2026 ASEE ANNUAL CONFERENCE June 21–24, 2026 | Charlotte Convention Center, NC
Host Sponsor UNC Charlotte
ASEE AMERICAN SOCIETY FOR ENGINEERING EDUCATION
Paper ID #52815

A University Response to the CMMC Mandate: Bridging the Gap Between Academia and the Defense Industrial Base

Sumner Kirby, The University of Oklahoma Polytechnic Institute

Sumner Kirby is a graduate student in cybersecurity at the University of Oklahoma Polytechnic Institute.

Dr. Chad B Roller, University of Oklahoma, Polytechnic Institute

Chad Roller Ph.D. currently serves as a GKFF Assistant Professor at the University of Oklahoma Polytechnic Institute. Prior to joining academia, he spent over 20 years in the energy sector in both technical and executive leadership roles at Shell, Midcon Energy and Contango Resources. Chad earned a Ph.D. at Rice University in Electrical Engineering.

Christopher Freeze, The University of Oklahoma

I serve as an assistant professor at the Polytechnic Institute at the University of Oklahoma. I hold a Ph.D. in Organizational and Community Leadership and previously served as a Special Agent and Special Agent in Charge with the FBI. My work focuses on cybersecurity leadership, human-centered security, and behavioral risk in high-stakes environments. I research hope-centered leadership, burnout, workforce resilience, and trust, and I designed OUPI's Master of Science in Cybersecurity Leadership program to prepare the next generation of cybersecurity leaders.

Kristina Wadley, The University of Oklahoma Polytechnic Institute

Work-in-Progress: University Response to the CMMC Mandate; Bridging the Gap Between Academia and the Defense Industrial Base

Abstract

The Department of War (DoW) transition to the Cybersecurity Maturity Model Certification (CMMC) as a requirement for contracts has revealed a critical workforce deficit within the assessment ecosystem. With over 80,000 contractors requiring triennial Level 2 certifications, the current supply of Certified CMMC Assessors (CCAs) is insufficient to meet demand. This bottleneck is exacerbated by a fragmented professional education model and strict experience requirements that favor established professionals over new talent. This Work-in-Progress paper proposes a replicable institutional model for higher education to serve as a workforce pipeline for the Defense Industrial Base (DIB). Using the University of Oklahoma's Polytechnic Institute (OUPI) as a pilot case study, an integrated, credit-bearing academic concentration has been designed to embed Certified CMMC Professional (CCP) and CCA curricula directly into existing cybersecurity degrees. Further, the pilot incorporates community cybersecurity service, orchestrated through a cybersecurity clinic model to help fulfill, if not satisfy, the experience requirements of the CCA certification. We suggest that by replacing short-term training with semester-long mastery and clinical practice, academic institutions can produce assessment-ready graduates, partially address the assessor shortage, and enhance the long-term resilience of the national defense supply chain.

I. INTRODUCTION

As the DoW transitions into the active enforcement of the CMMC framework, the DIB faces significant structural challenges regarding audit and assessment workforce capacity. As of November 2025, the DoW has begun to require CMMC compliance as a condition for all new contract awards [1]. Organizations which work with Controlled Unclassified Information (CUI)

will now require at least a Level 2 CMMC certification. This certification involves both the implementation of 110 security controls derived from NIST SP 800-171, and an assessment of those criteria by a third-party certified auditing organization (C3PAO) [1]. While self-attestation is permitted under the framework for select non-critical scenarios, in practice it has proven insufficient for organizations seeking to remain competitive for prime- or sub-contracts. This is largely driven by mandatory flow-down requirements where prime contractors must ensure their subcontractors maintain a cybersecurity posture equivalent to the sensitivity of the data they handle. For example, if a prime contractor is required to hold a Level 2 certification to manage CUI, they must verify that any subcontractor processing that same CUI also holds a corresponding Level 2 certification [2].

The widespread requirement for third-party verification has created a substantial bottleneck in the certification pipeline. The DoW estimates that on the low end at least 80,496 contractors will require triennial Level 2 certifications performed by a C3PAO [3]. However, the supply of qualified professionals is not currently sufficient for this volume of work. As of July 2025, CyberAB, the official accreditation body of CMMC, listed only 267 lead CCAs and 402 CCA assessors [4]. Given that an assessment requires at least one CCA, maintaining the required 80,496 certifications over a three-year cycle would require roughly 26,832 assessments split between 670 qualified assessors annually. Given that a Level 2 assessment, on average, requires 3 months, multiple assessors and a C3PAO, this level of work is infeasible for the current number of CCAs [5]. Further, this assumes that these professionals only work in an assessment capacity, where in reality they perform consulting and other security services in addition to their CMMC auditing.

This capacity gap presents a notable risk to the national security supply chain and the overall federal acquisition process. As demand for triennial certified assessments outpaces the supply of available assessors, the resulting scarcity is likely to drive up costs of certification and potentially shrink the pool of available defense contractors. This environment may become even more stretched if the regulatory landscape expands beyond the DoW. The Federal Acquisition Regulatory (FAR) Council has already published proposed rules concerning CUI and Organizational Conflicts of Interest, which suggests CMMC or CMMC-style requirements for assessments and audits could eventually be adopted by all federal agencies [6].

The emerging bottleneck highlights a critical need for new educational initiatives and workforce development programs designed to train the next generation of cybersecurity assessors. The current path to becoming a CCA is fragmented and favors established professionals over new talent. Prospective assessors currently navigate a decentralized ecosystem of short-term, bootcamp-style courses provided by various private training providers. Achieving CCA status requires a minimum of three years of cybersecurity experience and one year of auditing experience, creating a significant time barrier for entry-level graduates. Further, candidates must also hold intermediate certifications, such as CompTIA Security+ or GIAC GSEC, mapped to the DoD Manual 8140.03 before they are eligible for the CCA certification [7]. (See Figure 1).

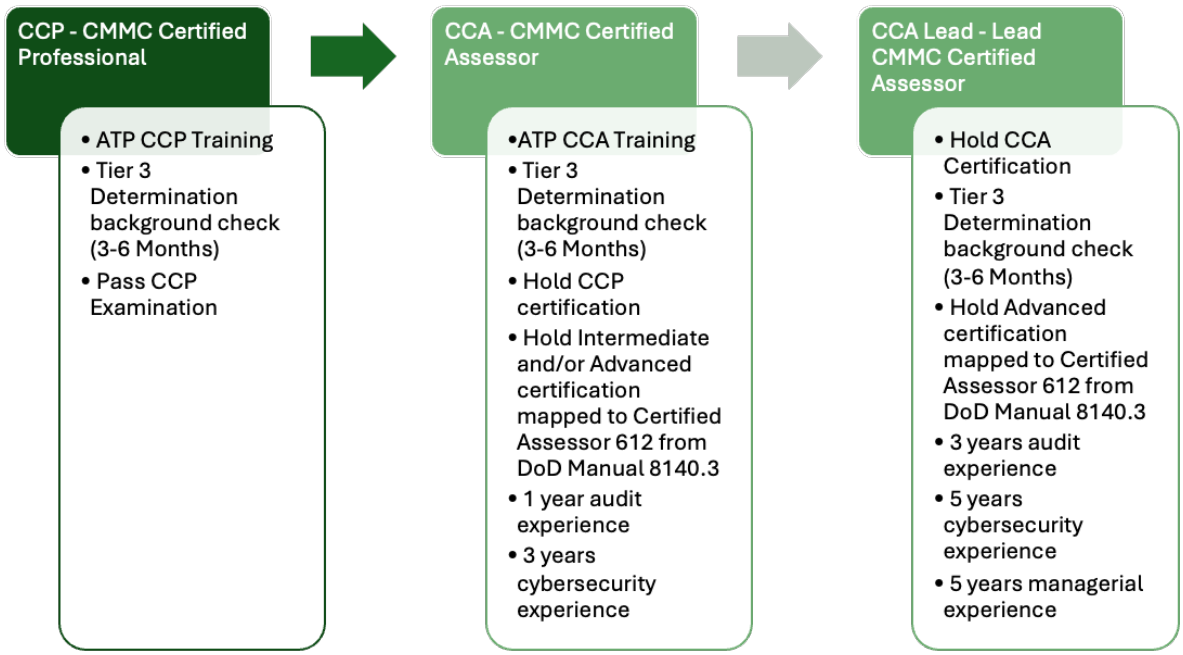


Figure 1
Baseline Requirements for CMMC Professional Certifications

II. METHODOLOGY

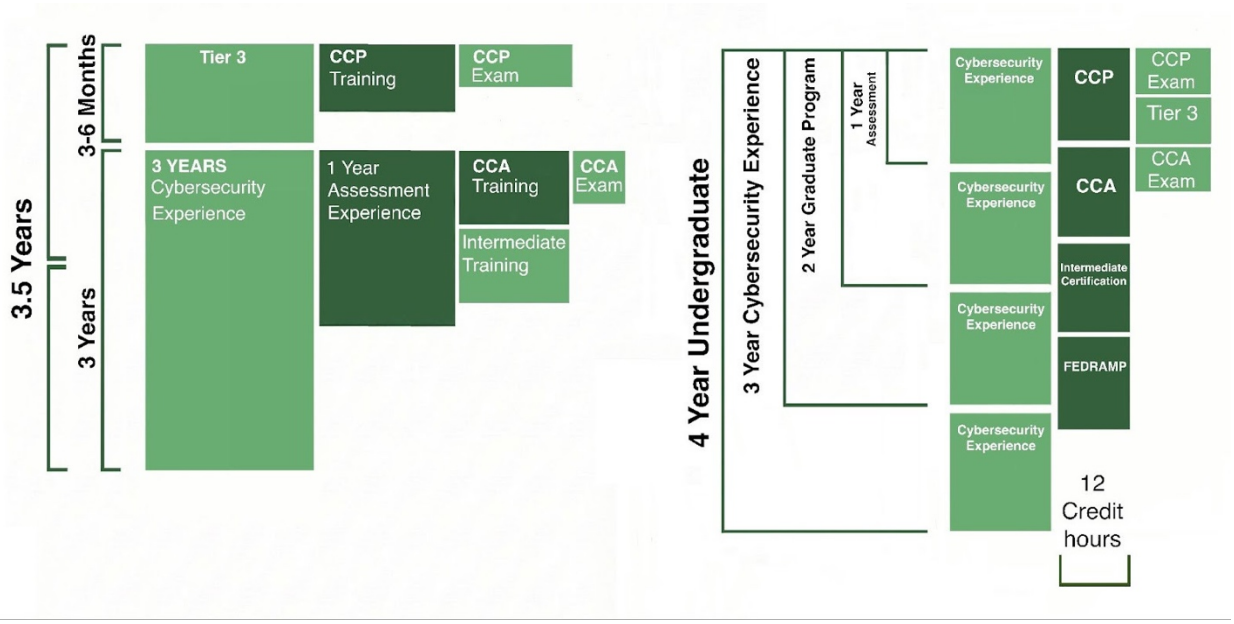
This study will utilize a mixed-methods approach to evaluate the pilot program approved by the Institutional Review Board (IRB). Quantitative data will consist of pre- and post-program competency assessments based on NIST controls and certification exam pass rates for the CCP and CCA (See Appendix A). Qualitative data will include semi-structured interviews with student participants and community clients to evaluate the efficacy of the clinic model (See Appendix B). Data collection milestones can be mapped to each course. Apart from the *CCA Training course*, which requires previous completion of the *Introduction to CMMC and CCP Training*, there is no logical order required for any of the elective concentration courses. They could be taken concurrently or spread across semesters. The proposed required classes and collection milestones are detailed later in Table 1.

II-A. Pilot Design

OUPI has designed a replicable institutional model that embeds professional certification requirements directly into its existing academic infrastructure within its Bachelor and Master of Science in Cybersecurity degree programs. The expected pilot cohort makeup is between 6-8 students from both the undergraduate and graduate cybersecurity programs. By achieving status as an Approved Training Provider (ATP) and employing a Certified CMMC Instructor (CCI), the university can offer the CCP and CCA curricula as credit-bearing academic courses that utilize official CAICO Approved Training Materials (CATM)[8].

In addition to the two CMMC certification courses, this academic track also includes a dedicated course on FedRAMP and technical writing. This inclusion is aimed at addressing workforce expectations in cloud computing and security standards, as over 80% of CMMC job postings list a secondary compliance framework like FEDRAMP [4]. Proficiency in technical writing is equally vital for assessor employability, as professionals must be able to translate complex technical findings into actionable reports and System Security Plans (SSPs) for non-technical business owners. Additionally, the curriculum leverages an existing Foundations of Cybersecurity course that aligns with and prepare students for the mandatory intermediate certification, allowing them to satisfy this prerequisite for the CCA exam without external study. The entire concentration comprises 12 credit hours that fit within the 15-18 available free elective hours, making it possible to earn this concentration without extending time-to-degree. (See Figure 2).

Figure 2
Standard CMMC Professional Timeline (left) Compared to OUPI Proposed Model (right)



II-B. Cybersecurity Clinic Model

To address the experience requirements mandated for the CCA, the proposed model utilizes a cybersecurity clinic to facilitate supervised, real-world engagements, specifically focusing on community outreach. Membership in the Consortium of Cybersecurity Clinics enables OUPI to leverage a pre-existing clinic framework to target SMBs and DIB sub-tier suppliers who may lack sufficient internal security resources. The CMMC Level 1 framework provides the ideal structure for these engagements; because it consists of 15 basic safeguarding requirements necessary for self-attestation, students can conduct gap analyses and provide remediation recommendations without exposing the university to the complexities and legal challenges associated with Level 2 assessments. These documented hours allow students to

accumulate verifiable assessment experience necessary for the CCA designation while hardening the regional supply chain. To evaluate the efficacy of this experiential model, the program will employ a data-driven assessment framework that tracks quantitative outcomes, such as the number of completed assessments and average remediation time, alongside qualitative feedback gathered through structured client satisfaction surveys and student exit interviews.

III. RESEARCH DESIGN AND EVALUATION FRAMEWORK

To evaluate the effectiveness of the OUPI pilot model, this study seeks to answer the following research questions:

- **R1:** How does academic delivery of CCP and CCA curricula compare to the traditional bootcamp model in terms of student retention of NIST Security Controls?
- **R2:** To what extent is it feasible to integrate a CMMC concentration into existing cybersecurity degree programs without extending the standard time-to-degree?
- **R3:** To what extent can an academic concentration satisfy the cybersecurity experience requirements of higher level CMMC assessor paths?
- **R4:** To what extent can a cyber-clinic model satisfy the audit experience requirements of higher level CMMC assessor paths?

The rationale for these research questions is grounded in the structural challenges of the current CMMC ecosystem, which is characterized by a piecemeal and decentralized professional education model. (R1) addresses the pedagogical limitations of the existing weeklong instructor-led training bootcamps, which may be poorly equipped to provide the in-depth mastery required for the 110 complex security controls of NIST SP 800-171. By contrasting the rapid pace of

traditional training with a 15-week academic semester, this study evaluates whether higher education provides an environment for more comprehensive learning.

(R2) investigates the institutional feasibility of this model, specifically examining if the modular nature of the 12-credit-hour concentration can be integrated into the 15-18 available elective hours at OUPI without significantly increasing the administrative burden or the student's time-to-degree. (R3) explores how academic alignment can satisfy the three years of technical cybersecurity experience required for the CCA and higher-level Lead CCA designations. Similarly, (R4) evaluates the efficacy of the university cybersecurity clinic model in providing the supervised, field-based assessment experience necessary to satisfy the mandatory one-to-three-year auditing requirements. By investigating these intersections, this study seeks to determine if a centralized institutional model can effectively produce assessment-ready graduates.

The proposed data collection plan utilized to answer these research questions is detailed in **Table I**. To support the study, several research artifacts will be utilized to track student progress and program efficacy. These include standardized testing materials and curriculum outlines designed to meet CAICO-mandated training objectives (See Appendix C).

Table I
Sample Data Collection Plan

Primary Course/Activity	Data Collection Milestones
Introduction to CMMC and CCP Training	• **Baseline Assessment:** Initial testing on 15 Level 1 safeguarding requirements. • **Post-Course Assessment:** Re-testing of Level 1 controls at term conclusion. • **Credential Record:** Collection of official CCP **e**xamination results.

Primary Course/Activity	Data Collection Milestones
Foundations of Cybersecurity **(Intermediate Certification)**	• **Pre-Intermediate Assessment:** Baseline of technical domains (e.g., CompTIA Security+) • **Credential Record:** Record of successfully earned intermediate CompTIA Security+.
CCA Training	• **Pre-CCA Assessment:** Baseline testing on all 110 NIST SP 800-171 security controls. • **Post-Course Assessment:** Final academic testing on complex assessment criteria. • **Credential Record:** Collection of official CCA **e**xamination results.
FEDRAMP and Technical Writing	• **Pre-Course Assessment:** Baseline testing on fundamental cloud security concepts, FIPS 199 system categorization, NIST SP 800-53 control families. • **Post-Course Assessment:** Final academic testing on complex assessment criteria, SSP's, and the application of FedRAMP Continuous Monitoring (ConMon) timelines for vulnerability remediation.

IV. DISCUSSION

Note: As this is a Work-in-Progress, the analysis of full results is pending. The preliminary findings and expected outcomes are discussed in the Conclusion below.

V. CONCLUSION

This work-in-progress study highlights that higher education institutions are uniquely positioned to address the critical shortage of qualified CMMC assessors by centralizing the fragmented certification pathway into a cohesive, credit-bearing academic concentration. By embedding the necessary training, certifications, and work experience into existing degree programs, the proposed model demonstrates that it is feasible to produce assessment-ready

graduates within the academic system without extending the standard time-to-degree or imposing significant administrative burdens.

V-A. Preliminary Results and Expected Outcomes

Preliminary analysis of the pilot model suggests that integrating the CMMC certification pathway into the academic curriculum is both structurally feasible and pedagogically superior to existing training alternatives. The concentration design's 12 credit hours fit easily into the available free elective hours of a regular undergraduate program, allowing students to specialize without extending their time-to-degree.

Early observations indicate that extending the training over a full semester rather than a condensed bootcamp provides students with significantly more time to master the 110 security controls of NIST SP 800-171 and develop additional workforce related skills like technical writing and FEDRAMP familiarity. Projected outcomes are that this comprehensive approach can produce graduates who have not only satisfied the CCP and CCA instructional mandates but have also accumulated enough auditing experience through clinic participation that they may enter the workforce as fully fledged CCAs. Future evaluation will utilize longitudinal tracking of these cohorts to quantify certification exam pass rates and validate the long-term impact of this institutional model on the DIB workforce shortage.

V-B. Limitations and Future Work

It must be noted that these findings are drawn from a pilot context; the results presented here are provisional and based on designs which require further validation through larger sample sizes and prolonged observation. Future work will focus on the full launch of the pilot cohort in

Fall 2026, accompanied by longitudinal data collection to track technical competency gains, certification exam pass rates, and long-term workforce placement within the Defense Industrial Base. Furthermore, the scalability of this educational pipeline is subject to regulatory constraints of the CMMC ecosystem, most notably the requirement for all prospective assessors to undergo a Tier 3 background check for a non-critical sensitive national security position. This mandatory screening process, which can take up to six months to complete, restricts program eligibility thereby limiting the potential pool of cohort candidates.

Declaration of Generative AI and AI-assisted Technologies in the Writing Process

During the preparation of this work, the authors utilized Generative AI to correct errors, enhance language, and refine some arguments. After using these, the authors reviewed and edited the content as needed, taking full responsibility for the paper's content.

REFERENCES

[1]
U.S. Department of Defense, "About CMMC," *dodcio.defense.gov*, 2024. https://dodcio.defense.gov/CMMC/About/
[2]
Department of Defense, "Technical Application of CMMC Requirements," *dodcio.defense.gov*, Feb. 2025. https://dodcio.defense.gov/Portals/0/Documents/CMMC/TechImplementationCMMC-Rqrmnts.pdf (accessed Jan. 16, 2026).
[3]
Federal Register, "Defense Federal Acquisition Regulation Supplement: Assessing Contractor Implementation of Cybersecurity Requirements (DFARS Case 2019-D041)," *Federal Register*, Sep. 10, 2025. https://www.federalregister.gov/documents/2025/09/10/2025-17359/defense-federal-acquisition-regulation-supplement-assessing-contractor-implementation-of#p-192 (accessed Jan. 10, 2026).
[4]
"CMMC Talent Insight Report | securitysearch.io," *securitysearch.io*, 2024. https://www.securitysearch.io/cmmctalentreport (accessed Jan. 18, 2026).
[5]
L. Davis, "CMMC Assessment Timeline - How Long Does the Certification Process Take?," *CMMC Audit Preparation*, Nov. 10, 2025. https://www.cmmcaudit.org/cmmc-

assessment-timeline-how-long-does-the-certification-process-take/ (accessed Jan. 18, 2026).
[6]
Federal Register, "Federal Acquisition Regulation: Controlled Unclassified Information," *Federal Register*, Jan. 15, 2025. https://www.federalregister.gov/documents/2025/01/15/2024-30437/federal-acquisition-regulation-controlled-unclassified-information
[7]
J. Sherman, "DOD MANUAL 8140.03 CYBERSPACE WORKFORCE QUALIFICATION AND MANAGEMENT PROGRAM," Feb. 2023. Available: https://dodcio.defense.gov/Portals/0/Documents/Library/DoDM-8140-03.pdf
[8]
"Training and Instructors | Cyber-AB," Cyberab.org, 2024. https://cyberab.org/CMMC-Ecosystem/Ecosystem-Roles/Training-and-Instruction (accessed Jan. 18, 2026).

APPENDIX A

Sample Pre- and Post-program Competency Assessment

CCP Knowledge Assessment

CCP Course – Knowledge Assessment (Pre / Post)

Measuring Mastery of CMMC, DFARS, NIST 800-53r5, NARA, and Related Processes

Participant Name: _____

Date: _____

Administration (Circle One): PRE-COURSE / POST-COURSE

Instructions

This assessment is designed to measure your knowledge growth regarding the CMMC ecosystem and regulatory requirements . You will complete this same form before the course begins and again upon completion to quantify learning gains.

- For **Section A**, select the best answer for each multiple-choice question.
- For **Section B**, provide a brief written response in the spaces provided.
- For **Section C**, circle the number that best reflects your current level of confidence.

Section A – Multiple-Choice Knowledge Check

1. **CMMC Ecosystem:** Which best describes the relationship between CMMC Levels and DoW contracts?
    - A. Level 1 is required for all contracts regardless of data.
    - B. Level 2 is required for any contract involving CUI.
    - C. Only Prime contractors require certification.
    - D. Self-attestation is acceptable for all Level 2 contracts.
2. **DFARS Clauses:** DFARS clause 252.204-7012 primarily requires contractors to:
    - A. Self-certify for Level 3 compliance annually.
    - B. Report cyber incidents and protect CUI on internal systems.
    - C. Implement only physical security controls.
    - D. Eliminate all third-party subcontractors.
3. **Control Families:** Which control family includes "Limit system access to authorized users"?
    - A. Identification and Authentication

- B. Physical Protection
- C. Access Control
- D. System and Information Integrity

4. **CAP Process:** During the CAP process, the first step after identifying a non-conformance is to:
   - A. Perform a Tier 3 background check on the assessor.
   - B. Terminate the existing DoW contract immediately.
   - C. Document the finding and establish a remediation timeline.
   - D. Re-apply for C3PAO status.
5. **Scoping Processes:** For CMMC scoping, a system is considered in-scope if it processes, stores, or transmits:
   - A. Only publicly available marketing data.
   - B. Financial payroll records of non-DIB employees.
   - C. Federal Contract Information (FCI) or CUI.
   - D. Any data used by the university's general student body.
6. **NARA Categories:** Under National Archives and Records Administration records classification, Category II records are defined as:
   - A. Records requiring the highest level of national secrecy.
   - B. Records requiring standard handling but with specified protections.
   - C. Public records with no protection requirements.
   - D. Records intended for immediate destruction.
7. **NIST 800-53r5 Controls:** Which NIST 800-53r5 control maps most directly to CMMC AC-3 (Separation of Duties)?
   - A. AC-5
   - B. IA-2
   - C. MP-6
   - D. PE-3

Section B – Short-Answer Scenario

Scenario 1: Your company has just received a new contract that triggers DFARS 252.204-7012 . Describe the steps you would take to determine whether a new system falls within CMMC scope.

Response:

Scenario 2: During a CAP review, you discover that a Category III record is stored on a system lacking multi-factor authentication. Explain how you would remediate this issue, referencing the appropriate CMMC control family and NIST 800-53r5 mapping.

Response:

Section C – Self-Confidence Rating (Likert Scale)

1. **I can accurately identify which DFARS clauses apply to an organization.**

   Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree

2. **I can understand and explain the control families within the CMMC Level one guide and NIST SP 800-53r5.**

   Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree

3. **I can classify records correctly according to NARA categories.**

   Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree

APPENDIX B

Sample Post-Assessment Feedback Form

CMMC Level 1 Assessment Feedback Form

Respondent Information

- **Name:** _____
- **Company:** _____
- **Date of Assessment:** _____
- **Contact Information (Email/Phone):** _____

Instructions Thank you for participating in this mock CMMC Level 1 assessment conducted by OUPI cybersecurity students. Your feedback is vital for the continuous improvement of our student training program and our clinic's community outreach efforts.

Section A – Assessment Experience

Please circle the following statements regarding the assessment process:

1) The assessment team explained the purpose of each security control clearly.
Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree
2) The students conducted themselves in a professional and respectful manner.
Statement Strongly Disagree Disagree NeutralAgree Strongly Agree
3) The communication regarding the assessment schedule and requirements was timely.
Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree
4) The assessment was conducted efficiently without excessive disruption to business operations.
Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree
5) The team respected the privacy and confidentiality of our organizational data.
Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree
6) The students were able to answer our technical questions effectively.
Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree

Section B – Security Controls Feedback

CMMC Level 1 consists of 15 basic safeguarding requirements grouped into six control families. Please evaluate how effectively the students identified gaps in these areas.

1. Access Control (AC)

How well did the assessment identify gaps in our current practices? On a scale 1 (poor) to 5 (excellent): ___

Which specific controls in this family do you feel need immediate improvement?

---

2. Identification and Authentication (IA)

How well did the assessment identify gaps in our current practices? On a scale 1 (poor) to 5 (excellent): ___

Which specific controls in this family do you feel need immediate improvement?

---

3. Media Protection (MP)

How well did the assessment identify gaps in our current practices? On a scale 1 (poor) to 5 (excellent): ___

Which specific controls in this family do you feel need immediate improvement?

---

4. Physical Protection (PE)

How well did the assessment identify gaps in our current practices? On a scale 1 (poor) to 5 (excellent): ___

Which specific controls in this family do you feel need immediate improvement?

---

5. System and Communications Protection (SC)

How well did the assessment identify gaps in our current practices? On a scale 1 (poor) to 5 (excellent): ___

Which specific controls in this family do you feel need immediate improvement?

---

6. System and Information Integrity (SI)

How well did the assessment identify gaps in our current practices? On a scale 1 (poor) to 5 (excellent): ___

Which specific controls in this family do you feel need immediate improvement?

Section C – Educational Outcomes

Please evaluate, circle the statement which reflects the educational value of this engagement for your business and the students.

Outcome: I now understand the basic cybersecurity hygiene required for CMMC Level 1.

Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree

---

Outcome: The students demonstrated adequate technical knowledge during the assessment.

Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree

---

Outcome: The gap analysis provided actionable insights for improving our security posture.

Statement: Strongly Disagree Disagree NeutralAgree Strongly Agree

Section D – Overall Satisfaction & Recommendations

Overall Rating of the Assessment Experience: On a scale 1 (poor) to 5 (excellent): ___

How likely are you to recommend this university clinic service to other SMBs in the defense sector? On a scale 1 (not likely) to 5 (likely): ___

Additional Comments or Recommendations:

Signature: _____ Date: _____

APPENDIX C

Sample CCP Course Syllabus

Course Syllabus
Introduction to CMMC and CCP Training

Course Number: CYBS 4XXX / 5XXX
Credit Hours: 3
Format: Lecture + Lab + Clinic
Prerequisites: Foundations of Cybersecurity, Network Security, or instructor permission

Course Description

This course prepares students to perform cybersecurity assessments under the Department of Defense Cybersecurity Maturity Model Certification (CMMC) framework. Students learn the regulatory environment, assessment methodology, and technical security practices required to support CMMC Level 1 self-assessments across Defense Industrial Base (DIB) organizations. This course meets the training goals established for the Certified CMMC Professional (CCP) certification by Cyber AB, as well as regulatory standards outlined in DFARS 252.204-7012 and NIST SP 800-171. Students complete a simulated assessment of a mock defense contractor environment and produce assessor-grade documentation.

Course Learning Outcomes

By the end of the course students will be able to:

1. Explain the purpose and structure of CMMC and the Defense Industrial Base ecosystem
2. Interpret federal cybersecurity requirements affecting contractors
3. Identify Controlled Unclassified Information (FCI) boundaries
4. Evaluate implementation of NIST 800-171 security requirements
5. Conduct evidence-based cybersecurity assessments
6. Produce compliant assessment artifacts (SSP, POA&M, evidence)
7. Participate in a mock CMMC Level 1 assessment as an assessor team member
8. Apply professional ethics and conflict-of-interest rules for assessors

Required Materials

- CCP Field Guide and Exam Prep Manual, 2nd Edition, ISBN: 1736881019

Primary Standards:

- NIST SP 800-171
- NIST SP 800-171A
- CMMC 2.0 Model Overview
- DFARS 252.204-7012
- CMMC Assessment Process (CAP) Guide
- CMMC Scoping Guides (Level 1 & 2)
- CMMC-AB Code of Professional Conduct
- NIST SP 800-53r5

Grading Structure

Component	Weight
Weekly Labs	20%
Quizzes	10%
Midterm Exam	15%
Assessment Practicum	25%
Final Assessment Report	30%

Students work in assessment teams simulating an audit engagement.

Weekly Schedule

Module 1 — The Defense Cybersecurity Ecosystem
Week 1: DoD cybersecurity regulation and supply chain risk
Week 2: Contract clauses, FCI, CUI, and data flow mapping

Module 2 — CMMC Framework & Assessment Methodology
Week 3: CMMC levels and certification structure
Week 4: Assessment scope & boundaries
Week 5: Evidence types and interview techniques

Module 3 — NIST 800-171 Security Requirements
Week 6: Access Control (AC)
Week 7: Identification & Authentication (IA)
Week 8: System & Communications Protection (SC)
Week 9: Incident Response (IR)

Module 4 — Documentation & Artifacts
Week 10: System Security Plan (SSP) development
Week 11: POA&M creation and risk scoring
Week 12: Policies vs procedures vs implementation

Module 5 — Assessment Practicum (Clinic)
Week 13: Mock interviews
Week 14: Evidence review & scoring
Week 15: Final findings briefing

Major Assignment — Mock CMMC Final Assessment Report
Students perform a full Level 1 style evaluation:
Deliverables:

- Assessment Plan
- Interview notes
- Evidence review worksheets
- SSP evaluation
- POA&M
- Executive briefing