McKonly & Asbury

# Cybersecurity Maturity Model Certification (CMMC): Are You Ready?

## CMMC L2 Key Documents

March 26, 2026

# Presenters

**David Hammarberg, Partner**
CPA, CFE, CISSP, GSEC, MCSE, CISA, CCSFP, CHQP, Lead CCA

- 26 Years with the firm
- Leads CMMC, SOC 2, HITRUST, and Internal Audits service areas
- Accountable for the firm's IT team

**Elaine Nissley, Director**
MBA, CISA, PMP, CRISC, CRMA, Lead CCA

- 21 Years with the firm
- Quality Assurance CCA
- Founding member of the CMMC C3PAO Team
- Internal Audit background including IT Audit and NIST 800-53 framework audits

**Michael Murray, Manager**
**CISA, Lead CCA**

- Manages the Assessment Staff
- Leads Assessment Teams
- Founding member of the CMMC C3PAO Team
- 10 years as a U.S. Army Intelligence Collector

**Ryan Handley, Supervisor**
**CISSP, Lead CCA**

- Leads Assessment Teams
- 7 years Experience with NIST 800-53, 800-171 assessments
- 15 years in the Pennsylvania Air National Guard

# Firm Overview

*Helping You Thrive!*

## McKonly & Asbury

M&A is a team of CPAs and Business Advisors serving clients from our offices in Camp Hill, Lancaster, Bloomsburg, and Philadelphia.

accountingTODAY 2025 Best Firms to Work For

accountingTODAY 2025 Best Firms for Young Accountants

BEST PLACES to work in PA 2025

## Services Provided

- Advisory & Business Consulting
- Audit & Assurance
- Tax
- Entrepreneurial Support & Outsourced Accounting
- SOC & Technology Consulting

## Industries Served

- Affordable Housing
- Architecture, Engineering, and Construction (AEC)
- Entrepreneurial
- Family-owned Business
- Franchises
- Healthcare
- Manufacturing & Distribution
- Nonprofit
- Public Companies

# Subscribe for M&A Insights

## Pick your perfect thought leadership mix from 15 newsletters!

McKonly & Asbury

macpas.com

# Agenda

- Authoritative Sources For Scoping Your Environment
- Key Documents
- System Security Plan
- Network Diagrams
- CUI Flow Diagram
- Categorized Asset List (CUI, SPA, CRMA, Specialized)
- Determining Service Provider Type
- SRMs (if applicable)
- Initial Evidence Package

# Scoping the Environment

- Authoritative sources for scoping your environment
  - CMMC Scoping Guide Level 2, Sep 2024
  - CMMC Assessment Guide Level 2, Sep 2024

# Key Documents

- Key Documents Include:
  - System Security Plan
  - Network Diagrams
  - CUI Flow Diagrams
  - Categorized Asset List
  - Share Responsibility Matrices (if applicable)

- These documents are crucial to determining scope during phase 1 of a CMMC L2 assessment. These documents should work in conjunction with each other to provide a clear picture of the environment.

# System Security Plan

- The SSP must address/include the following:
  - CMMC L2 Implementation at the objective level (320 objectives)
    - All 110 security controls and their associated 320 objectives described in detail
    - Reference supporting documents where applicable
  - An overview/description of the CMMC L2 environment
  - All applicable roles and responsibilities
  - Version/revision history
  - Network diagram
  - CUI flow diagram

These two may be included in a single diagram

# Network Diagrams

- All assets in the categorized asset list should be present on this diagram
- Overall network architecture should be present and apparent
- Should accurately describe the scope of the assessment

# CUI Flow Diagrams

- Should answer the following questions:
  - Where does CUI enter the environment?
  - Where does CUI traverse the environment? (in transit)
  - Where is CUI stored in the environment? (at rest)
  - Where does CUI exit the environment?

# Categorized Asset List

- Assets should be categorized IAW the CMMC L2 scoping guide

| Asset Category | Asset Description |
|---|---|
| Controlled Unclassified Information (CUI) Assets | Assets that process, store, or transmit CUI |
| Security Protection Assets | Assets that provide security functions or capabilities to the OSA's CMMC Assessment Scope |
| Contractor Risk Managed Assets | Assets that **can, but are not intended to, process, store, or transmit CUI** because of security policy, procedures, and practices in place. Assets are not required to be physically or logically separated from CUI assets |
| Specialized Assets | Assets that can process, store, or transmit CUI but are unable to be fully secured due to inherent design or other limitations. |
| Out-of-Scope Assets | Assets that cannot process, store, or transmit CUI; and do not provide security protections for CUI Assets. Assets that are physically or logically separated from CUI assets |

# Cloud Service Provider Characteristics

- See NIST 800-145 for reference.
- Essential characteristics for a Cloud Service Provider (CSP):
  - On-demand self-service
  - Broad network access
  - Resource pooling
  - Rapid elasticity
  - Measured service

# ESP/CSP Additional Details

- CSPs handling CUI must be FEDRAMP moderate or equivalent
- CSPs handing SPD only do not have to be FEDRAMP moderate or equivalent, but will be included in the OSC's assessment scope as Security Protection Assets (SPA)
- Non-CSP ESPs handing CUI will be included in the OSCs scope as CUI assets (All 320 objectives)
- Non-CSP ESPs handling SPD only will be included in the OSCs scope as SPA and will be assessed IAW the services that they provide

# Determining Service Provider Type

- Table from the final rule (32CFR)

TABLE 4 TO § 170.19(c)(2)(i)—ESP SCOPING REQUIREMENTS

| When the ESP processes, stores, or transmits: | When utilizing an ESP that is: | |
|---|---|---|
| | A CSP | Not a CSP |
| CUI (with or without SPD) .. | The CSP shall meet the FedRAMP requirements in 48 CFR 252.204–7012. | The services provided by the ESP are in the OSA's assessment scope and shall be assessed as part of the OSA's assessment. |
| SPD (without CUI) ..... | The services provided by the CSP are in the OSA's assessment scope and shall be assessed as Security Protection Assets. | The services provided by the ESP are in the OSA's assessment scope and shall be assessed as Security Protection Assets. |
| Neither CUI nor SPD ..... | A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP. | A service provider that does not process CUI or SPD does not meet the CMMC definition of an ESP. |

# Shared Responsibility Matrix

- A good SRM should avoid vague language, such as ‘may or may not,’ ‘might,’ ‘possibly,’ when describing the assignment of responsibility.
- The assignment of responsibility should mirror what is in the SSP
- The SRM should specify responsibility down to the objective level
- For objectives marked as shared, what part is OSC’s responsibility, and what part belongs to SRM owner?

# Initial Evidence Package

- Should include a complete listing of all applicable policies and procedures pertaining to the selected scope of the CMMC L2 Assessment
- Should include as many artifacts/evidence of implementation as possible
- Being prepared up front allows for the most efficient use of time during the assessment
- In addition to artifacts, assessors may choose to request a live demonstration during interview sessions to clarify any evidence/artifacts received

# NIST 800-171A Terminology

- Defined, Specified
  - If a NIST 800-171A objective states that something must be defined or specified, it must be written, *explicitly stated* in a policy, procedure, or the SSP itself.
  - Follow-on objectives within the same requirement usually ask assessors to determine if implementation is matching organizationally defined policy, so without these, determination on implementation cannot be made.
  - Sometimes enterprise policies are not specific enough. Policy definitions must speak to what is happening, or what is intended to be happening, within the scope of the CMMC L2 assessment.

# NIST 800-171A Terminology cont'd

- All objectives that do not specifically state that something must be defined or specified are looking for proof of implementation.
- This can be achieved through screen shots, live demonstration/shoulder-surf, processes, or interviews with applicable staff.

# Specific Objectives Example

- 3.3.1[e] – retention requirements for audit logs are defined
  - See pg. 14 of example AU policy included with presentation package

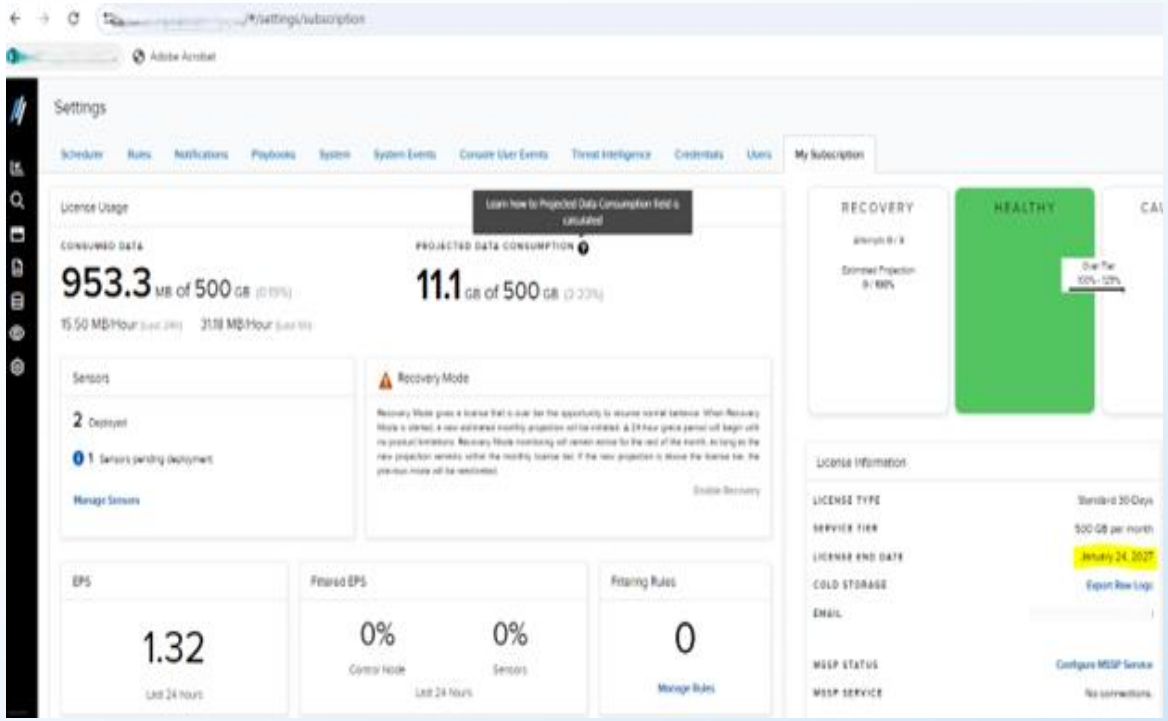
VM audit logs are retained within AlienVault SEIM for one year. AlienVault will alert the System Administrator, IT Director, and Security officer via e-mail in the event a VM experiences an audit logging process failure, shows signs of compromise, or configuration errors. AlienVault SEIM allows filtering by several parameters including: event type, time, device/system component. AlienVault can produce on-demand reporting and analysis. AlienVault allows in-depth analysis, providing insights and resources for potential indicators of attack, abnormal device behavior, and configuration issues.

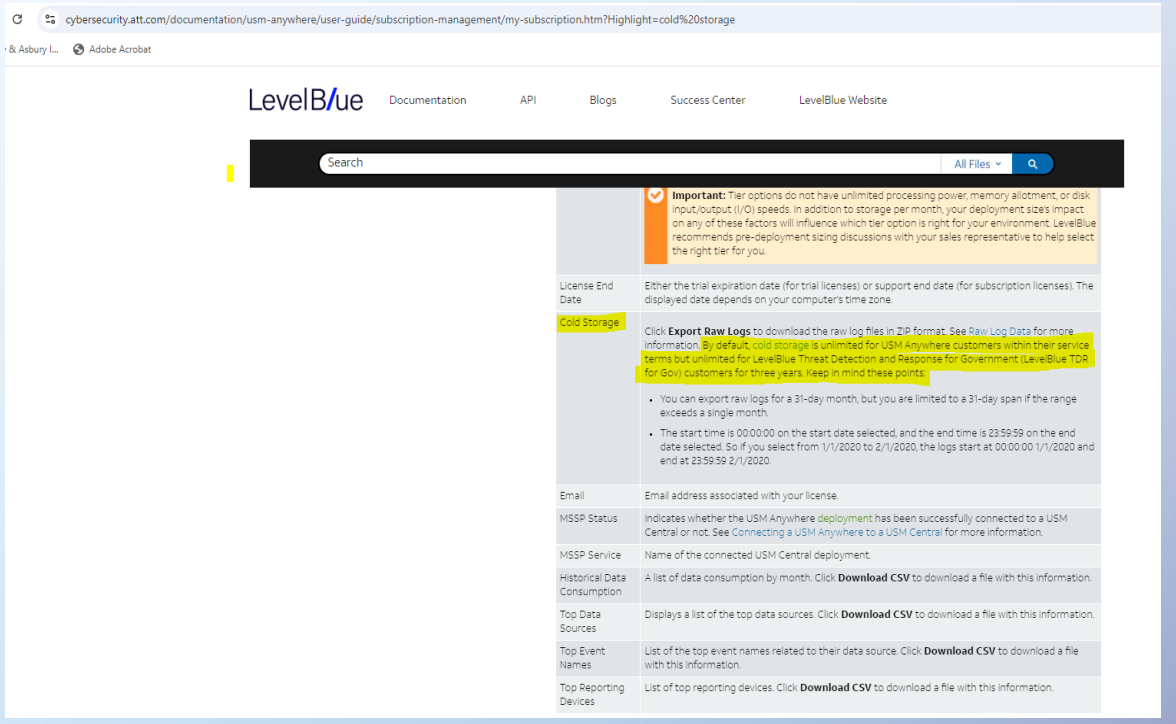
Unless otherwise stated within this document, all system flaws will be remediated according to the following table. If there are any identified items that need to be added to the Risk Registry, security assessment, and/or the Incident Response Repository. Please see the Risk Assessment, Security Assessment, and the Incident Response Plan for more information:

| System Flaw Severity | Time to Respond to System Flaw |
|---|---|

# Specific Objectives Example

- 3.3.1[f] – audit records are retained as defined
  - See “3.3.1 Evidence AlienVault logs.docx” included with presentation package



# Questions?

# Contact Information


**David Hammarberg, CPA, CFE, CISSP, GSEC, MCSE, CISA, CCSFP, CHQP, Lead CCA**

**Partner**

dhammarberg@macpas.com

717-761-7910



**Elaine Nissley, MBA, CISA, PMP, CRISC, CRMA, Lead CCA**

**Director**

enissley@macpas.com

717-972-5728



**Michael Murray, CISA, Lead CCA**

**Manager**

mmurray@macpas.com

570-317-9524



**Ryan Handley, CISSP, Lead CCA**

**Supervisor**

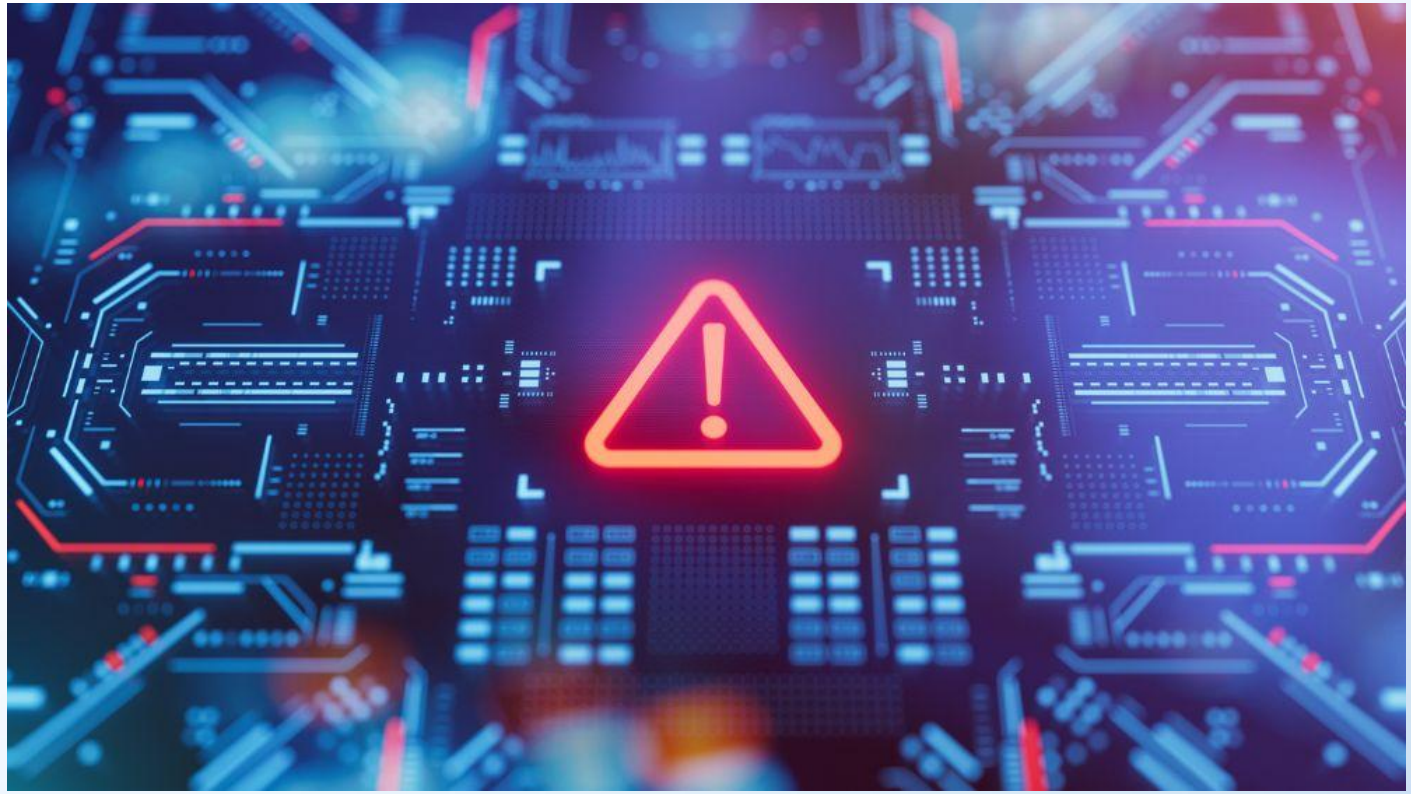
rhandley@macpas.com

717-200-4835

McKONLY & ASBURY

# Upcoming Events

# April 30 Webinar



## Are You Happy with Your SOC Provider? – Key Differentiators and Red Flags

**REGISTER NOW**