management and Program Analyst
Department of Defense
Office of the Secretary
4800 Mark Center Drive, Suite 12E08,
Alexandria, VA 22350
Phone:202 770-9100
Email: diane.l.knight10.civ@mail.mil

Can also be issued as an INTERIM FINAL RULE

Copyright 2023 Exostar LLC | All Rights Reserved

SPRS Revision

EXOSTAR®
We build trust.

Pentagon finalizes rulemaking directing contracting officers to consider supplier risk during evaluation process

By **Sara Friedman** / March 23, 2023

Tweet

. . .

"The objective of the final rule is to notify offerors, via the new solicitation provision at DFARS 252.204-7024, that SPRS collects performance data from a variety of Government sources on awarded contracts to develop item risk, price risk, and supplier risk assessments for contracting officers to consider during evaluation of quotations or offers. The final rule also requires contracting officers to consider the supplier risk assessment in the determination of contractor responsibility," according to the notice.

https://insidecybersecurity.com/share/14469#main-content

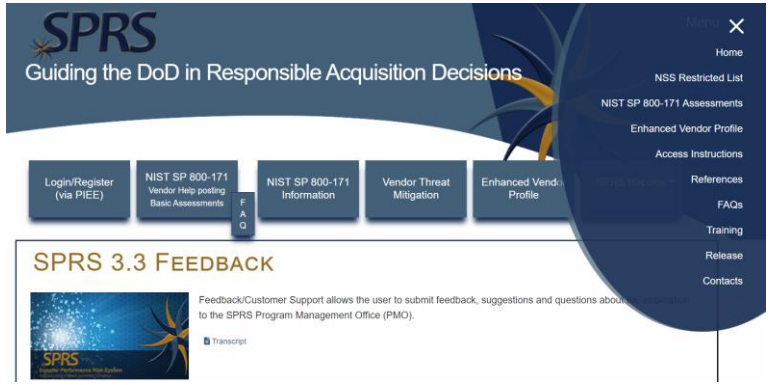
Copyright 2023 Exostar LLC | All Rights Reserved

What needs to be done today

EXOSTAR®
We build trust.

YES

7019



Check your contracts
DFARS Clauses

- **252.204-7012**
- **252.204-7019**
- **252.204-7020**

NIST 800-171/171a Compliance

If you're not abiding the regulation and/or reporting inaccurate scores, you are in violation of the False Claims Act

DFARS 7019 requires a self-assessment and accurate reporting of your Supplier Performance Risk System (SPRS) score

EXOSTAR®
We build trust.

CMMC Joint Surveillance Voluntary Assessment (JSVA) and Mock Assessment

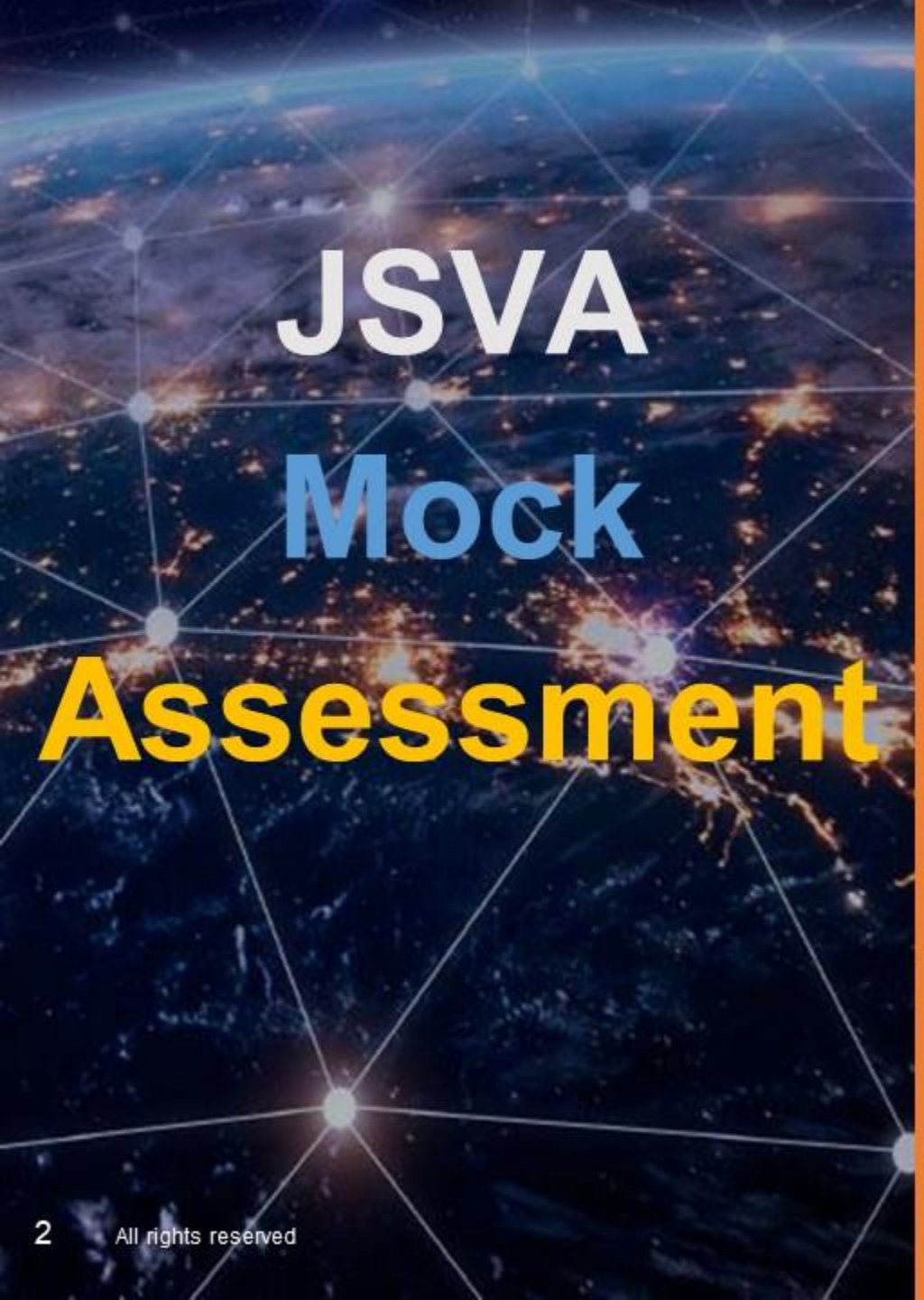
by KLC Consulting, Inc.

October 18 2023

All rights reserved

EXOSTAR® We build trust.

KLC CONSULTING A C3PAO COMPANY



Agenda

- About KLC
- CMMC Join Surveillance Volunteer Assessment (JSVA)
- Mock Assessment
- Q&A

KLC CONSULTING
A C3PAO COMPANY

All rights reserved

Acronyms

- **C3PAO** – Certified Third Party Assessment Organization
- **CAP** – CMMC Assessment Process
- **CCE** – Cage Code Entity
- **CI** – Configuration Item
- **CRM** – Customer Responsibility Matrix
- **CUI –** Controlled Unclassified Information
- **DFARS** – Defense Federal Acquisition Regulations Supplement
- **DIBCAC** – Defense Industrial Base Cybersecurity Assessment Center
- **DoD** – Department of Defense
- **eMASS** – Enterprise Mission Assurance Support Service
- **JSVA** – Joint Surveillance Voluntary Assessment
- **NIST** – National Institute of Standards and Technology
- **ODP** – Organizationally Defined Parameter
- **OSC** – Organization Seeking Certification
- **POAM** – Plan of Action and Milestones
- **SLA** – Service Level Agreement
- **SPRS** – Supplier Performance Risk System
- **SSP** – System Security Plan

KLC CONSULTING
A C3PAO COMPANY

Email Us Your Feedback & CMMC Journey

Email to: cmmc@klcconsulting.net

Feedback:

1. Where you are on your CMMC Journey
2. What is the most challenging part of the CMMC Compliance
3. Your feedback on our presentation

KLC CONSULTING
A C3PAO COMPANY

About KLC Consulting

- KLC Consulting is an authorized CMMC Third-Party Assessment Organization (C3PAO).
- We specialize in DFARs and CMMC compliance
- We distinguish ourselves with a spirit of advocacy with our clients; we foster a relationship of empathy for CMMC compliance because we've been there ourselves.
- Our clients range from Fortune 500 companies to small and medium-sized organizations; we meet them where they are.

All Rights Reserved

KLC CONSULTING
A C3PAO COMPANY

Presenters

Kyle Lai

President and CISO of KLC Consulting
CISSP, CSSLP, CISA, CDPSE,
CIPP/US/G, CMMC-CCA, CMMC-CCP

https://www.linkedin.com/in/kylelai

Klai@klcconsulting.net

Layla Remmert

Director of Cybersecurity Services
CASP, PMP, CMMC-CCA, CMMC-CCP

https://www.linkedin.com/in/layla-remmert-836ab431/

Lremmert@klcconsulting.net

- Former DISA (DoD) Operations Manager
- Former CISO of Pactera & Brandeis University – Heller School
- Former Penetration Tester for Fortune 500 firms
- Author of SMAC MAC Address Changer – Over 3 million users
- Run 3 LinkedIn Groups (including Cybersecurity C25+ years in IT and 20 years in Cybersecurity (Pentest, Third-party Risk, Compliance, Privacy, Engineering...)
- Security Advisor to Fortune 500 companies
- Experience with Software, DoD, Financial, Energy, Healthcare, High Tech, Consulting industries
- Security advisory for Microsoft, Boeing, Fidelity Investment, Akamai, ExxonMobil, DISA, Zoom
- SME on CMMC, NIST 800-171, NIST 800-53, DoD RMF

- Held cybersecurity positions as ISSO, ISSE, ISSM, and SCA rep over breadth of 16+ progressive years in the field
- Experiened Project and Progam Manager for both large and small cybersecurity teams
- Experienced in providing technical direction of varied staff members in quality assurance, communications, and process improvement w
- Have been working collaboratively in the CMMC advisory and assessment space since January 2021; integral part of a DIBCAC audit team that resulted in C3PAO certification in July 2022
- Proven leadership in varying environment
- Excellent written and oral communication skills and research/writing/editing processes

All Rights Reserved

The Joint Surveillance Volunteer Assessment Program

- JSVA is a pilot program for CMMC that is being executed before CMMC is formally adjudicated.
- A CMMC C3PAO assessment team is paired with a Defense Industrial Base Cybersecurity Assessment Center (DIBCAC) assessment team to conduct a CMMC assessment.
- **The Department of Defense indicated that a JSVA translates into a CMMC Level 2 certification issued by the participating C3PAO upon the CMMC final rulemaking** (currently appears to be early 2025)
- The 3-year recertification clock would then start at the time of rulemaking, not shortening the time of the assessment but essentially lengthening it

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

Which OSCs should do JSVA?

- OSCs with contracts with Defense Federal Acquisition Regulation Supplement (DFARS) clauses 252.204-7012 are coming up for renewal/recompete in 2024/2025.
- OSCs who already have a CMMC or 800-171 SSP that meets all of the NIST 800-171 security requirements
- OSCs who have already submitted their overall compliance score into the SPRS
- OSCs that want a competitive edge in CMMC and have the certification immediately upon rulemaking being finalized (according to DoD).
- Those who want to beat the expected rush to schedule an engagement with a C3PAO once rulemaking is complete.
- OCS who have already had a C3PAO verify their assessment readiness

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

The JSVA Preparation Process

Does my company qualify?

- You must be in an active DoD contract to be considered (can be a subcontractor)

How to get the JSVA started:

- You select an authorized C3PAO you wish to perform your JSVA
- C3PAO will submit your JSVA request to CyberAB.
- Once accepted, the DIBCAC will contact you (the OSC) and add you to the JSVA queue

Preparation:

- Your C3PAO assessment team is paired with DIBCAC to conduct a CMMC assessment “Jointly”
- C3PAO will meet with you to verify the CUI scope and boundary and create an assessment plan
- C3PAO & DIBCAC will ask for supporting evidence/artifacts
- DIBCAC will ask about DFARS 7012 requirements: Incident Reporting, Flow down

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

JSVA Duration & Expectation

- JSVA typically last for 5 full business days, which includes the following activities:
  - In brief, introductions and review of the OSC System Security Plan (SSP)
  - Interviews and Tests for all applicable practices and assessment objectives of the CMMC Maturity Level 2
  - Any physical onsite inspections and tests
  - Examination of all required documentation
  - Out brief
- Although the duration of any specific JSVA can depend on many factors, all parties should plan on participation of all 5 days.

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

JSVA Location: Onsite or Remote?

- Does OSC's physical office(s) store, process, or transmit CUI? **Yes = Onsite**
- If onsite, **15 CMMC practices must be observed by the C3PAO & DIBCAC Assessment Team in person and on the premises of the OSC**
- OSCs should plan for at least ONE DAY of the assessment to be held in-person/onsite
- **JSVA location**: agreement by all three parties – OSC, C3PAO, and the DIBCAC teams
- JSVA can be held at more than one location based on the OSC's facilities, scope, and boundaries
- The location of the JSVA will be specified in the overall Assessment Plan

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

What Artifacts do I Provide to C3PAO and DIBCAC?

At a minimum, the following Evidential artifacts are required to be **Available** and **Accessible prior** to the start of the assessment (lead time may vary depending on your C3PAO/DIBCAC teams):

- SSP
- Data Flow Diagram (DFD) that depicts CUI Boundary
- Asset Categorization diagram
- Policies and Plans for each of the 14 Security Domains approved by the OSC's Senior Stakeholder(s)
- All applicable documented procedures and processes referenced in SSP and Policy
- Configuration Items (CIs) and Organizational Defined Parameters (ODPs)
- Customer Responsibility Matrix (CRM) for all inherited practices from Cloud or Managed service providers
- Service Level Agreements (SLAs) for any vendors providing CUI services

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

JSVA C3PAO Pricing

- JSVAs are essentially certification assessments, so the C3PAO charges OSCs the same price for a JSVA as they would for the formal CMMC certification assessment
- JSVA pricing factors:
  - Size of the organization (# of endpoints and employees)
  - System Complexity (# of in-scope systems, applications, and users)
  - Number of locations within scope and travel for the onsite portion of the assessment
  - On-prem and cloud-based architecture and security solutions
  - Number of Cage Code Entities in scope
- Note: OSCs do NOT pay for the DIBCAC involvement

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

JSVA Results

When Will I Know I Passed?

- Typically, OSCs will be notified within a week of the assessment completion

What Happens if I Don't Pass?

- Per CAP, If you achieve the minimum score of 88, and deficiencies are allowed for POA&M Close-Out Assessment
  - Arrange a delta-assessment with C3PAO / DIBCAC team

- If an OSC is not adequately prepared, DIBCAC may cancel the JSVA
  - The OSC may wait until the CMMC adjudication to re-attempt the CMMC Assessment

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

Why do a Mock Assessment First?

- Informal assessment that evaluates all your CMMC practices (as if it were a real assessment).
- Detailed findings that describe weaknesses of your organization's processes relative to the desired NIST 800-171 requirement.
- Indication of whether the evaluated practices would be rated as “Met” in a formal assessment.
- A practice test conducted exactly like a formal CMMC Certification assessment; only results aren’t reported.
- Mock assessments are NOT an advisory service but an unofficial, comprehensive assessment that mirrors the CMMC Assessment.
- Help you predetermine the likely outcome and your team’s readiness during an official CMMC Assessment.

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

How is a Mock Assessment Different from a JSVA?

While a Mock Assessment mirrors a JSVA, there are some key differences:

- The Mock Assessment is informal, meaning a Fail does not "count against you." It does not preclude them from moving forward with a JSVA in any prescribed time frame
- Typically, Mock Assessments do not involve onsite requirements and do not strictly follow the 5-business day schedule; scheduling is based on the OSC's availability
- The DIBCAC is not involved in this process
- While the Mock Assessment follows the CAP, no documents are uploaded to DoD
- An OSC can take as much time as needed (before rulemaking) to remediate gaps and then schedule the JSVA when ready

All rights reserved

Is Using the same C3PAO a Conflict of Interest?

- Mock Assessments that do **NOT** include Recommendations or remediation guidance allow the same C3PAO to perform a JSVA. No conflict of interest.
- A Mock Assessment will take place before a certification or JSVA so that the OSC can remediate the gaps before the formal JSVA (either internally or using an RPO).
- Once the gaps identified in the Mock Assessment have been closed or remediated, the OSC may come back to the C3PAO to schedule the JSVA.
- Using the same C3PAO for a mock and JSVA assessment saves time and money because the C3PAO is already familiar with your environment.

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

Benefit of Mock Assessments

- Mock Assessment is a perfect preparation for JSVA
- You have the same C3PAO that is familiar with your environment to perform the JSVA
- C3PAOs may offer discounts if doing both Mock Assessment and JSVA

All rights reserved

KLC CONSULTING
A C3PAO COMPANY

Contact Information

KLC CONSULTING

A C3PAO COMPANY

KLC Consulting, Inc.

cmmc@KLCConsulting.net

https://www.Linkedin.com/in/kylelai

KLC Consulting Youtube Channel on CMMC

www.klcconsulting.net

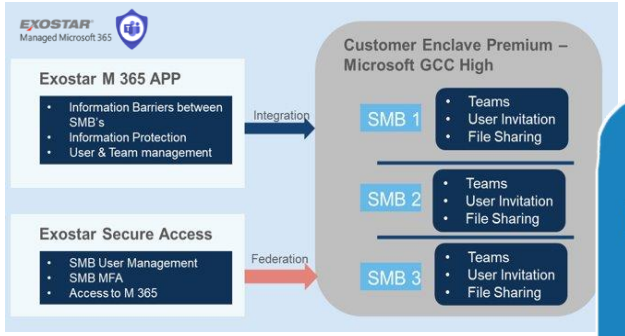
EXOSTAR®
We build trust.

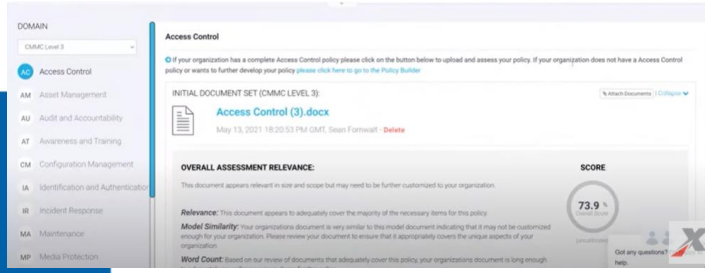
Exit Poll

See link in YouTube description

Exostar solutions

EXOSTAR®
We build trust.





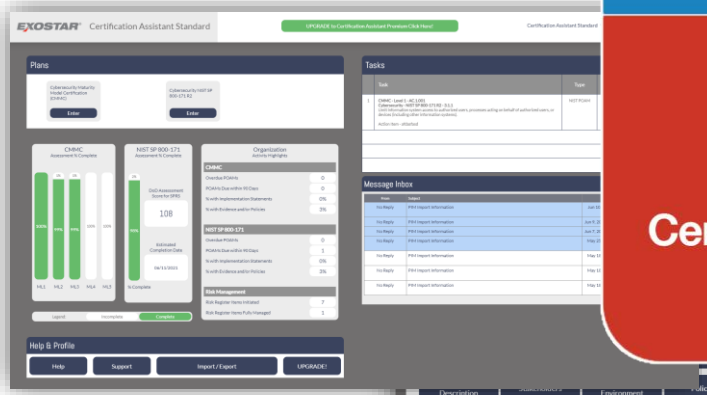
Managed Microsoft 365

PolicyPro

Exostar CMMC Ready Suite

Certification Assistant

NIST 800-171 / CMMC Basic Assessment



CMMC Partners

Our CMMC partners help Exostar to empower organizations to assess, measure, and mitigate risk across multi-tier partner and supplier networks.

KLC CONSULTING CYBERSECURITY · PivotPoint SECURITY · SysArc · Technical Support · T E S CONSULTANTS

Questions

EXOSTAR®
We build trust.

1. We have stood up a GCC High carve out for compliance. How should we handle any historical (unknown?) CUI that live in our out of scope commercial cloud? Doe this need to be discovered and cleaned?
2. Is a SIEM tool an absolute requirement for CMMC? The recurring costs of SIEM and SOC are simply too much. Please share the facts.
3. How is the process likely to work regarding multinational organisations?
4. Are there companies out there currently providing Readiness assessments? Can we use the same company that does our readiness assessment as our C3PAO (given they are a certified C3PAO)?
5. STIGS are not required, I see nothing in the documentation, yet this topic seems to be trending (at least in the Colo Springs area). Can you confirm STIG is not a CMMC 2.0 (level 2) item?

EXOSTAR®
We build trust.

Q&A

Useful sources of information

- Learn more about CUI at https://www.dodcui.mil/
- CMMC Accreditation Body website https://cyberab.org/
- DoD Procurement Reference website https://dodprocurementtoolbox.com/
- DoD CMMC Acquisition website https://www.acq.osd.mil/cmmc/index.html

Summary of the SPRS process with links to authoritative PIEE and SPRS materials hosted by DoD
https://www.exostar.com/blog/nist-800-171-basic-assessment-reporting-easy-as-1-2-3/

- Exostar Partner Listing https://www.exostar.com/partners/ (Note—Select CMMC)

Free Trial Information:

- Exostar Certification Assistant https://www.exostar.com/product/certification-assistant/
- Exostar PolicyPro https://www.exostar.com/product/policypro/

Questions

EXOSTAR®
We build trust.

6. We are a small business using 2 computers. One for email and internet, the other for all company business and not at all on line. What else might we need to do?
7. Is CMMC applicable to organizations that have their data center in the cloud.?
8. Are classification or retention policies required? Are annual pentests required? What are FIPS140-2 validated solutions?
9. Can a company plan for the assessors to visit company locations where CUI is processed and products are developed or is the focus on the data center(s) where CUI is digitally stored?
10. How does one submit a score to SPRS when do you not have a WWWF account?

EXOSTAR®
We build trust.

Exit Poll Reminder

See link in YouTube description

EXOSTAR®
We build trust.

Thank you for joining us

cmmc-team@exostar.com

EXOSTAR®

We build trust.