



National Centers of Academic Excellence in Cybersecurity
NCAE-C 2024
Program Validation Requirements and Application Process
For
Cyber AI Programs of Study (CyberAI)

Prepared by the
Application Process and Adjudication Rubric (APAR)
CyberAI Working Group (CyberAIWG)

December 2024

[20241211_CAE2024_CyberAI_PoSValidation_Requirements_Draft3](#)

This publication was partially supported by the National Science Foundation through the CyberCorps program DGE#1663184 at Towson University and by the CAE Community at the California State University, San Bernardino (CSUSB), under National Security Agency (NSA) award number H98230-22-1-0316

OVERVIEW

The following is an overview of the requirements for validation of a **CyberAI** Program of Study (PoS) in the National Centers of Academic Excellence in Cybersecurity (NCAE-C) programs administered by the National Security Agency (NSA). **The program of study validation requires the institution to hold a current CAE Cyber Defense (CAE-CD) or a CAE Cyber Operations (CAE-CO) designation given that these designations include first the PoS Validation process, which follows the same process as outlined in this CyberAI PoS Validation.** The **CyberAI** PoS validation is awarded to CAE-CD or CAE-CO designated institutions offering cybersecurity-related degrees including majors, minors, and/or certificates at the associates, bachelor's and graduate levels. The goal of the NCAE-C program is to promote and support quality academic programs of higher learning that help produce the nation's cyber workforce.

DRAFT

TABLE OF CONTENTS

Overview.....	i
Table of Contents.....	ii
Introduction to the NCAE-C CYBERAI Program Validation Process.....	1
Justifications	1
Definitions.....	2
PROGRAM OF STUDY (POS) VALIDATION REQUIREMENTS for CYBERAI	3
Overview.....	3
Self-Study Overview.....	3
Institution Details.....	4
Program(s) of Study (PoS) Validation Requirements	5
1. PoS Curriculum.....	5
2. Students.....	8
3. Faculty Members	9
4. Continuous Improvement.....	10
Appendix 1 – Required and Optional Knowledge Units list for Security of AI Program (aka SecureAI) & AI for Cybersecurity Program (aka AICyber).....	12
Appendix 2 – Examples of CyberAI PoS Validation Requirements.....	13
Application Process and Adjudication Rubric (APAR) - CyberAI Working Group (CyberAIWG)	22

INTRODUCTION TO THE NCAE-C CYBERAI PROGRAM VALIDATION PROCESS

CAE-AI Program of Study (PoS) Validation: Following approval of a checklist, the process will begin with the submission of elements pertaining to the academic program of study, including curriculum, student-related information, faculty profiles and qualifications, and continuous improvement information. There are two CyberAI program validation criteria - (1) Security of AI (SecureAI) and (2) AI for Cybersecurity (AICyber). This process and timeline apply to either application for Program of Study (PoS) Validation.

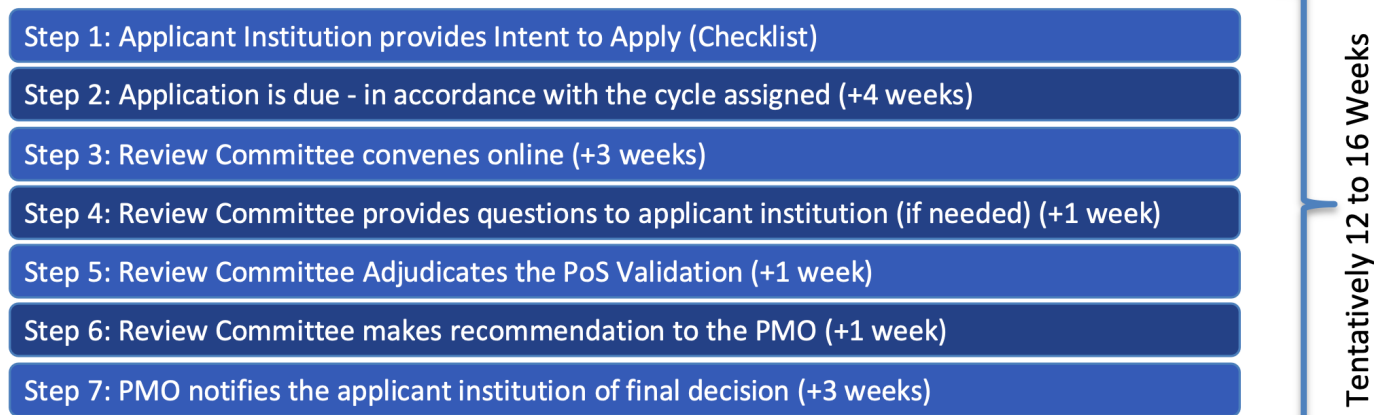


Figure 1. Tentative PoS Validation Application Process and Timeline

Timelines for submission will be published by the CAE Candidates National Center and are distributed throughout the year. The program office will make available an automated application tool to collect all required documentation and data. Applying institutions will be assigned to a submission cycle and expected to follow the deadlines indicated in the cycle timeline provided. Institutions that miss their cycle deadline(s) may be removed from applicant processing and the institution would need to resubmit a checklist to express their interest in continued processing.

Qualified cyber professionals and Subject Matter Experts from NCAE-C Academic Institutions, National Security Agency (NSA), Cybersecurity and Infrastructure Security Agency (CISA), Federal Bureau of Investigation (FBI), and other government partners will assess applications. By submitting an application, an institution grants consent to having its application reviewed by assessors approved by the NCAE-C PMO. Institutions not fully meeting all requirements, will be provided with a set of questions and/or further clarification requests and given an opportunity to respond to the Review Committee's questions, and if needed the Point-of-Contact (POC) will be asked to appear before the Review Committee for further clarifications, followed by a final notification from the PMO (See Figure 1). Each PoS will need to have a designated POC, which may or may not be the same individual and may or may not be from the same academic unit or department. The first POC from each academic institution submitting a PoS for Validation is expected to mentor additional POCs (if applicable) from that same academic institution on PoS validation requirements. Given that all currently applying CyberAI academic institutions are required to hold a NCAE-C Designation (either CAE-CD or CAE-CO), the NCAE-C POC should serve in that capacity and be kept aware of all newly submitted PoS for Validations. The PMO will not provide multiple mentors to an institution and expects that POC to 'lead-by-example' also within their institution. Incomplete applications will be returned without comment.

Justifications

Throughout the CyberAI PoS Validation application process applicant institutions are provided an optional feature in the application tool to attach a justifications file (in one PDF) that they deem needed to clarify issues during the review process.

Definitions

An **institution** is a U.S. legal entity authorized to award associate degrees or higher. All institutions applying to the NCAE-C program must be a U.S. institution of higher education and hold current regional accreditation as outlined by the U.S. Department of Education (<https://www.ed.gov/accreditation>).

An **academic unit** operates within an institution offering associate degrees or higher and depends on the institution for authority to grant degrees and for financial, human, and physical resources.

A **program of study (PoS)** is a defined series of elements that leads to the completion of a degree, a certificate or other defined set of outcomes by the institution.

An **example** is defined as a characteristic or set of characteristics to illustrate a requirement or set of requirements. Examples provided in this document were not intended for the purpose of replication rather as a general illustration of how the required information can be presented.

An institutional **Point-of-Contact (POC)** is a designated full-time/permanent faculty member of the institution directly involved with the representative academic program from the applying institution who will serve as the liaison between the institution and the NCAE-C Program Management Office (PMO). This person will be contacted by the PMO and/or the National Centers for all NCAE-C program updates, grants and scholarship opportunities, upcoming events, and other administrative communications. This person is responsible for the Annual Report, Re-designation, and any other important milestones in the institution's NCAE-C participation.

An institutional **Alternate POC** is an individual who is a full-time/permanent employee in a professional capacity (not an administrative assistant personnel) and is a secondary contact to the POC. This person may be a Department Chair, an Associate Dean, a Center or Program Director, or a Dean.

Security for AI (aka SecureAI) refers to securing AI systems and infrastructure throughout their lifecycle.

AI for Cybersecurity (aka AICyber) refers to leveraging AI to support traditional cybersecurity.

Program-Level Learning Outcomes are a description of what graduates should know or be able to do upon completion of the program of study. Combined, these serve as a key measure of graduates' success from the program of study and should be assessed by the identified program outcomes assessment indicators. Each Program of Study should have multiple Program-Level learning outcomes that are consistent with the needs of the program's focus and various constituencies.

A **program outcome assessment indicator** (assessment metric) is a measure conducted by a faculty member of students' academic performance, student growth, and/or other measure of students' performance of one or more Program-Level learning outcome(s).

Curriculum Map and Plan (Noted in green in Figure 2): documentation of how the PoS courses are mapped to the Program-Level learning outcomes, and documentation of the courses where program outcome assessment indicators provide evidence for the Program-Level learning outcomes.

A **Knowledge Unit (KU)** is a thematic grouping that encompass multiple, related KU outcomes and learning topics.

A **Knowledge Unit (KU) outcome** is a specific assessment of a concept associated with a particular KU.

Course outcomes are the expectations that the academic institution and the PoS is anticipating students to be able to demonstrate when completing a course.

KU Alignment (Noted in purple in Figure 2): the process of documenting how the KUs and KU outcomes are aligned to the relevant courses in the PoS.

Continuous Improvement (Noted in blue in Figure 2): documentation of a plan, a process, and a regular evaluation schedule that an academic institution and/or academic unit have to enhance the overall quality of its PoS.

Continuous Improvement Plan: documentation of a structured set of actions the academic institution and/or academic unit plans to perform to enhance the overall quality of its PoS.

Continuous Improvement Process: documentation of the continuous improvement plan executed and evaluation of the results of the current continuous improvement plan.

Continuous Improvement – Regular Evaluation Schedule: periodic evaluation of the continuous improvement process documentation and assessment metrics to enhance the overall quality of the PoS.

PROGRAM OF STUDY (POS) VALIDATION REQUIREMENTS FOR CYBERAI

Overview

The Program of Study (PoS) Validation requirements for NCAE-C – CyberAI programs include evidence of Self-Study that all academic institutions will submit in the application tool. Academic institutions will be required to outline faculty, student, curriculum, and continuous improvement information. In addition, any PoS being submitted for validation must have Program-Level Learning Outcomes identified and on file at the submitting institution, preferably on the program's website/webpage. Those Program-Level Learning Outcomes will then be *mapped* to the courses in the PoS. Moreover, the Self-Study will include documentation of the identified KUs for the PoS and the *alignment* of the KUs to the relevant courses in the PoS. Figure 2, the CyberAI PoS Validation Conceptual Model, provides a graphical representation of the: (1d) Curriculum Map and Plan courses with associated documentation, the (1e) KU alignment courses, and (4) Continuous improvement plan, process, and evaluation schedule. The examples provided are to be used as illustration or guide, they are not intended to be a complete assessment of a PoS. No elective courses should be indicated in the KU alignment, as all students should take all courses indicated in the KU alignment.

Self-Study Overview

Self-study is required of all CyberAI Programs seeking PoS Validation. It includes the following requirements (See Appendix 2 for relevant examples):

1. PoS Curriculum

- a) The Cybersecurity PoS Offered by the Institution
- b) NICE Framework/DCWF Work Role Crosswalk Alignment
- c) Courses Syllabi and Courses Requiring Applied Lab Exercises (For KU Aligned Courses Only)
- d) Curriculum Map and Plan with Assessment Documentation
- e) Knowledge Units (KUs) Alignment (See Appx. 2)

2. Students

- a) Student enrollment/graduation in the PoS(s)
- b) Sample student certificate/notation on transcript/official letter (if program has graduated students)
- c) Students' work products (papers, assignments, labs, etc.)
- d) Student participation in extracurricular activities

3. Faculty Members

- a) Cyber Program(s) of Study PoC
- b) Full-time, part-time, and adjunct faculty members + Faculty qualifications (publications, research, industry involvement, certifications, etc.) related to PoS type
- c) Faculty support of enrolled students
- d) Process of Faculty Promotion/Reappointment (e.g. Faculty Policy Manual)

4. Continuous Improvement

- a) Continuous Improvement plan
- b) Continuous Improvement process
- c) Regular evaluation schedule

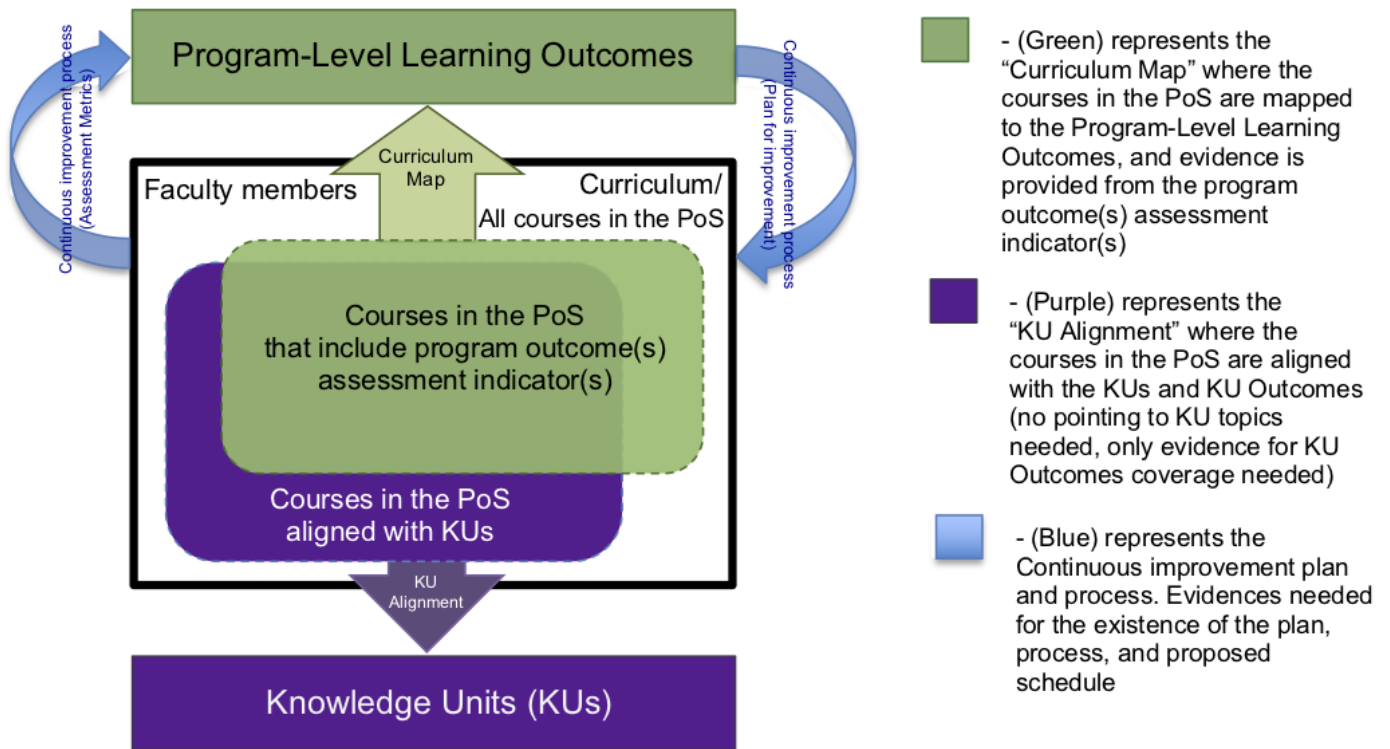


Figure 2. PoS Validation Conceptual Model

Institution Details

The applicant will identify and/or confirm the official initial institution details in the application tool.

Requirements:

- Identify/confirm the official institution name
- Provide link to the homepage of the institution (not department)
- Provide the address of the institution

Additional Information for Grant Related Opportunities (Not guaranteed):

Applying academic institutions are highly encouraged to provide further evidence of eligibility for NSA grants for the benefit and ease of applying for grants. Doing so will allow NSA to identify potential NCAE-C institutions for grant solicitations. Specifically, applicants may need to consult their Office of Sponsored Programs, Research Office, the office which will handle any grant submission for the institution, or other entity that administer their grants to obtain a copy of the most recent A-133 Summary of Auditor's Results, DUNS, Cage Code, and Employer Identification Number/Tax Identification Number (TIN#) to ensure the correct numbers are being provided. This same office/entity may have the proof of the most recent A-133 Summary of Auditor's Results, SAM and ARC registrations (Proof of SAM and ARC registrations may be a simple email from the organization, or a screenshot of the registration).

Information Needed (Optional):

- Provide a copy of the most recent A-133 Summary of Auditor's Results (in PDF)
- Provide the DUNS number
- Provide the CAGE Code
- Provide the Employer Identification Number/Tax Identification Number (TIN#)
- Provide proofs of the SAM and ARC registrations (in PDFs)

Program(s) of Study (PoS) Validation Requirements

1. PoS Curriculum

A U.S. institution of higher education will apply by submitting an academic program for Program of Study (PoS) validation. The academic institution must show its curriculum and show that students are enrolled and can successfully complete the path and receive recognition. A single academic institution may have multiple PoSs validated. All institutions applying for PoS validation must be a U.S. institution and regionally accredited.

PoS is defined as sets of courses that are designed to develop Program-Level learning outcomes in the student population over time. It is possible to have multiple cybersecurity PoSs at an academic institution, in different departments, producing students with different knowledge and skills. Degree plans or Program plans can document the options available to a student and form a basis for determining the correct path. Program sequence diagrams that define the relationship between courses (prerequisites) can be useful in assisting students as they navigate the classes. Cohorts are another mechanism that can assist in navigation of program plans. Transcripts, or other institutional completion records, can document student completion of validated PoS.

a. The Cyber AI PoS offered by the institution

The applicant will identify the official name of the CyberAI PoS offered by the institution and the academic leadership relevant to that PoS. Courses identified in the *Curriculum Map and Plan* as well as the *KU Alignment* must be mandatory for all students completing the PoS. If the application is approved, only the PoS identified in this criterion is allowed to be marketed as a validated PoS. Applicants may not refer to NCAE-C until the applicant receives official approval. To initiate the application, applicant will first need to identify if the CyberAI PoS is a *SecureAI* or *AI/Cyber* (refer to section 1e for proper KU alignment) and state the official name of the cybersecurity PoS.

Requirements (All needed):

1. State the official name of the CyberAI PoS (including degree level, if applicable, minor, concentration, certificate). If validated, the PoS name will be displayed on a NCAE-C website list, thus, it must be the official name (Examples: AAS in Computer Technology with a Cybersecurity Certificate; BS in Cybersecurity; BS in Computer Science with CyberAI track; MS in AI with concentration in Cybersecurity; Ph.D. in AI). ***State **only** the official PoS curriculum name. The text provided will be printed on the validation certificate, if approved. Do NOT include any other text aside from the official PoS curriculum name in this field ***
2. Provide a link to the institutional site where the PoS is documented (i.e. link to program's course catalog, curriculum webpage, etc.).
3. Identify department(s) official name(s) as it appears in the accreditation where PoS resides.
4. Academic institutions applying for the validation will affirm that PoS curriculum is in existence.
5. Identify the administrative head of the academic unit housing the PoS (Dean, Associate Dean, Department Chair, etc.) including name, phone number, and e-mail address.
6. List all courses that are part of the PoS Curriculum Map and Plan – i.e. courses that are used to assess the Program-Level Learning Outcomes (Course Number/Course Name/Course Descriptions as appears in catalog, excluding General Education courses) and all courses that are part of the KU alignment (identify the KU aligned courses in the list).
7. Provide evidence for PoS Curriculum Sheet in PDF (See Appendix 2 - Example 1a).

b. Cybersecurity Work Roles Crosswalk Alignment

The applicant will state the cybersecurity PoS crosswalk alignment through the identification of cybersecurity work roles. To better assist both graduates of NCAE-C Validated PoSs and hiring managers from industry and government, it is important that the applicant institution will identify the cybersecurity work roles that are

most relevant to their applying PoSs. Such crosswalk alignment will enable explicit declaration of the focus of graduates produced by the PoSs to address the bridge between education and employment. The cybersecurity work roles crosswalk alignment also enables the capabilities to further sharpen the relevant competencies of the PoS graduates in alignment with industry and government needs. The Workforce Framework for Cybersecurity (NICE Framework) (NIST Special Publication 800-181, Revision 1 <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-181r1.pdf>) outlines 52 cybersecurity work roles. Additionally, the Department of Defense (DoD) Cyber Workforce Framework (DCWF) (<https://dodcio.defense.gov/Cyber-Workforce/DCWF/>) outlines over 70 cyber-related work roles. By identifying and selecting each work role, the applying institution indicates in their submitted PoS that their graduating students fit the work roles identified and that graduates acquire the knowledge as well as demonstrate the competencies associated with those work roles. While an applying institution may consider its PoS to produce graduates in many work roles, this criterion calls for the work roles that are the most relevant to that PoS. The identified cybersecurity work roles crosswalk alignment should also be evident by the type of courses (curricular experiences), as well as other co-curricular and extracurricular experiences that students are exposed to at the PoS. By providing students with clearly selected topmost aligned cybersecurity work roles to the PoS, institutions assist students in inspiring their career choices, preparing them for job interviews, the work recruitment process, and increasing their competitiveness in the marketplace.

Requirement:

1. Identify the top three most relevant work roles that are aligned with the cybersecurity PoS submitted. Work roles identified shall be selected from the NICE Framework and/or the DCWF. Any of the three cybersecurity work roles identified can only be from the NICE Framework and/or the DCWF.

c. Course Syllabi and Courses Requiring Applied Lab Exercises (For KU Aligned Courses Only)

The applicant will provide syllabi of all courses in the KU Alignment (See section 1e below) and identify those that require applied lab exercises (hands-on) that develop competencies in the CyberAI domain, provide lab exercises guidelines and highlight lab requirements in the syllabus. A typical course syllabus includes the official name and number of the course, the term it is offered, who teaches the course, the textbook(s) assigned if any, relevant course information (course descriptions, course learning outcomes, etc.), supplemental material (if applicable), course topic coverage outline and/or a weekly/module schedule to indicate list of lectures, topics/reading, assignments, labs assigned, course grade components, and grading scale/system.

Requirements (All needed):

1. Provide a concise syllabus of each course in the KU Alignment (all must be from the last three years) (in PDF).
2. For KU aligned courses that require applied labs exercises (i.e. hands-on labs that develop competencies) in the CyberAI domain, highlight the lab(s) on the syllabus, and highlight in which unit/week the lab(s) are required for the lab(s) provided (all must be from the last three years).
3. Provide the guidelines (i.e. what students are asked to do) of one lab exercise from each course that requires applied lab exercises and indicate within the guidelines the course that each lab is used (all must be from the last three years) (in PDF).

d. Curriculum Map and Plan with Assessment Documentation

Program-Level Learning Outcomes are the basis for determining the effectiveness of a NCAE-C program in developing the cybersecurity workforce. Each PoS should have a defined set of Program-Level Learning Outcomes as documented by the academic institution to the regional (or other) accreditation. The number of Program-Level Learning Outcomes may vary depending on the academic institution and level of the program. The Program-Level Learning Outcomes are the basis for continuous improvement efforts. No elective or optional courses should be included in the Curriculum Map and Plan, as all students should take all courses used to assess the Program-Level Learning Outcomes.

Requirements (All needed):

1. State the Program-Level Learning Outcomes of the PoS.
2. Provide documentation of the Program-Level Learning Outcomes (link to academic institutional webpage with the outcomes and/or PDF document of the outcomes).
3. Provide evidence for the Program-Level Learning Outcomes *Curriculum Map and Plan* that identified the PoS courses where the outcomes are assessed (Combined to single PDF) (See Appx. 32 example 1d1).
4. Provide documentation for the *General Information* for each Program-Level Learning Outcome (Combined to single PDF). For each Program-Level Learning Outcome, "General Information" documentation provided should include: (a) The stated Program-Level Learning Outcome; (b) Term it was assessed; (c) Course used for the assessment; (d) Total number of assessed students (See Appx. 32 example 1d2).
5. Provide documentation for the *Assessment of Indicators* for each Program-Level Learning Outcome (Combined to single PDF). For each Program-Level Learning Outcome, "Assessment of Indicators" documentation provided should include: (a) The stated Program-Level Learning Outcome; (b) Course used for the assessment; (c) Program outcome assessment indicator(s) used to assess the Program-Level Learning Outcome (assessment metric(s)); (d) Performance expectations; (e) Average assessment score for the assessed students; (f) overall performance rating of assessed students (See Appx. 32 example 1d3).
6. Provide documentation for the *Overall Assessment Information* of each Program-Level Learning Outcome (Combined to single PDF). For each Program-Level Learning Outcome, "Overall Assessment Information" documentation provided should include: (a) The stated Program-Level Learning Outcome; (b) Course used for the assessment; (c) Program outcome assessment indicator(s) used to assess the Program-Level Learning Outcome (assessment metric(s)); (d) Overall performance rating of assessed students; (e) Qualitative analysis of the assessment results; (f) Qualitative statement/plan for improvement(s) resulting from the assessment; (g) Indication of when the recommended improvement(s) are projected to be implemented (See Appx. 2 example 1d4).

e. Knowledge Units (KUs) Alignment

The NCAE-C program will rely upon the institutional accreditation for sufficiency of program construction and maintenance. Courses, or other academic elements, should be institutionally approved per the institutional requirements for accreditation and aligned to the KUs. The PoS content as demonstrated by KU alignment will be used to determine if the courses together as a whole constitute sufficient material in quantity and form. All CyberAI programs need to cover the foundational, appropriate core, and required elective KUs as indicated in Figure 3. No elective or optional courses should be included in the KU alignment, as all students should take all courses indicated in the KU alignment. One course may align with one or more KU(s), however, a course should not be aligned to an excessive number of KUs given the challenge of so many KU Outcomes coverage with a single course. One KU may align to multiple courses; however, this is not recommended. KU alignment is only needed for courses that are identified for alignment with the KUs. Course learning outcomes will also be aligned (as a set) to the relevant KU(s), while the KU Outcomes will be shown (as a set) to provide guidance on the coverage (See Appendix 2 - Example 1e1). As part of the application, the academic institution will provide information on the academic year that each of the KU aligned courses was last offered. Additionally, the academic institution will provide explanations on how they manage multiple sections of the KU aligned courses in some form of equivalency.

Requirements:

1. Provide a narrative on the description of the PoS, explain the overall KU alignment to the PoS.
2. For graduate programs (MS or Doctoral) that seek exemption from any of the KUs, provide evidence that students are admitted with the foundational and core knowledge.
3. Provide the KU Alignment Summary Table for the PoS (in PDF) (See Appendix 2 - Examples 1e2).
4. Identify PoS courses that are part of the KU alignment.
5. Provide *course learning outcomes* for all KU aligned courses as documented in official academic institution documentation (Course catalog, program website, etc.).

6. Provided the academic year each KU aligned course was last offered or is planned to be offered.
7. In the case of multiple sections of a KU aligned course, provide explanation on how they all are managed in some form of equivalency. If no multiple sections are offered, provide a statement to attest to that.

Appendix 1 provides a list of **Required and Optional Knowledge Units for the CyberAI Program**.

Appendix 2 provides an overview and examples of the **KU Alignment Requirements for the CyberAI Program**.

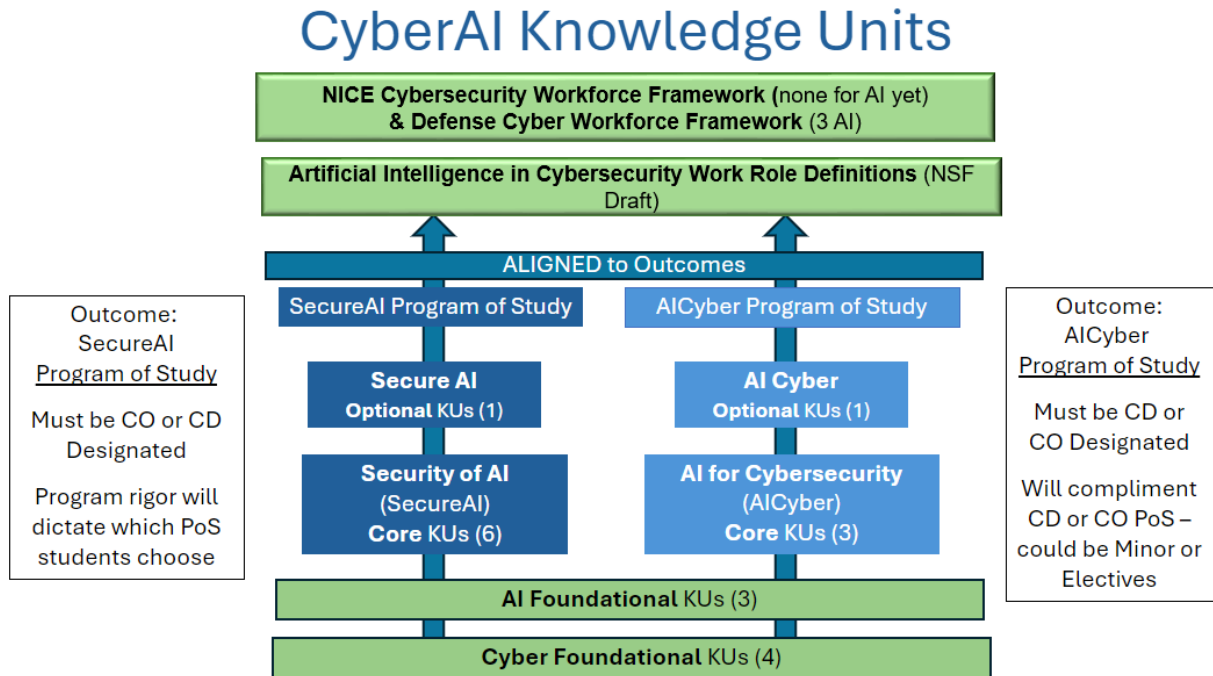


Figure 3. CyberAI Program of Study Model

2. Students

All the following elements should be directly relatable to the defined PoS as documented in the application.

a. Student Enrollment/Graduation in the PoS(s)

Demonstration that a PoS has actual student outputs is an essential part of the application.

Requirements (All needed):

1. Provide student enrollment (unduplicated/headcount) in PoS for the last three years (each year separately).
2. Provide official institutional letters for the enrollment (unduplicated/headcount) and graduation in the PoS for the last three years, each year separately (letter from Registrar, Institutional Effectiveness, or equivalent) (in PDF).
3. Provide at least three (3) redacted student transcripts, showing the student graduated or attended within the last three years and clearly highlight the courses taken that are in the KUs alignment. All KU aligned courses must appear on the transcript.

b. Sample student certificate/notation on transcript/official letter

Graduates from CyberAI validated PoS should receive documentation from the institution recognizing their completion of the NSA Validated PoS and if the academic institution also holds an NSA NCAE-C, recognition should be made for their completion from a PoS that is also under an NSA NCAE-C designated “Center”.

Requirement:

1. Provide a sample certificate, draft of official letter, or proposed notation on transcript to be issued to students completing the PoS indicating they completed the NSA Validated PoS and if the academic institution also holds an NSA NCAE-C, recognition should be made for their completion from a PoS that is also under an NSA NCAE-C designated "Center".

c. Students' Work Products (papers, assignments, labs, etc.)

Sample student work products are important to evaluate the quality and depth of students' work during the PoS. Student work products are (but not limited to): papers, assignments, projects, presentations, lab exercises, test questions.

Requirement (All needed):

1. Provide samples of six students' work products from six different assignments (six files total) within the last three years. Samples can be (but not limited to): papers, assignments, projects, presentations, lab exercises, test questions from at least two courses in the PoS that are in the KU alignment. Student names should be removed prior to submission. Students' work products should not include grades or grading comments, only the original students work. Combine the guidelines (i.e. what students are asked to do) for students' work products, indicate the course and the KU that each is associated with, and one sample student work (name redacted) into a single file for each of the student's work (in six separate PDFs).

d. Student Participation in Extracurricular Activities

Documentation of student participation in extracurricular activities can demonstrate program opportunities for students.

Requirements (All needed):

1. Provide evidence of three student participation in extracurricular activities within the last three years, which may include (but not limited to): experiential learning activities, local/regional/national cyber exercises and competitions, outreach to community colleges and high schools, computer check-up days, summer internship program, industry guest lectures, etc.
2. Provide dates and description for each evidence provided.

3. Faculty Members

Faculty members are the instrument that delivers the PoS content to students via courses and other learning experiences. The cyber AI faculty should have appropriate experience associated with the PoS and courses they are assigned. The NCAE-C program will rely upon the institutional accreditation process to determine the correct credentials to be a faculty member. An examination of faculty members' curriculum vitae (CV) or resume as part of the review process can determine the appropriate level of cybersecurity experience, knowledge, and preparation. A portion of the faculty responsible for the program is required to be full-time members teaching at the PoS, with the remainder being adjuncts or part-time. The institution's accreditation-based documentation for faculty academic credential qualifications will be the basis for this PoS validation requirement. Faculty members must support enrolled students by serving as mentors or advisors to student-led activities, and by participation or sponsorship of CyberAI exercises and competitions (including in-class competition) within the last three years. Evidence must include links to student clubs, cyber defense exercises, link to team roster on a competition website, link to social media about the exercise, or other forms of official acknowledgement that include a full description of the activity, the date, and the nature of the participation.

Requirements (All needed):

1. Identify the Point-of-Contact (POC) for the PoS (a full-time/permanent faculty member of the institution directly involved with the representative academic program) including name, phone number, and e-mail address. The POC is expected to take full responsibility and provide support for the validation. This means ensuring programs are fully supported by the institution long term. Note: This will be the person who will

be contacted by the PMO and/or the National Centers for all NCAE-C program updates, grants and scholarship opportunities, upcoming events, and other administrative communications.

2. Identify the Alternate POC for the PoS. The individual assigned to this role is one whom is a full-time/permanent employee in a professional capacity (not an administrative personnel) and is a secondary contact to the POC.
3. Identify all faculty members in the program including name, phone number, and e-mail address, highest degree earned, field and year, academic rank, type of academic appointment (Tenure Track, Tenured, Continuing Contract, Non-Tenure Track, etc.), full-time, part-time, or adjunct status, and years of academic experience.
4. Provide a CV or resume for each faculty member teaching course(s) in the KU alignment with their cybersecurity or related qualifications identified. These CVs should be abbreviated to up to four pages each to address necessary elements including maintenance of currency, publications, research, industry involvement, Continuing Professional Education (CPE), publications, presentations, certifications, workshops attended, professional registration and/or certification (if applicable), level of activity in professional organization, professional development, and consulting or summer work in industry (high, medium, or low) (One PDF per faculty member teaching course(s) in the KU alignment, 10 max).
5. Provide evidence for faculty members support of enrolled students by serving as mentors or advisors to student-led activities, and by participation or sponsorship of cybersecurity exercises and competitions (including in-class competition) within the last three years. Evidence must include link(s), such as: link to student clubs, link to cyber defense exercises, link to team roster on a competition website, link to social media about the exercise, or other forms of official acknowledgement that include a full description of the activity, the date, and the nature of the participation (all links and evidence information provided within a single PDF).
6. Provide evidence for institutional process of faculty promotion/reappointment (e.g. Faculty Policy Manual) (in a single PDF).

4. Continuous Improvement

A key element to ensure vitality and functionality over time is a strong continuous improvement plan, process, and regular evaluation schedule. A process-driven continuous improvement plan directed at the Program-Level Learning Outcomes is an essential element of the program. At regular academic intervals, selected Program-Level Learning Outcomes should be assessed by an analysis of student work via the learning outcome assessment indicators to demonstrate whether attainment of defined levels of performance is being achieved. This is done by assessing specific elements of student performance against defined rubrics to demonstrate student level of achievement. This is not just using course grades, but rather a granular analysis of specific assignments that demonstrate competence associated with the defined Program-Level Learning Outcomes. For each Program-Level Learning Outcome item, a defined set of student work elements will be identified, associated rubrics developed to score them defined, and a desired standard of student achievement defined. Then, student work will be scored to see if the program is meeting the desired level of attainment for each of the Program-Level Learning Outcomes. As a normal part of the process, one or more steps should be initiated to improve the Program-Level Learning Outcomes over time. The changes will be evaluated at a future assessment period. All the associated process improvement activities should be driven by the faculty associated with the PoS, not by random individual actions. Records of the assessments, the process, and the documented plans for improvement, should be kept and submitted as part of the annual reports and re-designation. Documentations for continuous improvement plan, process, and regular evaluation schedule are expected to match those that the academic institution files with their accreditation body(ies).

a. Continuous Improvement Plan for the PoS

The *Continuous Improvement Plan* for the PoS commonly includes four parts that the academic institution and/or academic unit documents to enhance the overall quality of its PoS:

- 1) Strategic process planning goals for the PoS
- 2) The Program-Level Learning Outcomes for the PoS

- 3) Description of the assessments of the Program-Level Learning Outcomes
- 4) Proposed changes to enhance the quality of the PoS

Requirement:

1. Provide documentation of a Continuous Improvement Plan for the PoS (in PDF).

b. Continuous Improvement Process for the PoS

The *Continuous Improvement Process* commonly includes the four parts of the plan indicated above with a clearly identified end of a given process cycle (See Figure 4). Evidence must be provided of specific improvement efforts linked to assessment of the designated metrics. An institution should be prepared to adjust the process upon completion of a Continuous Improvement Process cycle.

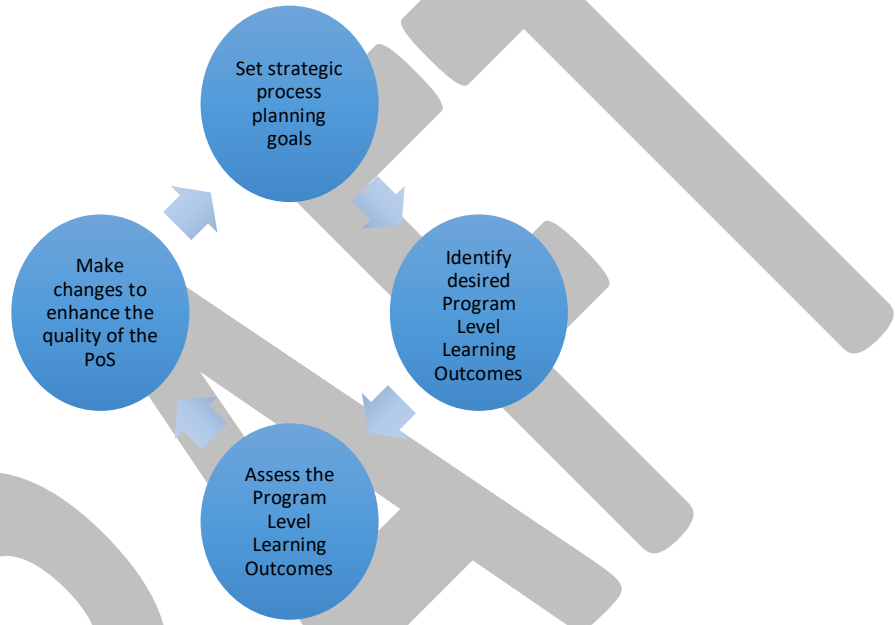


Figure 4. Continuous Improvement - Regular Evaluation Cycle

Requirement:

1. Provide documentation of the Continuous Improvement Process with specific improvement efforts linked to assessments (in PDF).

c. Continuous Improvement - Regular Evaluation Schedule for the PoS

Continuous Improvement - Regular Evaluation Schedule for the PoS may include (but not be limited to) a quarterly (or monthly) curriculum committee meeting set to evaluate the Program-Level Learning Outcomes, the assessment indicators, all other metrics, discussing the continuous improvement plan and process along with adjustments needed.

Requirement:

1. Provide documentation of the Continuous Improvement - Regular Evaluation Schedule (in PDF).

APPENDIX 1 – REQUIRED AND OPTIONAL KNOWLEDGE UNITS LIST FOR SECURITY OF AI PROGRAM (AKA SECUREAI) & AI FOR CYBERSECURITY PROGRAM (AKA AICYBER)

Both program of studies has the same Cyber Foundational and AI foundational KUs:

(4) Cyber Foundational KUs (all required): IT Systems Components (ISC), Cybersecurity Foundations (CSF), Basic Scripting and Programming (BSP), and Math Fundamentals (MAF).

(3) AI Foundational KUs (all required): AI Governance, Laws, and Ethics (AIG), AI Fundamentals (AIF), Machine Learning Fundamentals (MLF).

The **Core KUs** are central to the design and focus of each program of study. They build on the foundational KUs to establish the specialized skills and knowledge necessary for success in the chosen field. Each program tailors its core KUs to address specific objectives, ensuring alignment with the program's goals.

(6) Core KUs for SecureAI program: This program is dedicated to protecting AI systems and ensuring their integrity, resilience, and reliability throughout their lifecycle. It requires **six core KUs**, reflecting a comprehensive focus on safeguarding AI technologies.

(3) Core KUs for AICyber program: This program focuses on applying Artificial Intelligence (AI) techniques to enhance cybersecurity. It requires **three core KUs**, which form the foundation for leveraging AI to detect, assess, and mitigate cyber threats.

Both programs of study require alignment with Core Knowledge Units (KUs) to ensure consistency and specialization. **Associates and bachelor's programs** must align their courses with the Core KUs of either SecureAI or AICyber. **Graduate programs**, however, have flexibility in meeting these requirements. They can either align their curriculum to the Core KUs or document a system to verify that incoming students have met the Foundational and Core KUs through prior coursework or professional experience. Institutions may use systems for evaluating students' readiness or require completion of specific courses and experiences during the program to address any gaps. This structure ensures that all students, regardless of their entry point, are equipped with the necessary expertise to succeed in their chosen program of study.

The six **Security of AI** Program (aka SecureAI) **core** KUs are:

- Computer Science Foundations (from CAE-CO) (COF)
- Advanced Math for AI (AVM)
- Securing the AI Lifecycle (AIL)
- Machine Learning Algorithms (MLA)
- Deep Learning (DPL)
- Adversarial Learning (ADL)

The three **AI for Cybersecurity** Program (aka AICyber) **core** KUs are:

- Basic Networking (from CAE-CD) (BNW)
- Network Defense (from CAE-CD) (NDF)
- AI for Security Assessment (AIS)

(1) Optional KUs (2 to choose from for each program) one must be adopted by the corresponding program to complete their program of study.

The two Security of AI Program (aka SecureAI) **optional** KUs are:

- Model Selection, Evaluation, and Specification (MES)
- Risk Management of AI (AIR)

The two AI for Cybersecurity Program (aka AICyber) **optional** KUs are:

- Defensive Applications of AI (DFA)
- Offensive Applications of AI (OFA)

The latest KUs are available at <https://public.cyber.mil/ncae-c/documents-library/>.

APPENDIX 2 – EXAMPLES OF CYBERAI POS VALIDATION REQUIREMENTS

Example for requirement 1a: PoS Curriculum Sheet (SecureAI):

Master of Science | Curriculum | Total Credits: 30

Students must take all 10 required courses. Students who wish to take an elective (above the 10 required courses) must request approval from the program office before registration.

- **SEC 500** Python Programming for AI
- **SEC 501** Advanced Mathematics for AI
- **SEC 502** Computer Systems and Architectures
- **SEC 577** Intro to Cybersecurity
- **SEC 503** Introduction to Machine Learning
- **SEC 680** Securing the AI Lifecycle
- **SEC 620** Deep Learning Applications
- **SEC 640** Adversarial Learning Techniques
- **SEC 650** Ethical and Secure AI Development
- **SEC 660** Risk Management of AI Systems

DRAFT

Example for requirement 1a: PoS Curriculum Sheet (AICyber):

Master of Science (M.S.) in Artificial Intelligence Cybersecurity | Curriculum

ARTIFICIAL INTELLIGENCE CYBERSECURITY

MASTER OF SCIENCE (M.S.)

Curriculum

PREREQUISITE COURSES

			Credits
CISC	501	Computer Organization and Architecture	3
CISC	502	Mathematics in Computing	3
CISC	503	Data Structures and Algorithms	3
MSIT	501	Foundations of Programming, Data Structures, and Algorithms	3

CORE COURSES (30 credits)

CISC	650	Computer Networks	3
CISC	670	Artificial Intelligence	3
ISEC	615	Fundamentals of Cybersecurity	3
ISEC	640	Database Security	3
ISEC	660	Advanced Network Security	3
ISEC	675	Information System Auditing	3
ISEC	692	AI Cybersecurity Project	3
MMIS	623	Ethics in Computing	3
MMIS	671	Data Analytics and AI	3
MSIT	675	Deep Learning	3

DRAFT

Example 1 for requirement 1d1: Curriculum Map and Plan:

Program-Level Learning Outcomes Curriculum Map and Plan
 Program Name: BS in AI for Cybersecurity (AICyber)
 Updated: 2024.XX.XX

Program-Level Learning Outcomes: <i>Graduates should be able to...</i>	AIC 210	AIC 290	AIC 202	AIC 336	AIC 377	AIC 461	AIC 440	AIC 450	AIC 418	AIC 481
1. [Program-Level Learning Outcome 1, Ex. "Apply security principles and practices to maintain operations in the presence of risks and threats"]	I	R			R		R	R		A
2. [Program-Level Learning Outcome 2, Ex. "Communicate professionally with customers and co-workers"]		I			R	R	R		R	A
3. [Program-Level Learning Outcome 3, Ex. "Analyze and design AI-driven systems and applications"]	I	R		R		R	R			A
4. [Program-Level Learning Outcome 4, Ex. "Assess and mitigate ethical, legal, and societal concerns of AI in cybersecurity."]							I	R	R	A
5. [Program-Level Learning Outcome 5, Ex. "Develop solutions for detecting, responding to, and mitigating cyber threats using AI techniques."]					I	R	R	R		A
6. [Program-Level Learning Outcome 6, Ex. "Demonstrate proficiency in programming, data analysis, and machine learning for cybersecurity applications."]	I	R	R	R		R				A

I, R, and A indicate the courses in which each Program-Level Learning Outcome is: introduced (I), reinforced (R), and formally assessed (A). The number of Program-Level Learning Outcomes may vary depending on the academic institution and level of the program.

Example 2 for requirement 1d1: Curriculum Map and Plan:

Program-Level Learning Outcomes Curriculum Map and Plan

Program Name: MS in SecureAI

Updated: 2024.XX.XX

Program-Level Learning Outcomes: <i>Graduates should be able to...</i>	SEC 500	SEC 501	SEC 502	SEC 503	Sec 577	SEC 626	SEC 646	SEC 656	SEC 666	SEC 686
1. [Program-Level Learning Outcome 1, Ex. "Communicate cybersecurity management concepts professionally"]	A1				A1			A2		
2. [Program-Level Learning Outcome 2, Ex. "Develop solutions for securing the AI lifecycle to mitigate risks."]			A1		A1		A1			A2
3. [Program-Level Learning Outcome 3, Ex. "Identify and mitigate vulnerabilities in AI models and pipelines."]			A1		A1		A2			
4. [Program-Level Learning Outcome 4, Ex. "Apply ethical and legal principles in the design of secure AI systems."]								A1		A2
5. [Program-Level Learning Outcome 5, Ex. "Design robust AI models resistant to adversarial attacks."]				A1						A2

A1 and A2 indicate the courses in which each Program-Level Learning Outcome is: formally assessed via Indicator 1 (A1) and formally assessed via Indicator 2 (A2). The number of Program-Level Learning Outcomes may vary depending on the academic institution and level of the program.

Example for requirement 1d2: General information for Program-Level learning outcome

Need to be submitted for each Program-Level Learning Outcome

Date report submitted	12-09-2024
Program faculty who contributed to this report	Dr. Jane Doe
Program-Level learning outcome	Apply AI techniques to design, evaluate, and deploy defensive and offensive cybersecurity strategies.
Course(s) that formally assess(es) this program-level learning outcome (at its highest level, see Curriculum Map and Plan)	AIC 481 Case Studies in Cybersecurity Using AI
Number of students assessed for this program-learning level outcome	30
Quarter/Semester students were assessed (e.g., Winter 2024)	Fall 2025

DRAFT

Example for requirement 1d3: Assessment of indicators for the Program-Level learning outcome (add more rows if necessary)

Can be one or more assessment indicators for each Program-Level Learning Outcome. Need to be submitted for each Program-Level Learning Outcome.

Program-Level Learning Outcome: Apply security principles and practices to maintain operations in the presence of risks and threats					
Course(s) that formally assess(es) this program-level learning outcome: ABC 216 - Industrial Control Systems Security					
Assessment Indicator(s) (taken from rubric)	Teaching and learning activities: List the most significant teaching and learning activities used by program faculty to facilitate the learning of this indicator in their class(es).	Graded assignment(s) that formally assesses each indicator at its highest level	Performance expectations: identify the percentage range for each level of performance by replacing the “xx’s” below	Average score for the indicator as a percent	How well did the students perform? (right-click on the checkbox and select ‘properties’ and ‘checked’)
Malware Detection and Profiling	Students use AI-based tools to detect and analyze malware behaviors. Activities include running malware samples in a controlled sandbox, extracting features, and profiling malware families.	Group Project	Below expected levels: 0 – xx % At expected levels: xx – xx % Above expected levels: xx – 100 %	61%	<input type="checkbox"/> below expected levels <input checked="" type="checkbox"/> at expected levels <input type="checkbox"/> above expected levels
Offensive AI: Crafting Adversarial Examples	Students learn techniques to craft adversarial examples to bypass detection models using hands-on Python lab sessions. These activities are guided by program instructors.	Individual applied (hands-on) lab	Below expected levels: 0 – 70 % At expected levels: 71 – 89 % Above expected levels: 90 – 100%	100%	<input type="checkbox"/> below expected levels <input type="checkbox"/> at expected levels <input checked="" type="checkbox"/> above expected levels
Risk Analysis and Threat Modeling	Students analyze AI-generated security reports and create a threat model for a simulated organization. This includes in-class discussions and group presentations.	Final Report	Below expected levels: 0 – 70 % At expected levels: 71 – 89 % Above expected levels: 90 – 100%	100%	<input type="checkbox"/> below expected levels <input type="checkbox"/> at expected levels <input checked="" type="checkbox"/> above expected levels

Example for requirement 1d4: Overall assessment of a Program-Level learning outcome (please be thorough in all responses). Need to be submitted for each Assessment Indicator(s) in each Program-Level Learning Outcome.

Program-Level Learning Outcome: Apply security principles and practices to maintain operations in the presence of risks and threats	
Course(s) that formally assess(es) this program-level learning outcome: AIC 481 - Case Studies in Cybersecurity Using AI	
Assessment Indicator: Malware Detection and Profiling	
Overall, how well did the students perform on this Program-Level learning outcome? (right-click on the checkbox and select 'properties' and 'checked')	<input checked="" type="checkbox"/> below expected levels <input type="checkbox"/> at expected levels <input type="checkbox"/> above expected levels
Analyze assessment of indicator results documented by the “Average score for the indicator as a percent” and “How well did the students perform?”: What does the information in the previous reporting suggest to you about the performance expectations, the teaching strategies, and student learning?	The results indicate that while students performed well on the hands-on aspects of malware detection, some struggled with profiling and documenting malware behaviors in a structured format. Key areas needing improvement include understanding feature extraction from malware behaviors and creating detailed malware family profiles. Teaching strategies should include more hands-on labs focused on profiling techniques and report writing, as these are critical for cybersecurity professionals.
Next steps: Plans for reinforcing effective teaching and learning strategies and for improving student learning (clearly identify what will be done, by whom, by when, and how you will assess the impact of the changes)	<ul style="list-style-type: none"> ● Introduce additional labs focused on feature extraction and profiling malware families, implemented by the course instructor in the next offering of AIC 481. ● Include a preliminary lecture on structured documentation of malware behavior to improve reporting quality. ● Provide an optional online module on using sandbox tools for malware analysis. ● Assessment will include both pre- and post-lab quizzes to measure the improvement in profiling and documentation skills.
Projected quarter/semester of implementing “next steps”	Fall 2026
Results of “next steps” implementation – this section is to be completed the following year (describe how the implementation of the above “next steps” impacted teaching and learning in the program)	After implementing additional labs and lectures, the students’ performance in profiling malware families improved significantly. The average score for this indicator rose from 85% to 92%, with students demonstrating stronger documentation and feature extraction skills. Feedback from students indicated that the sandbox-focused online module was particularly helpful for reinforcing practical skills.
Suggestions for improving this report or process (if any)	[Suggestion text here]

Example for requirement 1e1: Knowledge Unit (KU) Alignment for AICyber – The PoS courses are aligned to chosen KUs and KU outcomes (See A. AICyber KU requirements below for validation level). One course may align with multiple KUs. One KU may align to multiple courses. Provide all course outcomes for each course that is aligned with KU(s) and provide a URL or other evidence for the course outcomes indicated at the academic institution via the institutional Web site or within course syllabi. KU alignment is needed for courses that are aligned to the KUs only.

Program of Study Name: BS in Cybersecurity (add more rows if necessary)

Course Number	Course Name	Course Outcomes	KU Alignment	KU Outcomes (Listing only, no assessment of outcomes. KU Topics are recommended and not required for alignment)
AIC 481	Case Studies in Cybersecurity Using AI	Upon successful completion of this course, each student should be able to: 1. Apply AI techniques to detect and respond to cyber threats. 2. Evaluate the effectiveness of AI-based defensive and offensive security solutions. 3. Analyze real-world cybersecurity scenarios using AI.	(DFA) Defensive Applications of AI	<ol style="list-style-type: none"> 1. Implement AI techniques to enhance security posture. 2. Develop AI models for risk identification. 3. Understand XAI-driven solutions.
			(OFA) Offensive Applications of AI	<ol style="list-style-type: none"> 1. Identify adversarial attacks on AI. 2. Use AI for penetration testing.
AIC 440	System Security and AI	Upon successful completion of this course, each student should be able to: 1. Analyze the integration of AI into system security practices. 2. Detect and mitigate system-level vulnerabilities using AI-driven solutions. 3. Evaluate security measures for AI-based systems.	(AIS) AI for Security Assessment	<ol style="list-style-type: none"> 1. Identify AI techniques for security assessments. 2. Apply AI to evaluate vulnerabilities and mitigate risks. 3. Integrate AI-driven tools for continuous system monitoring and threat detection.
			(DFA) Defensive Applications of AI	<ol style="list-style-type: none"> 1. Apply AI models for vulnerability detection. 2. Automate cybersecurity processes.

Example for requirement 1e2: Knowledge Unit (KU) Alignment Summary Table for CyberAI PoS – The Knowledge Unit (KU) Alignment Summary Table for CyberAI PoS provides an overview of the Courses-to-KU for the PoS. Below see two examples of KU Alignment Summary Tables.

Example: KU Alignment Summary Table for MS CAE-AI (AICyber) PoS with Eight Courses in KU Alignment.

Master CAE AICyber (Total 11 KUs)											
PoS Courses in KU Alignment	Cyber Foundational				AI Foundational			Core			Optional
	CSF	ISC	BSP	MAF	AIG	AIF	MLF	BNW	NDF	AIS	DFA
MAIC602				X							
MAIC615	X	X									
MAIC623					X						
MAIC640			X								
MAIC650								X			
MAIC660									X		X
MAIC670						X					
MAIC675							X			X	

DRAFT

**APPLICATION PROCESS AND ADJUDICATION RUBRIC (APAR)
- CYBERAI WORKING GROUP (CYBERAIWG)**

CyberAI Working Group

Co-Chairs

Kaza, Siddharth - Towson University, CAE-CD, CAE-CO

Taylor, Blair - Towson University, CAE-CD, CAE-CO

Lead Authors

Banik, Shankar - The Citadel, CAE-CD

Nestler, Vincent - California State University, San Bernardino,
CAE-CD

El-Sheikh, Eman - University of West Florida, CAE-CD

Sajid, Md - Towson University, CAE-CD, CAE-CO

Flores, Paige - Towson University, CAE-CD, CAE-CO

Samtani, Sagar - Indiana University, CAE-CD, CAE-R

Hamman, Seth - Cedarville University, CAE-CD, CAE-CO

Tague, Patrick - Carnegie Mellon University, CAE-CD, CAE-CO, CAE-R

Levy, Yair - Nova Southeastern University, CAE-CD, CAE-R

Wagner, Paul - University of Arizona, CAE-CD, CAE-CO, CAE-R

The APAR-CyberAIWG would like to thank Lynne Clark, Angie Painter, Renae Weathers, and Victor Piotrowski for their leadership that led to this document.

This project is partially funded by NSF through the CyberCorps program DGE#1663184 at Towson University and by the CAE Community at the California State University, San Bernardino (CSUSB), under National Security Agency (NSA) award number H98230-22-1-0316.