Supplier Cybersecurity Readiness Webinar

Cybersecurity Webinar: Complying with DFARS 252.204-7020 (NIST Assessment) and Preparing for CMMC – Delta Practices & Assessment Prep

May 25 2021

LOCKHEED MARTIN

Disclaimer

- Webinar content is based on:
  - Office of Under Secretary of Defense (OUSD) CMMC publications
  - National Institute of Standards & Technologies (NIST) publications
  - Carnegie Mellon University (CMU) Software Engineering Institute (SEI) Computer Emergency Response Team (CERT) publications
  - Defense Industrial Base Sector Coordinating Council (DIB SCC) Supply Chain Task Force – CyberAssist

- This webinar will not address technical implementations, configurations, or specific pass/fail criteria questions for Organizations Seeking Certification (OSC)

- Lockheed Martin does not take responsibility for suppliers’ certification by the CMMC 3rd Party Assessment Organization (C3PAO)

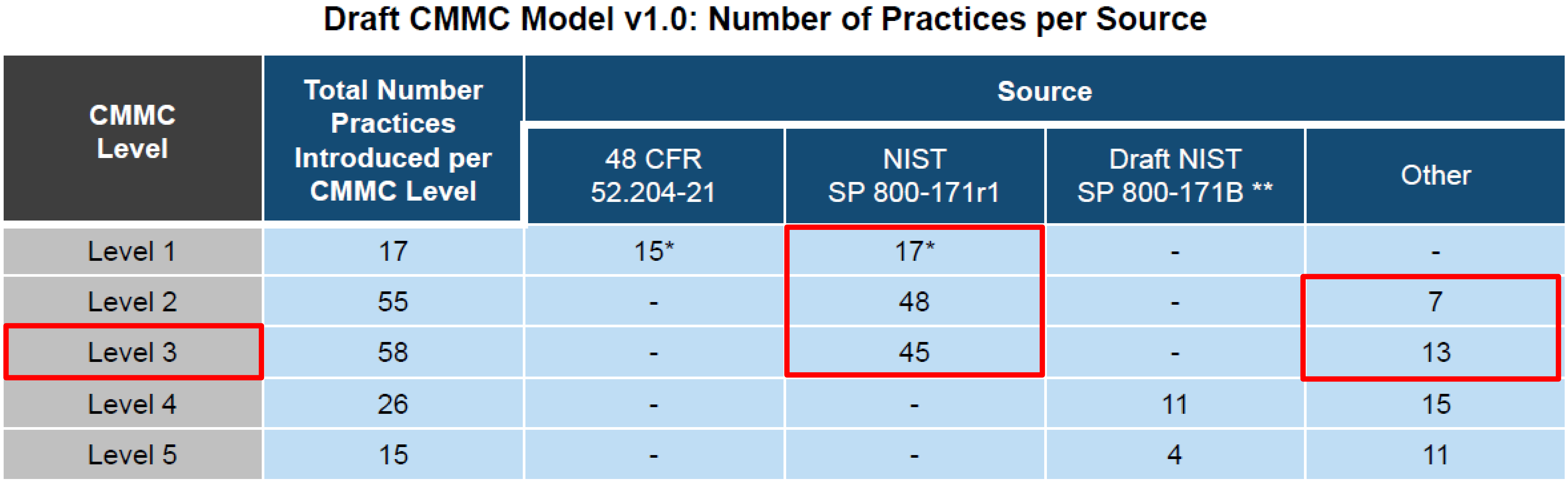
Learning Objectives

- CMMC Level 3 – NIST 800-171 plus
- Preparing for CMMC assessment: Lessons Learned from Mock Assessments & Training
  - Follow the Data
  - Get To Know: Assessment Guide/Practices/Assessment Objectives
    - Essential Artifacts
    - Evidences
    - Inter-Connected Practices
- Explain Lockheed Martin’s expectation for CMMC deployment

Level 3 Background and Delta 20

Model leverages multiple sources and references

- CMMC Level 3 includes all of the Level 1 – Level 3 practices from NIST SP 800-171 as well as others



Draft CMMC Model v1.0: Number of Practices per Source

CMMC Level	Total Number Practices Introduced per CMMC Level	Source			
		48 CFR 52.204-21	NIST SP 800-171r1	Draft NIST SP 800-171B **	Other
Level 1	17	15*	17*	-	-
Level 2	55	-	48	-	7
Level 3	58	-	45	-	13
Level 4	26	-	-	11	15
Level 5	15	-	-	4	11

What are the Delta 20 practices?

- The CMMC Practices and their Source Mapping can be found in Appendix E of the CMMC Appendices V1.02
  - The Practices in Level 1-3 without an entry in the NIST SP 800-171 Rev 1 column

AM.3.036	AU.2.044	AU.3.048	IR.2.093	IR.2.094
IR.2.096	IR.2.097	RE.2.137	RE.3.139	RM.3.144
RM.3.146	RM.3.147	CA.3.162	SA.3.169	SC.2.179
SC.3.192	SC.3.193	SI.3.218	SI.3.219	SI.3.220

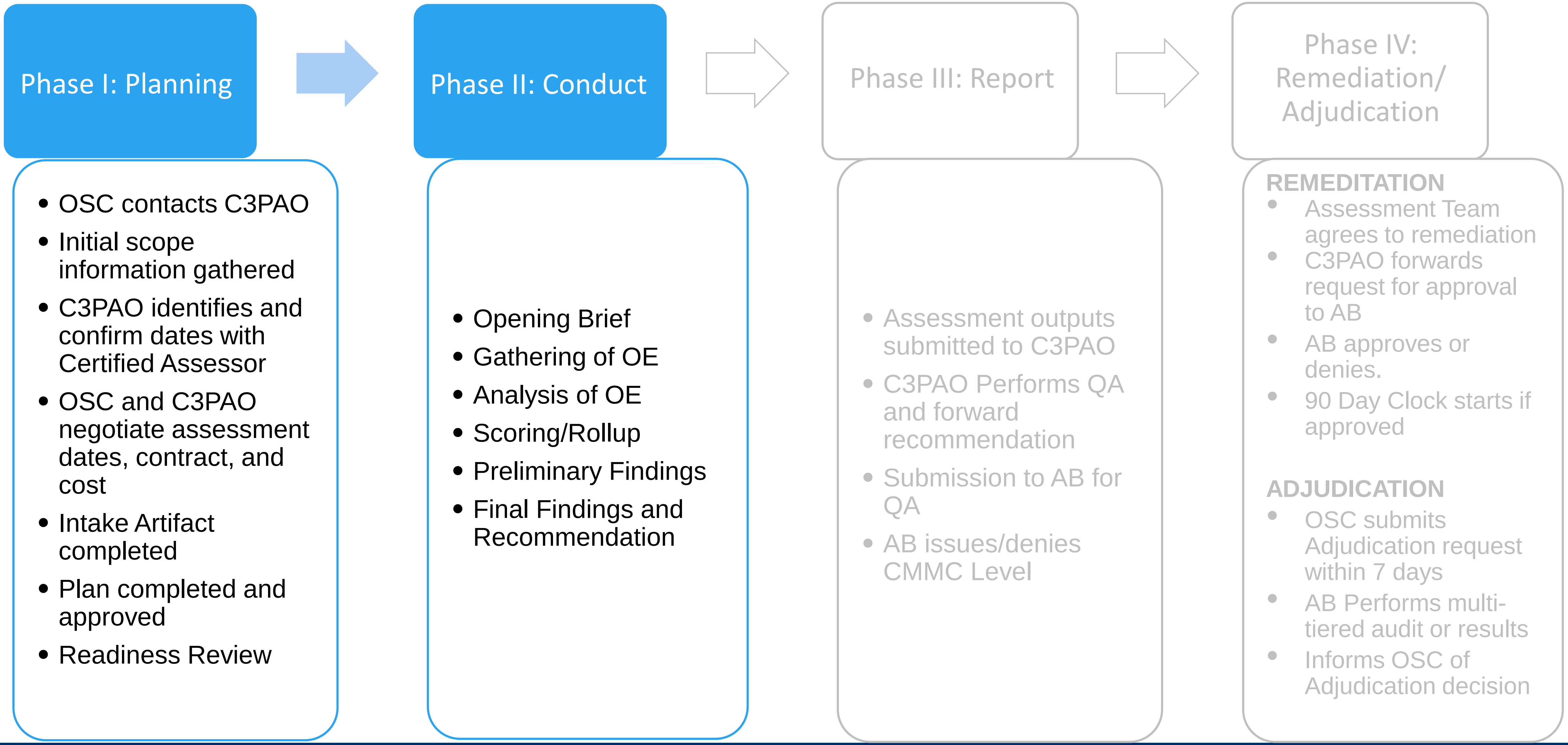
- These Practices should be the follow-on step after Implementing the NIST SP 800-171 controls

Documentation, Documentation, Documentation

- There are 3 Maturity Processes applied to each of the 17 domains
  - ML.2.999 -- **Establish** a policy
  - ML.2.998 -- **Document** the CMMC practices to implement the policy
  - ML.3.997 -- Establish, maintain, and **resource** a plan
  - L3 Assessment Guide defines the Assessment Objectives for each process
- There is not a preferred format or hierarchy. The goal is to address which Practices are addressed by which policy
- CERT Resilience Management Model (RMM) is the informative reference for each of the Maturity Processes
  - ML.2.999 -- (CERT RMM v1.2 ADM:GG2.GP1 sub practice 2)
  - ML.2.998 -- (CERT RMM v1.2 ADM:GG2.GP2 sub practice 2)
  - ML.3.997 -- (CERT RMM v1.2 ADM:GG2.GP2 sub practice 1,3,4 and ADM:GG2.GP3)

Establish, Document, Resource

What does the Assessment look like?



Phase I: Planning

- OSC contacts C3PAO
- Initial scope information gathered
- C3PAO identifies and confirm dates with Certified Assessor
- OSC and C3PAO negotiate assessment dates, contract, and cost
- Intake Artifact completed
- Plan completed and approved
- Readiness Review

Phase II: Conduct

- Opening Brief
- Gathering of OE
- Analysis of OE
- Scoring/Rollup
- Preliminary Findings
- Final Findings and Recommendation

Phase III: Report

- Assessment outputs submitted to C3PAO
- C3PAO Performs QA and forward recommendation
- Submission to AB for QA
- AB issues/denies CMMC Level

Phase IV: Remediation/ Adjudication

REMEDITATION

- Assessment Team agrees to remediation
- C3PAO forwards request for approval to AB
- AB approves or denies.
- 90 Day Clock starts if approved

ADJUDICATION

- OSC submits Adjudication request within 7 days
- AB Performs multi-tiered audit or results
- Informs OSC of Adjudication decision

Graphic obtained from CMMC-AB Provisional Assessor Course materials

Pre-work analysis activities/artifacts

- OSC Sponsor and Lead Assessor will determine the assessment scope
- Complete Self-Assessment using L3 Assessment Guide
- Gather Essential Artifacts for Assessment Team to review
  - System Security Plan
  - Network Diagram and Information Flow Diagram (information flow reference)
  - Policies and Procedures (including any referenced instructions or checklists)
  - Organization Chart (as it applies to managing CUI)
  - Cloud Service Provider “Customer Responsibility Matrix”
  - DIBCAC Assessment results / Service Provider certifications (i.e., FedRAMP)*
  - Any additional references or materials that may enable the Assessment team to fulfill an Evidence requirement
- Avoid mismatches in documentation between SSP, policy, and procedures. Avoid documents still in draft. Ensure clear policy and procedure delineation

* - No reciprocity agreements have been approved at the time of this presentation

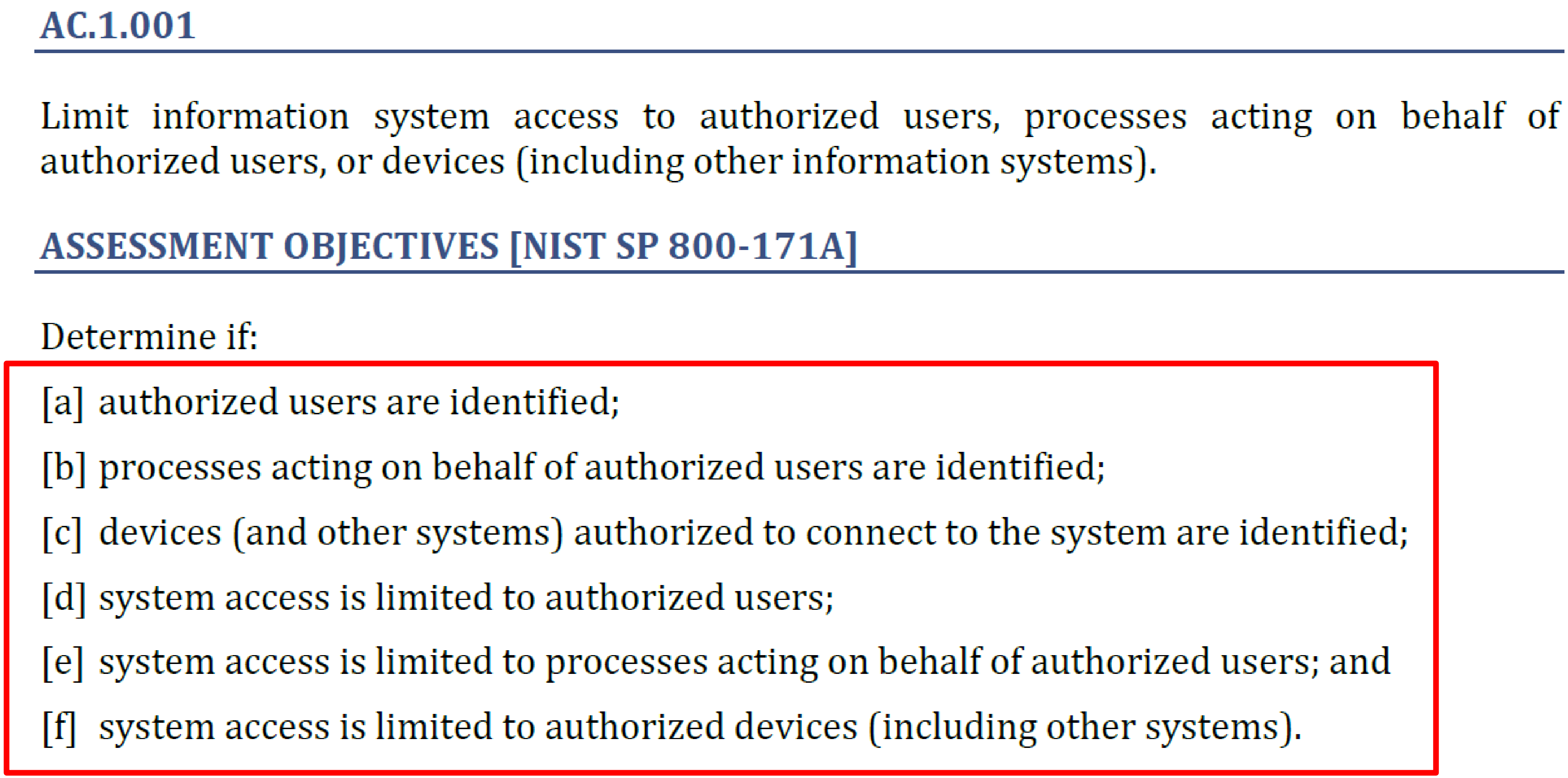
Assessment Observation Activities

- OSC should become intimately familiar with the CMMC L3 Assessment Guide and the Assessment Objectives associated with each practice

- Each practice will require two types of Objective Evidence
  - **Assessment <u>Objectives</u>** identify the specific list of objectives that must be satisfied to receive MET for the practice or process
  - **Assessment <u>Methods</u>** define the nature and the extent of the assessor's actions –
    - Examine (Artifact)
    - Interview (Observation/Affirmation)
    - Test (Demonstrate)
  - **Assessment <u>Objects</u>** identify the specific items being assessed and can include specifications, mechanisms, activities, and individuals

- Assessors will seek 'sufficiency and adequacy' when reviewing objective evidence

Assessment Observation Activities cont.



AC.1.001

Limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems).

ASSESSMENT OBJECTIVES [NIST SP 800-171A]

Determine if:

[a] authorized users are identified;

[b] processes acting on behalf of authorized users are identified;

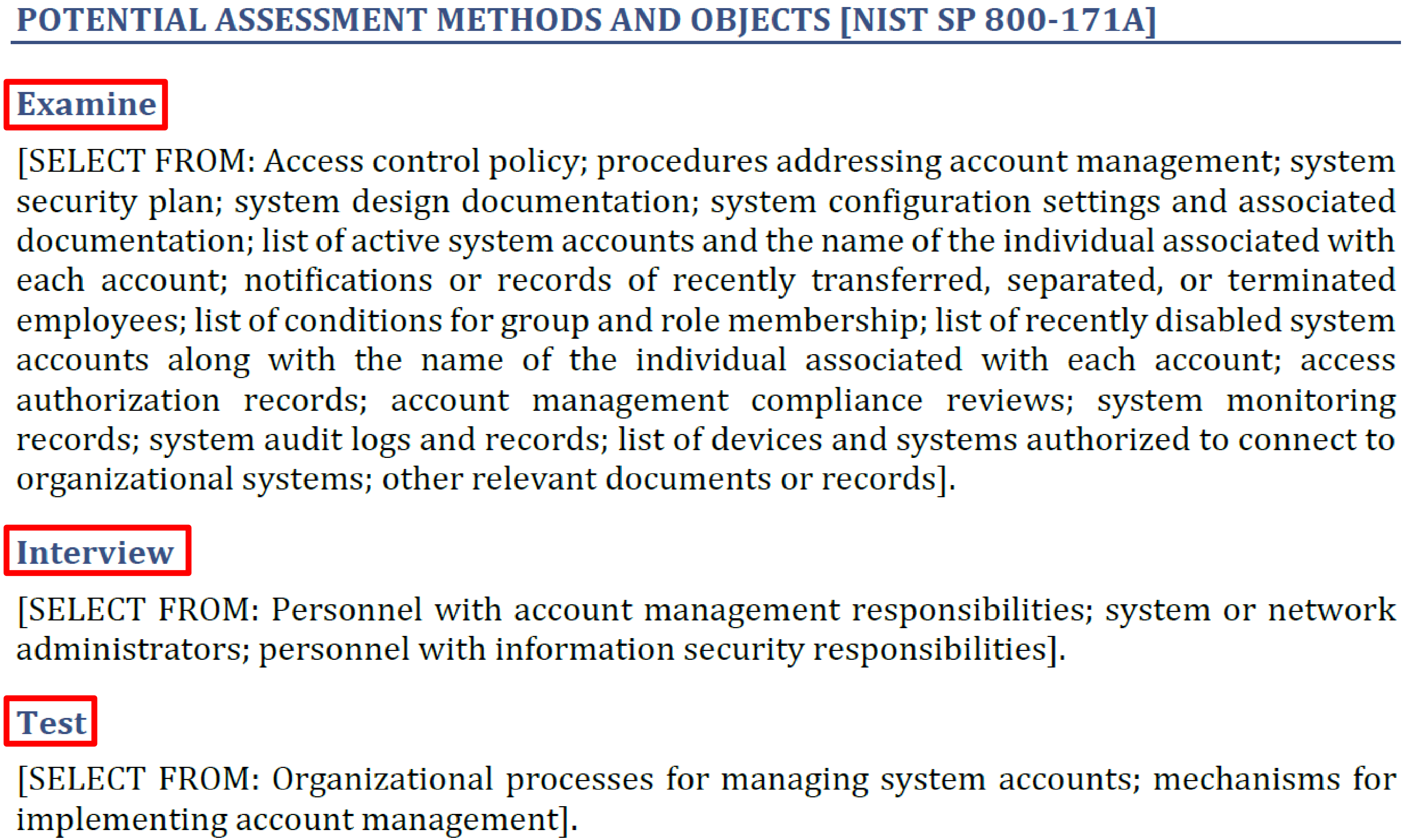
[c] devices (and other systems) authorized to connect to the system are identified;

[d] system access is limited to authorized users;

[e] system access is limited to processes acting on behalf of authorized users; and

[f] system access is limited to authorized devices (including other systems).

Second half of Assess Guide



POTENTIAL ASSESSMENT METHODS AND OBJECTS [NIST SP 800-171A]

Examine

[SELECT FROM: Access control policy; procedures addressing account management; system security plan; system design documentation; system configuration settings and associated documentation; list of active system accounts and the name of the individual associated with each account; notifications or records of recently transferred, separated, or terminated employees; list of conditions for group and role membership; list of recently disabled system accounts along with the name of the individual associated with each account; access authorization records; account management compliance reviews; system monitoring records; system audit logs and records; list of devices and systems authorized to connect to organizational systems; other relevant documents or records].

Objects

Interview

[SELECT FROM: Personnel with account management responsibilities; system or network administrators; personnel with information security responsibilities].

Test

[SELECT FROM: Organizational processes for managing system accounts; mechanisms for implementing account management].

Interconnected Control Examples

- **AC.1.001, controls system access based on user, process or device identity**
  - Leverages IA.1.076

- **AC.2.013, requires the control of remote access sessions**
  - Complements 5 other practices

- **MP.1.122, requires all media, hardcopy and digital, must be properly marked to alert individuals to the presence of CUI stored on the media**
  - A component of many other practices

Lockheed Martin's Expectations

- **Continue to progress your NIST 800-171 implementation… Full implementation (closing all POAMs) is foundational to Cybersecurity Maturity Model Certification (CMMC) Readiness**
  - Accurately maintain your vendor profile in Exostar TPM (applicability of cyber DFARS requirements)
  - Perform and regularly update your NIST 800-171 self assessment
    - Leverage the Exostar questionnaire in PIM to document and share your progress
    - Document your self assessment result in DoD's SPRS using the DIBCAC assessment methodology (Exostar developing tools to translate your PIM self assessment to the required SPRS format)
  - **Monitor subcontracts and PO terms and ensure flow down of all mandatory clauses to your suppliers when applicable**
    - Cyber DFARS 252.204-7012 / 252.204-7020
- **Communicate progress to Lockheed Martin via status updates on our Survey**
  - Responses to the survey ensure LM buyers know you are compliant (potential business impact)
  - Expand cyber maturity focus to prepare for CMMC Level 3
    - Implement additional 20 CMMC Level 2/3 practices
    - Implement CMMC Level 2/3 maturity processes

Take action to avoid disruption to new contract awards

Additional Cybersecurity Resources

- Key CMMC and CUI Information Sources
  - Official CMMC document source
  - Official CMMC Updates
  - Official CMMC FAQ
  - Exostar blog entry on CMMC
  - Cyber Assist (CMMC help website)
  - CMMC Accreditation Body
  - CMMC For Suppliers
  - CMMC Vs. NIST 800-171 and other Frameworks
  - CUI Categories
  - CUI Training from National Archives
  - CUI Marking Handbook from National Archives
  - NIST HB 162 -Self-Assessment Handbook For Assessing NIST SP 800-171
  - CMU SEI CERT Resilience Management Model v1.2
- SPRS
  - Hotline #: 1-207-438-1690
  - DCMA general mailbox: dcma.lee.hq.mbx.dibcacscheduling-inbox@mail.mil
  - SPRS Quick Entry Guide: https://www.sprs.csd.disa.mil/pdf/NISTSP800-171QuickEntryGuide.pdf
  - SPRS Frequent Asked Questions: https://www.sprs.csd.disa.mil/pdf/NISTSP800-171FAQs.pdf

Questions & Answers

LOCKHEED MARTIN