Defense Industrial Base (DIB) CMMC Requirements Impact on Back-Office Information Systems

A Case Study in Sales & BD CUI Data Protection

CAPTURE 2 PROPOSAL®

SUMMIT7

SERABRYNN®

Introductions

Chris Flook
Moderator
CAPTURE 2 PROPOSAL

Mark Edwards
ISSO
CAPTURE 2 PROPOSAL

Sam Morthland
CFO
SERABRYNN®

Scott Edwards
CEO/President
SUMMIT7

Alexy Johnson
Senior Cyber Security Analyst
SERABRYNN®

DISCUSSION TOPICS

- **(1) How does CMMC impact DIB contractors use of back-office systems?**
  - What constitutes back-office systems (Saas, IaaS)
  - CUI boundaries with respect to back-office systems
  - DFARS 252.204.7012 Applicability
    - (b)(2)(i) NIST SP 800-171 Revision 2
    - (b)(2)(ii)(D) cloud service provider (CSP) compliance with FedRAMP Moderate
    - (c) through (g)

- **(2) How is CMMC compliance achieved for back-office systems?**
  - CMMC Level 2 compliance requirements within CUI boundaries
  - CSP FedRAMP Moderate, CMMC Level 2, DFARS 7012
  - Body Of Evidence (BOE) to support DIB CMMC assessments

Poll #1

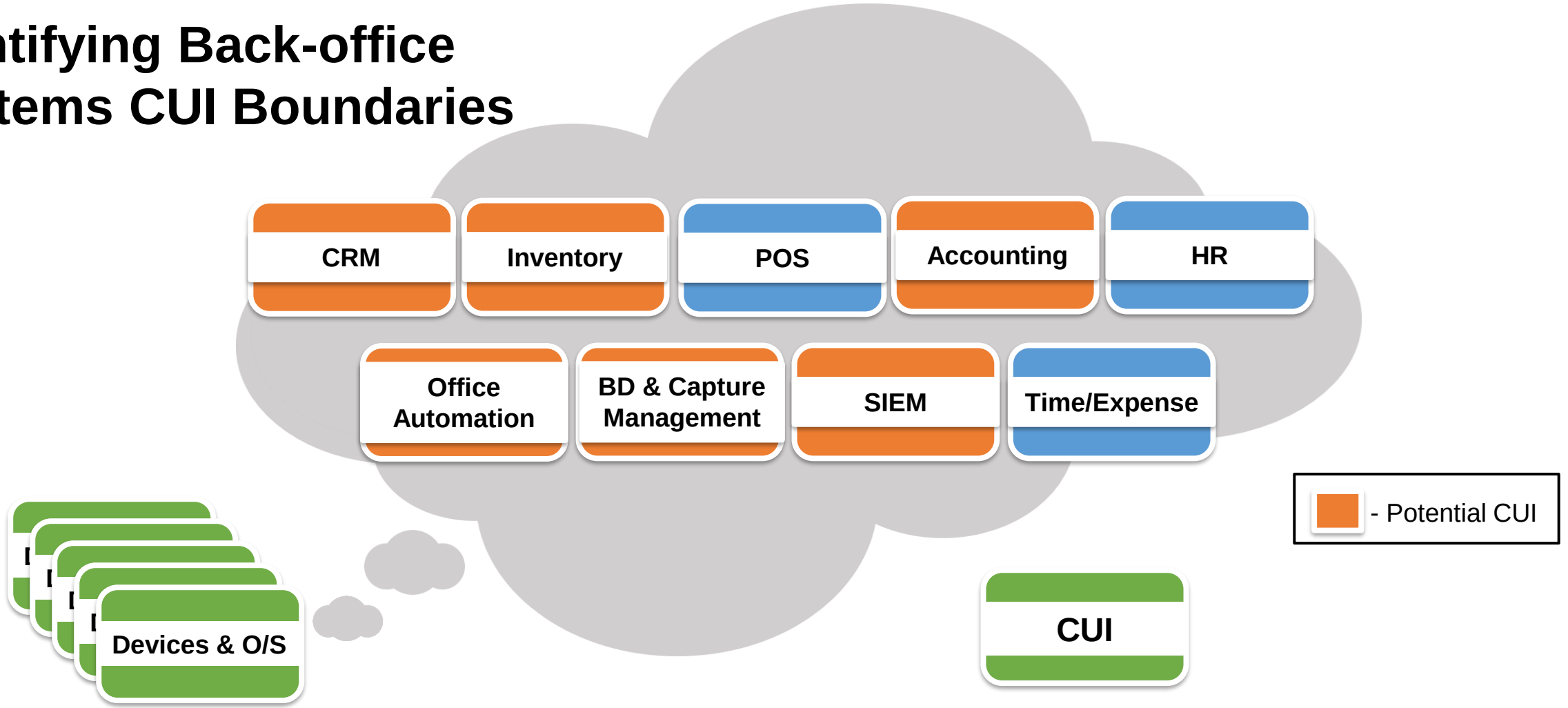
Is your company currently preparing for a CMMC Level 2 Assessment?

a. Yes, self-assessment
b. Yes, C3PAO assessment
c. Unsure
d. No

CMMC Model 2.0 - Summary

CAPTURE 2 PROPOSAL®
GovCon's Market Intelligence & Pursuit Platform

Identifying Back-office Systems CUI Boundaries



Identifying Back-office Systems (SaaS)

Back-office systems comprise the software that an organization uses to administer operations that are not related to any direct sales effort (such as a salesperson with a customer present) and interfaces that are not seen by consumers.

- Devices and Operating Systems
- Office Automation (document management, reporting, email, backup, remote conferencing, etc.)
- Security Information and Event Management (SIEM)
- Customer Relationship Management (CRM)
- Inventory Control, Point Of Sale (POS) Management, Accounting, Human Capital Management (HCM)
- **Business Development, Capture and Proposal Management**

Back-Office Systems Compliance - CSP Examples

- **Office 365 Commercial on Azure Commercial**
  - Not DFARS 7012 Compliant
  - Not ITAR Ready
  - Non-US Person Support
  - FedRAMP High
- **Office 365 GCC on Azure Commercial**
  - DFARS 7012 Compliant
  - Not ITAR Ready
  - Non-US Person Support
  - FedRAMP High
- **Office 365 GCC High** on **Azure Government**
  - DFARS 7012 Compliant
  - ITAR Ready
  - FedRAMP High
  - US-only personnel
- **Google G-Suite**
  - Not DFARS Compliant
  - Not ITAR Ready
  - Non-US Person Support
  - FedRAMP High
- **AWS GovCloud**
  - DFARS 7012 Compliant
  - ITAR Ready
  - FedRAMP High
  - US-Only Personnel
- **Oracle Cloud Infrastructure – Gov Cloud**
  - Not clear on DFARS 7012 Compliance
  - Not ITAR Ready
  - FedRAMP High

Poll #2

Does your company store CUI data in your external SaaS/IaaS cloud service provider (CSP) application(s)/environment?

a. Yes
b. No
c. Unsure
d. Not Applicable

DFARS 252.204.7012: Safeguarding Covered Defense Information and Cyber Incident Reporting

- **(b)(2)** . . contractor information systems **that *are not part of an IT service or system operated on behalf of the Government*** and . . not subject to . . paragraph (b)(1)
- **(b)(2)(i)** the covered contractor information system shall be subject to *the security requirements in* ***NIST SP 800-171 in effect at the time the solicitation*** is issued
- **(b)(2)(ii)(D)** If the Contractor intends to use ***an external CSP*** to store, process, or transmit any covered defense information ***in performance of this contract***, the Contractor shall require and **ensure that the CSP meets security requirements equivalent to *FedRAMP Moderate* and that the CSP complies with requirements in *paragraphs (c) through (g)*** of this clause for cyber incident reporting, malicious software, media preservation and protection . .
- ***(c) – (g)*** Incident reporting, malicious software, media preservation/protection, forensic analysis, and incident damage assessment

DIB Contractor CMMC Requirements

- **CMMC v2.0 Level 2** (Advanced, inclusive of Level 1)
  - "***Level 2 is equivalent*** *to all of the security requirement in* ***NIST SP 800-171*** *Revision 2*" (ref: CMMC v2.0 Model Overview)
  - 110 controls in 14 families that align with CMMC Level 2 domains
  - Triennial C3PAO assessments for critical national security information (CUI, prioritized acquisitions)
  - Annual self-assessment for select programs (CUI, non-prioritized acquisitions)
- A **CSP that meets FedRAMP Moderate**, as specified in DFARS 252.142.7012 (b)(2)(ii)(D), is required if using to store CUI data
  - 325 NIST 800-53 controls
  - And (c) through (g)
- **Export Control (ITAR, EAR, NOFORN) may be a consideration**
  - Only US persons supporting CSP, such as Azure Government and Capture2Proposal

DIB Contractor CMMC impact on back-office systems

- DIB contractor back-office systems handling CUI
  - Must meet CMMC Level 2 (NIST 800-171 rev 2)
  - If CSP, must meet requirements for FedRAMP Moderate
    - DFARS 7012: ". . the Contractor shall require and ensure that the CSP meets security requirements equivalent to *FedRAMP Moderate . .*"
  - DFARS 7012 (c) through (g)

- Compliance artifacts to support DIB CMMC C3PAO assessments

Poll #3

How would you describe your company's level of CMMC preparation?

a. Nothing (waiting on final CMMC publication)
b. Have started compliance efforts
c. NIST 800-171 compliant
d. Unsure

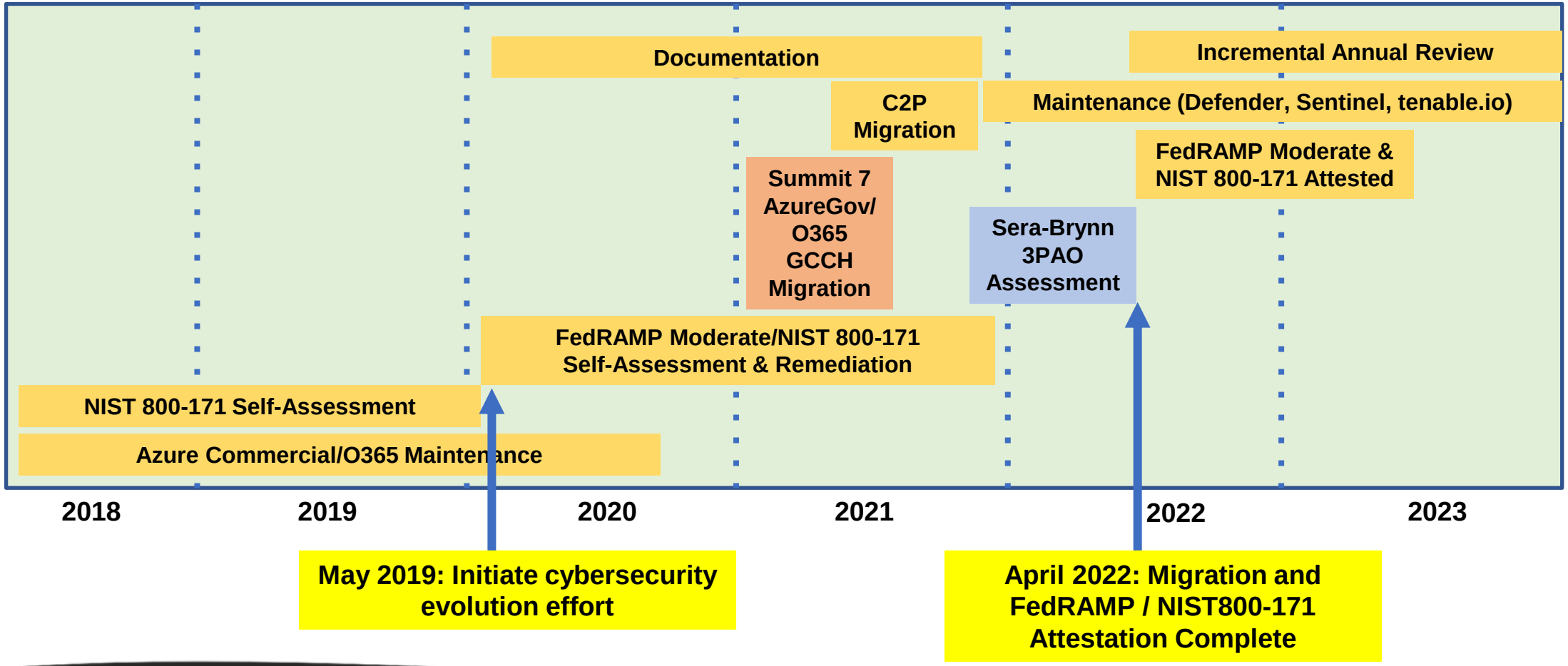
Background/Case Study – Capture2Proposal

- **Summit 7** migrated corporate and application resources to Azure Government and O365 GCC High

- **Capture2Proposal** efforts: configure, document, and maintain resources as required by FedRAMP Moderate and NIST 800-171 controls (ISP, SSP, CONOPS, POA&M)
  - All customer documents are FIPS 140-2 encrypted in transmission and storage
  - MFA authentication and Role-Based Access to customer features

- 3PAO **Sera-Brynn** performed FedRAMP Moderate and NIST 800-171 assessment and penetration test

Capture2/Capture2Proposal Cybersecurity Evolution



CMMC Ready

Based on DoD FAQ and requirement for Body of Evidence

- Compliance Summary Letter
- Letter of Attestation (FedRAMP Moderate)
- Letter of Attestation (NIST 800-171)
- Control Implementation Summary (CIS) and Customer Responsibility Matrix (CRM)
- CSP Shared-Responsibility Matrices (FedRAMP and NIST)

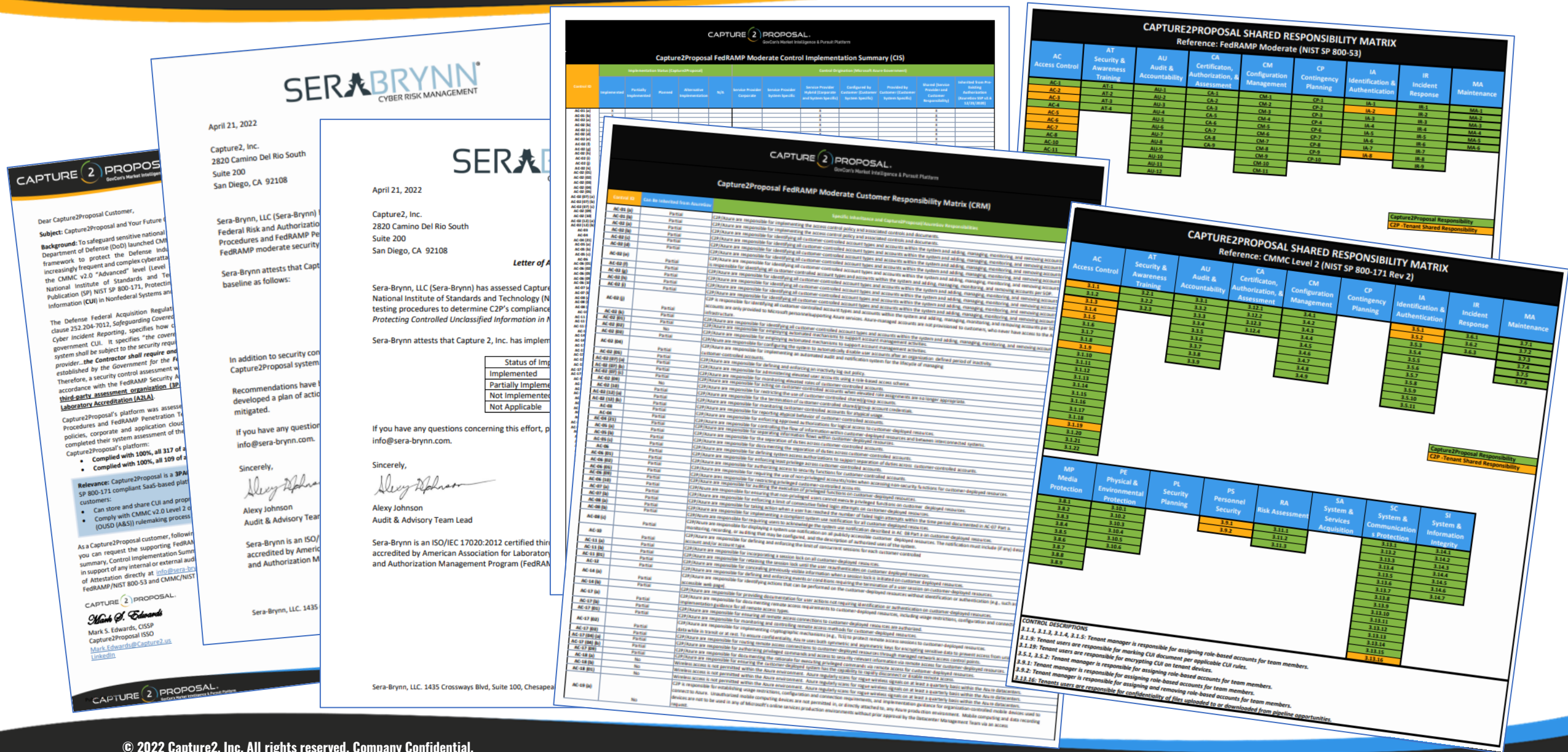
Poll #4

Does your back-office CSP provide you with body of evidence (BOE) to support your DFARS/CMMC compliance artifacts?

a. Yes
b. No
c. Unsure

Body of Evidence – Visual Examples

CAPTURE 2 PROPOSAL®
GovCon's Market Intelligence & Pursuit Platform



Recommendations

- DIB companies examine portfolio of CSP applications used to determine what is needed to demonstrate compliance to DFARS
- CSP providers (IaaS, PaaS, CaaS, SaaS) need to examine potential requirement for FedRAMP Moderate Baseline assessment and resulting Body of Evidence to provide to clients
- The clock is ticking…**Take Action Now**…CMMC expected to be here in May 2023, some DIB Prime Contractors asking for assessment results now

Questions?

Additional Resources

- DFARS 252.204.7012
- NIST 800-171
- NIST 800-53
- FedRAMP Moderate Resources

CAPTURE 2 PROPOSAL®

sales@capture2.com

SUMMIT7

cmmc@summit7.us

SERA BRYNN®

info@Sera-Brynn.com