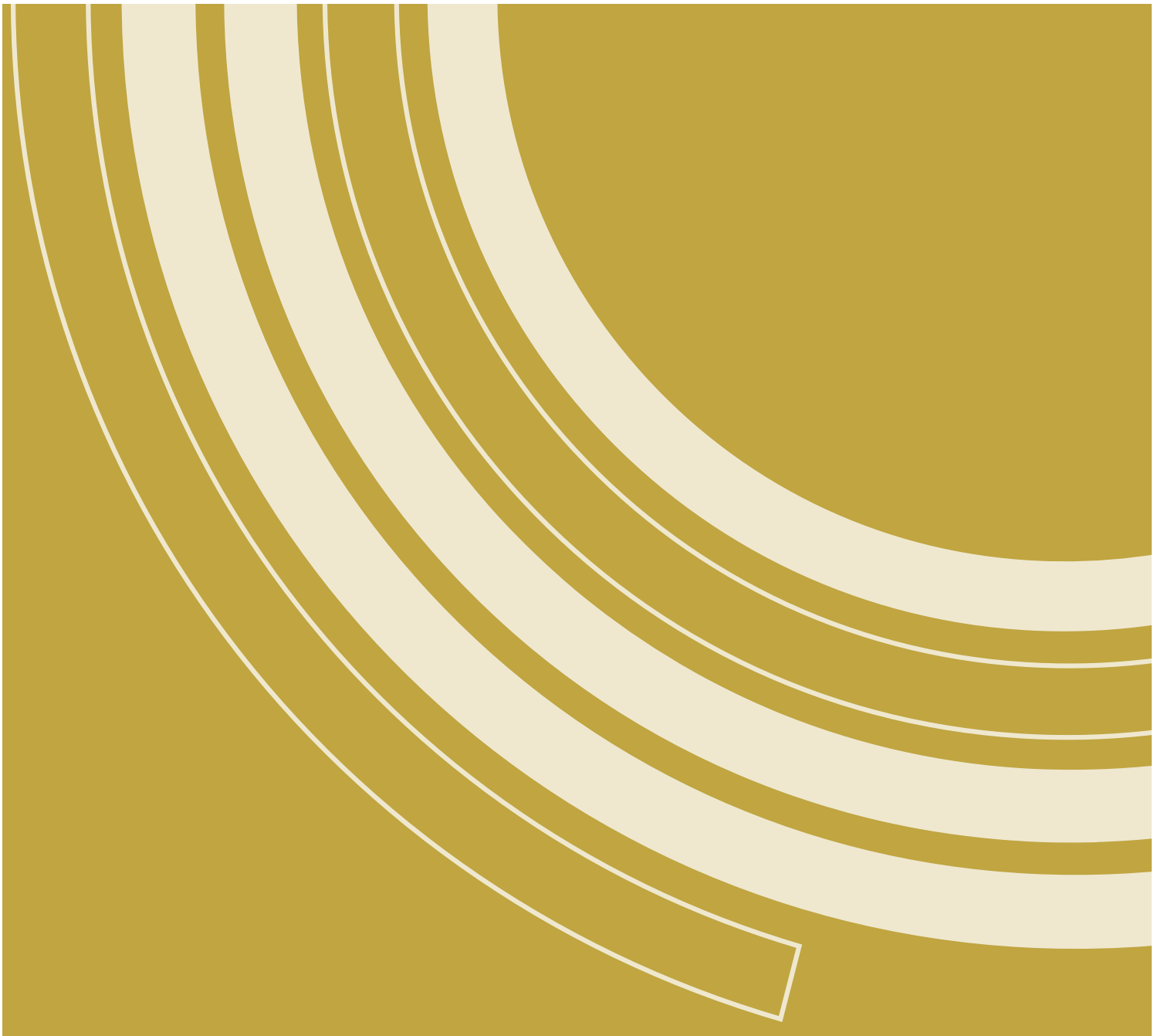
NATIONAL CYBERWATCH CENTER

RESOURCE GUIDE

GUIDE AND WORKBOOK FOR COMPLETING CAE CRITERIA: ASSOCIATE LEVEL

AUTHOR: **DR. FRED KLAPPENBERGER, FEBRUARY 2019**



NATIONAL CYBERWATCH CENTER

National CyberWatch Center Digital Press ID *NCC-2019-CAE-01*

Guide and Workbook for Completing CAE Criteria: Associate Level

Dr. Fred Klappenberger

Table of Contents

I. Introduction *5*

CAE Application Process 5

II. Getting Started *6*

Criteria and Point System 6

An Exception 6

General Format of Major Criteria and Sub-Criteria 6

Justifications, Links, and Attachments 7

Tips 8

Common Questions 8

III. How to Use This Guide / Workbook *9*

IV. Criteria Workbook *10*

1a. Cyber Defense Program of Study 11

1b. Student Participation in Curriculum Path 12

1c. Curriculum Program Path Identification 13

1d. NICE Framework Crosswalk 13

Criterion 2. Student Skill Development and Assessment *14*

2a. Courses Required for Student Scholarly Skills Development 14

2b. Scholarly Skills Development Requirements for Cyber Defense Students 15

2c. Courses Requiring Lab Exercises 15

2d. Students Assessed by: Lab assignments/Hands-on Activities 16

2e. Student Participation in Cyber Competitions 17

2f. Cybersecurity Practitioners/Industry Partnerships 17

Criterion 3. "Center" for Cyber Education *18*

3a. The center provides the following services: 18

3b. External Board of Advisors 19

Criterion 4. Cyber Faculty Qualifications and Courses Taught *20*

4a. Head of the Cyber Program of Study 20

4b. Designated Alternate and Additional Faculty 21

4c. Faculty Cybersecurity Qualifications 22

4d. Cyber Defense Presentations 22

4e. Faculty Support to Cyber Student activities, Clubs, Competitions, etc. 23

Criterion 5. Cyber Defense is a Multidisciplinary Practice at the Institution 24

5a. Cyber Defense Concepts Taught in Other Fields of Study 24

5b. Non-Cyber Defense Courses Encourage Papers, Projects or Test Questions in CD topics 25

5c. Professional Development Courses 25

Criterion 6. Institutional Security Plan 26

6a. Security Plans 26

6b. Security Officer – Provide Name and Job Description 27

6c. Implementation of Cyber Security Practice 27

Criterion 7. Cyber Outreach/Collaboration Beyond the Institution 28

7a. Faculty Involvement in Sharing Expertise 28

7b. Transfer of Credit – 4-year institutions 29

7c. Transfer of Credit or Partnerships - High School 30

7d. Support/Participation to the CAE Community 30

7e. Community Outreach – Activities Outside of Student/Campus Events 31

7f. Business/Industry Collaboration 31

V. Reference - Summary of Criteria and Points 32

I. Introduction

This document offers suggestions and tools to assist in the preparation of the Criteria section of the CAE application. This guide is based on the 2019 Criteria. Criteria are subject to change each year and should be used for exact criteria requirements. For information on general institutional eligibility, requirements, expectations, and other specifics about the application process, refer to: https://www.iad.gov/NIETP/CAERequirements.cfm.

CAE Application Process

The CAE application process consists of two key activities: 1 – mapping program courses to identified CAE Knowledge Units (KU), and 2 – providing evidence that an institution satisfies prescribed criteria broader than the technical educational components alone. The first activity is formulaic – an institution shows how courses in a program path satisfy KU topics and outcomes. The second activity is somewhat freeform - an institution states its credentials and tell its unique story about how it qualifies to be designated a Center of Academic Excellence in the Cybersecurity field based on a set of broad NSA/DHS criteria.

Each institution has its own personality – variants in programs of study, access to resources, faculty backgrounds, business community needs, student community, etc. No two institutions will satisfy the criteria in the same way. Institutions use the criteria to tell their unique stories and distinguish themselves from others.

Like the mapping component, completing the criteria section requires significant time commitments and attention to detail. Whereas most of the mapping component relies on common syllabi related data (i.e., topics, objectives, assessment methods), the criteria section has a large free-form component requiring a narrative (*Justification)* and a range of supporting evidence (*Links and Attachments)*. Completing this component also usually requires assistance and cooperation of others outside the department in which the CD program resides to provide information and documents.

The following pages offer procedures and suggestions about how one might go about completing the criteria in an organized fashion. It follows in lock-step with the criteria submission process in the NIETP database tool.

II. Getting Started

Criteria and Point System

To successfully earn CAE-CDE designations, 2-Year and 4-Year institutions must satisfy a set of major criteria. They are designated by number (0, 1, 2, …, 7) and name. Criteria specifics differ only slightly between the 2- and 4-year schools to reflect the depth of programs and the communities served. Criteria further divide into sub-criteria which provide depth and detail to each criterion.

Every criterion (major or sub) has specified point values. Most criteria have mandatory (i.e., minimum) point values and are so noted in the instructions. The point values for major criteria are calculated by summing the point values of each of their sub-criteria.

An Exception

An exception to the above comments about Criteria and Points should be noted. The "0" criterion (i.e., 0. Letter of Intent and Endorsement) counts as one of the official criteria. While this is a mandatory criterion and all its requirements must be satisfied, it carries no point value. It is just plain mandatory! (A similar comment applies to sub-Criteria 1c and 1d.)

General Format of Major Criteria and Sub-Criteria

The main components of a major criterion are the title, the requirements summary, the point value(s) (mandatory, maximum), and the sub-criteria. As previously noted, sub-criteria, too, have their requirements and point values. In this structure, sub-criteria parse and expand upon their respective parent major criterion. In other words, a major criterion broadly defines its range of requirements and the sub-criteria provide the detail. So, in completing an application, the institution provides information to meet the requirements specified in the sub-criteria.

Except in a couple of instances, in completing sub-criteria, an applicant must supply two types of information. First, a statement how the institution meets the requirement (Fig. 1). This is referred to as the "Justification." Second, evidence to substantiate the justification must be furnished via links and/or attachments. Figs. 1, 2, and 3 are taken from the NIETP database entry tool and are the means for providing the information.

Fig. 1 Justification

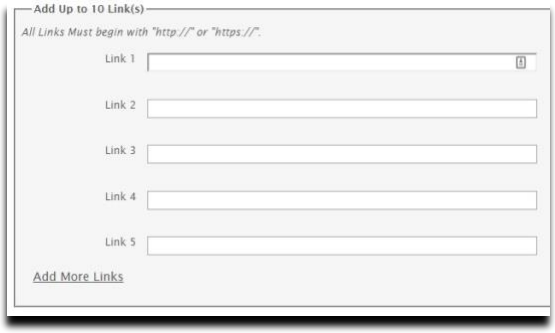


Fig. 2 Links

Fig. 3 Attachments

Justifications, Links, and Attachments

An applicant uses the Justification box (Fig. 1) to furnish a narrative statement explaining how the institution satisfies the relevant sub-criterion. The statement should fully and directly address the requirements outlined in the sub-criterion. It should be organized, to the point, and grammatically correct. Rambling, vagueness, and obfuscation are to be avoided. The narrative must be supported with links and/or attachments (Figs. 2 and 3) providing explicit evidence for the claims made.

Text can be typed or pasted into the Justification box (Fig. 1). Formatting (bold, underline, italics, tabs) is ignored. All entries (even formatted pastes) will be converted to plain text. A Justification box has the capacity to accept over 10,000 characters. So, while an applicant has no practical limit on the size of description, the statement should fully, directly and succinctly address the requirements outlined in the sub-criterion.

Up to ten links and ten attachments can be cited as evidence to support the justification statement.

Tips

- Liberally use “Justifications” to explain the purpose of attachments and links.

- Employ highlighting in attachments to direct attention to key words, phrases, or sentences that support statements made in Justifications. For example, a justification stating that John Doe acts as a faculty advisor to the student computer club might be supported with an attachment showing some club activity, event, or membership that includes the highlighted name of the advisor.

- When providing evidence via links, make sure the links work! If an ID or password is required to access the linked site, be sure to furnish that information in the justification statement.

- If there’s an option of providing evidence by either a link or an attachment, an attachment would usually be preferred for three reasons. First, an attachment can be easily highlighted whereas link content cannot; second, attachments can focus on the pertinent information related to the justification; and third, links can be broken making a linked document unavailable, but an attachment is fixed.

- Ask a third party to read the justifications for clarity, coherence, grammar and completeness.

- Think of the reviewer who will evaluate the application as your friend. Make the reviewer’s job easier by writing clear, direct responses and providing relevant, targeted evidence.

Common Questions

1. **How long does it take to complete the Criteria section?**

   It depends on a number of variables, not the least of which is cooperation of fellow faculty and staff. Institutions that have never applied before should expect to spend 40 to 80 person hours dedicated to preparing and gathering materials and inputting the required information into the NIETP database.

2. **Can I see another institution’s submission?**

   No, sorry. As an aspirant to being designated as a Center of **Academic Excellence**, an institution is expected to independently make its case for recognition without borrowing the work of other institutions.

III. How to Use This Guide / Workbook

The guide suggests a process to methodically prepare material for Program Criteria. It interlaces excerpts from the *CAE CDE Associate Level Criteria – 2019* (black font) augmented with suggested data gathering tables and check boxes (blue font).

To use this guide …

- Carefully read (parse) each black fonted official CAE CDE criterion and its sub-criteria descriptions to identify the specific information elements required. Be sure to address every element in your response.
- Formulate a Justification statement that explains how your institution satisfies the criterion.
- Use the blue-fonted tables and boxes as a checklist for links and attachments that provide evidence supporting the Justification statement.

Note: The black fonted criteria text in this Workbook identifies the "official" requirement that an institution must satisfy; the text in blue font is a general, abbreviated summarization that emphasizes core elements to include in the Justifications, Links, and Attachments that will be entered into the NIETP database.

The following pages are an abridgement of the CAE-CDE Associate Level Criteria – 2019 document (https://www.iad.gov/NIETP/documents/Requirements/CAE_Associate_Criteria.pdf) interspersed with tables detailing the data elements that the criteria require. The reader should consult the document at the link provided for additional details.

IV. Criteria Workbook

Criterion 0. Letter of Intent and Endorsement

Provide official notice of institutional endorsement and intent to participate in the CAE-CDE program. Shows management support of the program(s) at the institution. The letter must:

- Be written on official institution letterhead, signed by the Provost or higher
- Express institutional commitment to excellence in the cyber defense field and support of the program the institution is submitting for CAE designation
- Identify the CAE point of contact (POC) from the institution
- Provide institutional support of an official Cyber "Center" within the institution
- Identify regional accreditation information
- List pertinent accomplishments in the cyber defense field
- The letter shall be addressed to:

  National Security Agency
  Attn: CAE Program Director
  9800 Savage Road
  Ft. Meade, MD 20755-6804

The Letter of Intent must be uploaded within the CAE-CDE application. Do not mail. This is a mandatory requirement. Designated schools are expected to actively participate in the CAE Community and support the CAE-CD program. Submission of this letter acknowledges the following minimum participation expectations:

Submission of an Annual Report with all required information

- Attendance at the CAE Community Symposium each year
- Regular communication with the CAE Program Office, the CAE Community, and the CAE Regional Resource Center. (Responds to email, offers input and suggestions for workshops, programs, program decisions, etc.)
- Maintenance of institution information on https://www.iad.gov/NIETP/index.cfm

Use the following Checklist to verify that each of the elements are addressed in the Letter of Intent and Endorsement:

Requirement	Check
Institution letterhead	
Signed by Provost or higher	
Commitment to & support of CD excellence	
CAE point of contact (POC)	
Official Cyber "Center"	
Regional accreditation	
Accomplishments in cd field	
Correct NSA address	

Criterion 1. Cyber Defense Academic Curriculum Path

The Cyber Defense (CD) curriculum path must have been in existence for at least 3 years. Evidence must show one (1) year of students that complete the curriculum path with recognition. The institution must have a mature program path in place that leads to a two-year associate's degree or a certificate in a related cyber discipline. The path is defined as a series of courses that meet all the mandatory Knowledge Units (KUs). The institution must show its curriculum path and show that students are enrolled and successfully complete the path and receive recognition. Applicant institution must provide a list of courses (number and title) included in meeting the cyber defense curriculum path and provide data showing when each course was last taught.

Overall Point Value: 10 pts mandatory

1a. Cyber Defense Program of Study

Describe the CD curriculum path offered by the institution. This description must contain the following:

- List curriculum path(s) – must contain all courses mapped to KUs. Courses must be identified in current course catalog.
- Identify department(s) where curriculum path resides.
- If more than one path, each must be mapped separately and meet all of the mandatory KUs. If application is approved, only the CD curriculum program path(s) identified in this criterion are allowed to be marketed as a designated CAE2Y.

(5 pts mandatory)

1a. Program Path (i.e., Courses Mapped to KUs)

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Program of Study				
Name(s) of Program(s)				
Catalog link(s) or attachment(s) highlighting program path				
Courses that make up program path (i.e. courses mapped to KUs)				
Course No.	**Course Title**	**Dept.**	**Last taught**	**Link/attachment**

(Add rows as necessary)

1b. Student Participation in Curriculum Path

- Evidence provided must include, but is not limited to:
- Student enrollment in curriculum path for the last 3 years (letter from Registrar)
- Number of students that have received a degree and completed the Cyber Defense program path within one (1) year of submission (Registrar letter)
- Provide at least three (3) redacted student transcripts, dated within the last 3 years and clearly highlight the courses taken that meet the Cyber Defense program path. All courses used to map to the KUs must be present
- Sample certificate or notation on transcript issued to students completing the CD program path **(5 pts mandatory)**

1b.1 & 1b.2 Include Following Data in Registrar's Letter

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Registrar Signed Letter Citing Number of Student Enrollments		
Last year – (this year-1)	**Year before last (this year-2)**	**Two years before last (this year-3)**
No. of Program Graduates w/in 1 Yr of application submission		

1b.3 Provide at Least Three Redacted Student Transcripts

Highlight mapped courses (i.e., program path) on transcripts. All courses mapped to KUs must be present. Use the following self-check list to assure that all required information is provided in the Justification and Attachment boxes of the NIETP database tool:

Redacted Student Transcripts	
Student 1	
Student 2	
Student 3	

(Add rows as necessary)

1b.4 Sample Certificate or Notation

Provide a sample certificate or transcript notation issued to students completing the CD program path. Use the following self-check list to assure that all required information is provided In the Justification and Attachment boxes of the NIETP database tool:

Sample Certificate or Transcript Notation	
Attachment 1	

1c. Curriculum Program Path Identification

Identify the name of the curriculum path that maps to the KUs. Only the name of the curriculum program path is required; e.g., "BS in Computer Science, Cyber minor." This information will be used to market the CAE program at the applying institution, on nsa.gov and other related websites and for program identification on the designation certificate. All other information about the program should be entered in 1a.

(0 pts awarded, but must provide - mandatory)

1c. Provide Name of CAE Program

Use the following self-check list to assure that the required information is provided In the Justification box of the NIETP database tool:

Name of curriculum program path

1d. NICE Framework Crosswalk

Identify how the mapped curriculum path relates to the NICE Cybersecurity Workforce Framework (NCWF), NIST SP 800-181. Select one or more NCWF Categories that best define the applying institution program: Operate and Maintain; Oversee and Govern; Protect and Defend Investigate; Collect and Operate; Analyze; and/or Securely Provision. Only identification of the NCWF categories is required, no explanation is needed.

(0 pts awarded, but must provide - mandatory)

1.d. Checkoff the NICE Cybersecurity Workforce Framework (NCWF) Category or Categories That Program Best Fits

Use the following self-check list to assure that the appropriate NCWF Category is identified in the Justification box of the NIETP database tool:

NCWF Category	Our program fits: (check all that apply)
Operate and Maintain	
Oversee and Govern	
Protect and Defend	
Investigate	
Collect and Operate	
Analyze	
Securely Provision	

Criterion 2. Student Skill Development and Assessment

The institution must show how it fosters student development and assessment in the field of Cyber Defense. This criterion focuses on STUDENT-based skills development as it contributes to evolution of theory and practice in the field of Cyber Defense and how students are assessed. Skills development shall relate back to one or more of the mapped KUs. Courses used in this section must be KU mapped courses.
Overall Point Value: 17 pts mandatory, 27 pts maximum

2a. Courses Required for Student Scholarly Skills Development

- Provide syllabi of CD courses that require papers, presentations, projects, test questions – highlight requirement – courses must map to the KUs and must relate to papers/projects/etc. submitted in criterion 2b
- Courses requiring papers/projects/presentations/test questions must have been taught within the last 3 years
- Courses requiring papers/projects/presentations/test questions must be a part of the CD curriculum path as identified in the application

(1 point per course/at least 3 different courses/3 mandatory/5 pts maximum))

2a. Courses Required for Student Scholarly Skills Development: Identify and Attach Syllabi for At Least Three Mapped Courses Requiring Papers, Presentations, Projects, Test Questions. On Each Syllabus, Highlight the Requirements (I.E., Papers, Presentations, etc.) the Syllabus Satisfies

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Course No.	Course Title	AttachedHighlighted Syllabus	Last Taught (w/in 3 years)

(Add rows as necessary)

2b. Scholarly Skills Development Requirements for Cyber Defense Students

- Students assessed by one or more methods: Provide actual student work (can be redacted) in the form of papers, projects, test questions, etc. from students in the curriculum path (**must** be from courses in the curriculum path identified in 2a). Papers/projects, etc. **must** be clearly identified with course title, course number, and date of submission.
- Links or attachments to actual papers/projects/presentations/test questions are required – not a subscription service

(1 pt per paper/project/etc./from at least 3 different courses/4 pts mandatory/ 5 pts maximum)

2b. Provide actual papers, projects, test questions, etc. from students in the curriculum path (must be from 3 different courses in the curriculum path). Attachments must include clearly identified (Highlighted) course title, number, and date of submission. Links or attachments to actual papers/projects/ presentations/test questions are required.

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Course No.	Course Title	Assessment Example Attachment or Link	Date of Submission

(Add rows as necessary)

2c. Courses Requiring Lab Exercises

- Provide syllabi of CD courses that require labs – highlight lab requirement – must relate to student labs submitted in criterion 2.d, must be courses used to map to KUs
- Courses must have been taught within the last 3 years

(1 pt per course/at least 3 different courses/3 pts mandatory)

2c. Provide syllabi of courses in program path (i.e., mapped) that require labs/exercises. (Highlight lab/exercise requirements in syllabi.)

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Course No.	Course Title	Attach Highlighted Syllabus	Last Taught (w/in 3 yrs)

(Add rows as necessary)

2d. Students Assessed by: Lab assignments/Hands-on Activities

Demonstrate that physical and/or virtual labs and equipment are available and demonstrate how these resources are used by students and faculty to enhance hands-on learning in the Cyber Defense program path of study.

- Provide a description of required lab projects or exercises required for students participating in the CD program path of study. Identify the related course for each of the lab projects and exercises. Must be courses used to map to KUs
- Provide examples of actual student lab work (**must** be from courses in the curriculum path identified in 2c) and describe how the lab enforces curriculum taught in the path.

(1 pt per lab assignment/from at least 3 different courses/5 pts mandatory)

2d. Provide Descriptions and Examples of Student Labs/Exercises Required by Courses in Program Path and How They Enforce Curriculum

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Course Number	Lab/Exercise Id	Description	Lab / Hands-On Activities Attachment

(Add rows as necessary)

2e. Student Participation in Cyber Competitions

- Provide evidence of participation in Cyber Defense exercises and/or competitions for students enrolled in applying institution within the last 3 years, (e.g., link to team roster on the competition website, link to social media about the exercise, etc.). This can include in-class exercises with explanation.
- Explain the benefit of participating in the Cyber Defense Exercise/Competition. How did the team place? What were the lessons learned? What basic cyber content was reinforced by participating on a team?

(1 pt per competition/1 pt mandatory/5 pts maximum)

2e. Cite Cyber Competitions in Last 3 Years, Team Placement, Content Reinforced, and Lessons Learned

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Competition Name or Exercise	
Date	
Team Placement	
Evidence* Link/Attachment	
CD Content Reinforced	
Lessons Learned (Benefits)	

* Cite team roster on competition website or institution "Cyber Center", social media, etc.

(Add tables as necessary)

2f. Cybersecurity Practitioners/Industry Partnerships

- Provide evidence that the program is providing students with access to cybersecurity practitioners (e.g., Guest lecturers working in the Cybersecurity industry, government, faculty exchange program with industry and/or government, internship opportunities, etc.). Provide fliers, posters, letters, etc.

(1 pt per partnership/1 pt mandatory/4 pts maximum)

2f. Cybersecurity Practitioners/Industry Access and Partnerships

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool. At least one partnership must be completed:

Access to Cyber Practitioners	Attachments of Fliers, Posters, Letters, etc.
Industry	
Government	
Faculty Exchange	
Internships	

Criterion 3. “Center” for Cyber Education

The institution must have an officially established entity (either physical or virtual) serving as the focal point for its cyber curriculum and practice. The center shall provide the following services: program guidance and oversight; general cyber defense information; and collaboration and outreach opportunities among students, faculty, and other institutions. Additionally, the center must be supported by a website that is dynamic, current and visible within the institution and the external community at large.
Overall Point Value: 10 pts mandatory/13 pts maximum

3a. The center provides the following services:

- Cyber “Center” shall provide program guidance and general CD information, and promote collaboration and interaction with other students, faculty, and programs.
- For the purpose of this document, “Center” is used as a generic term allowing for other terminology to be used because of restrictions at some academic institutions
- The Cyber “Center” and its website must be operational, dynamic, current and visible within the institution and to the community at large.
- Evidence provided must include, but is not limited to:
    - Information about the CD program of study and faculty
    - Program guidance and oversight
    - “Center” points of contact
    - Links to student CD activities available to students at the institution and beyond
    - Include both internal and external CD news. Internal news should highlight CD activities and efforts at the institution and/or other CD activities of students and faculty representing the institution. External CD news should highlight up to date trending CD information
    - Institutional security resources and awareness
    - Up-to-date links to key CD resources such as other academic institutions, government sites, conferences, workshops, and cyber competitions
    - Center Website (url) - visible within the institution and the external community at large

(8 pts mandatory)

3a. "Center" Provides Comprehensive CD Information Services to Institution's Community

Use the following self-check list to assure that all required information is provided:

"Center" Services	Y/N	Links, Attachments
URL of Center (internal & external)		
Information about CD program of study and faculty		
Program guidance and oversight contact		
"Center" points of contact		
Links to student CD activities available to students at the institution and beyond		
Internal CD news		
CD activities and efforts		
CD activities of students and faculty		
External CD news		
up-to-date trending CD information		
Links to key CD resources		
Other Academic Institutions		
Government Sites		
Conferences, Workshops		
Cyber Competitions		

3b. External Board of Advisors

The department that houses the Cyber "Center" must have an external board of advisors – local/national industry professionals, faculty from other institutions, etc. to provide programmatic guidance over the activities of the center and the program as a whole. This board provides a connection between the program and the local community. Provide names, meeting minutes, etc.

(2 pts mandatory/5 pts maximum)

3b. Identify "Center's" External Board of Advisors, Meeting Minutes

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

"Center's" External Board of Advisors	Links/Attachments
Meeting Minutes (dates)	

Criterion 4. Cyber Faculty Qualifications and Courses Taught

The institution must demonstrate that it has faculty responsible for the overall CD program of study and sufficient faculty members, either full- or part-time to ensure continuity of the program. The criterion requires a link or attachment to the biography, curriculum vitae or resume for each faculty member with school affiliation clearly identified. It **must** be possible to locate all permanent faculty members by searching the Institution website.

Overall Point Value: 10 pts mandatory/15 pts maximum

4a. Head of the Cyber Program of Study

- Identify by name faculty member with overall responsibility for the CD curriculum path.
- Provide evidence, i.e., verification letter and/or job description. Provide link or attachment to biography, resume or curriculum vitae (CV) with cyber background and school affiliation clearly identified. Institution affiliation must be clearly identified.
- Highlight or list professional societies and level of effort.

(5pts mandatory)

4a. Head of Cyber Program of Study – Name, Verification, CV, Courses Taught

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Requirement	Specify
Name of Head	
	Link/Attachment
Verification ltr or job description citing institution position	
Bio or CV, courses taught, highlight prof'l societies	

4b. Designated Alternate and Additional Faculty

- Must provide a permanent faculty as a designated alternate for notices: CV required
- Identify by name additional full-time, part-time or adjunct faculty members teaching CD courses within the department that sponsors the CD program path identified in Criterion 1a. Do not include faculty listed in criterion 4a
- Provide link to biography, CV or resume with cyber background clearly identified. Institution affiliation must be clearly identified
- Identify courses taught at applying institution within the last 3 years

  (1pt each/1 pt mandatory)

4b.1 Identify Alternate Head of Program Faculty

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Requirement	Specify
Name of full time program alternate	
Institution position	
	Link/Attachment
Verification letter or job description	
Bio or CV	

4b.2 Identify Additional Faculty Who Teach CD Courses in Program Path

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Requirement	Specify
Other CD Faculty	
Institution Position	
Check Status	Full-Time ____ Part-Time _____ Adjunct _____
	Link/Attachment
Verification letter or job description	
Bio or CV	
Course(s) Taught	

(Repeat table for each additional CD faculty member)

4c. Faculty Cybersecurity Qualifications

- Provide evidence in the form of CV supporting the faculty member's qualifications to teach cybersecurity. At least one faculty member is expected to be professionally certified with at least one of the Cybersecurity/Information Assurance certifications listed under DOD Directive 8570, such as CISSP, CISA, CISM, CEH, Security+, etc. (see attached DoD 8570 list here) **- or -**
- A minimum of 15 hrs of graduate coursework and/or appropriate experience in a related field could be considered in lieu of a professional certification – explanation is required if faculty members do not have relevant certifications. (Please Note - can be same individual as listed in Criteria 4a/b)

(1 pt each/1 pt mandatory)

4c. Provide Evidence of Faculty Cybersecurity Qualifications

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Requirement	Specify
Name	
Certification(s) or Graduate Coursework	
	Link/Attachment
Verification letter or job description	
URL of Bio or CV (searchable); include courses taught	

(Repeat table for each CD faculty member)

4d. Cyber Defense Presentations

- Provide evidence that faculty members have presented CD content at Local/Regional/National/International conferences and events within the last 3 years (link to program or website with presentation clearly highlighted)
- Provide a synopsis of the involvement. This can include guest lecturer at other institutions or government organizations (provide proof – link to program, website, etc.)

(1 pt per presentation/5 pts maximum)

4d. Faculty Conference Presentations / CD Competition Events Within the Last 3 Years

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Conference/Event	Link/Attachment	Synopsis

(Add rows as necessary)

4e. Faculty Support to Cyber Student Activities, Clubs, Competitions, etc.

- Provide evidence that CD faculty members support their students by serving as mentors or advisors to student led activities. Evidence must include links to student clubs, cyber defense exercises, etc.
- Provide evidence of participation in or sponsorship of CD exercises and competitions within the last 3 years, (e.g., link to team roster on the competition website, link to social media about the exercise, etc.) This can be an in-class competition. Evidence must be provided.
  (1 pt per item/1 pt mandatory)

4e. Faculty Mentoring/Advising to Cyber Student Activities, Clubs, Competitions, etc.

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Faculty Name	Link/Attachment	Identify Activity

(Add rows as necessary)

Criterion 5. Cyber Defense is a Multidisciplinary Practice at the Institution

The institution must demonstrate that Cybersecurity is not treated as a separate discipline but integrated into additional programs within the institution. Courses cannot be from the department mapped to the Knowledge Units.

Overall Point Value: 7pts mandatory/15 pts maximum

5a. Cyber Defense Concepts Taught in Other Fields of Study

- Provide evidence that CD topics are integrated in courses outside of the department that contains the CD program path of study. *For example*: health practitioners learning about privacy and patient electronic data protection; criminal justice learning about chain of custody for electronic evidence; or accountants learning about data backup and protection. **Provide course name and syllabus with cyber modules clearly highlighted.**
- Cannot be courses in the department or curriculum path used to map to the Knowledge Units; exception would be a course that all students are required to take on basic cyber hygiene.
- Courses taught outside the CD program of study can be technical or non-technical. For example: health practitioners learning about privacy and patient electronic data protection; accountants learning about data backup and protection; criminal justice learning about chain of custody for electronic evidence; or non-credit continuing education courses on IT security basics.

(1 pt per course/3 pts mandatory/5 pts maximum)

5a. Identify Where CD Concepts are Taught in Other Departments and Provide Syllabi of Courses

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Course Name	Attachments: Syllabus (w/ Highlighted CD Modules from Outside Depts)

(Add rows as necessary)

5b. Non-Cyber Defense Courses Encourage Papers, Projects or Test Questions in CD topics

- Provide evidence that courses taught outside the CD program path of study require CD topic papers/projects/posters/test questions/etc. For example: health care practitioners write a paper on the importance of safeguarding electronic patient health care records.
- Provide links or attachments to 3 to 5 best papers, presentations, etc.- Cyber topics clearly highlighted within 3 years of application. Must be at least one from each of the courses listed in 5a. **Actual student work required – _not just the assignment required of students.**
- Paper/projects/presentations/test questions must correspond to course syllabi provided in 5a.

(1 pt each/3 pts mandatory/5 pts maximum)

5b. Provide Student Work of Papers, Projects or Test Questions from Courses Cited in 5a

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Course Name	Paper/Project/Test Question from Each Course in 5a. (Attachments w/Highlighted CD Topics)

(Add rows as necessary)

5c. Professional Development Courses

- Provide evidence (catalog, syllabi, class schedule) of the availability of non- credit/credit Cyber related professional development courses (e.g., First responders, K- 12 teachers)

(1 pt per course/5 pts maximum)

5c. Credit/Non-Credit Cyber Related Professional Development Courses

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Course Name	Links/Attachments

(Add rows as necessary)

Criterion 6. Institutional Security Plan

The objective of system security planning is to improve protection of information system resources. All systems have some level of sensitivity and require protection as part of good management practice. The protection of a system must be documented in a system security plan. The purpose of the system security plan is to provide an overview of the security requirements of the system and describe the controls in place or planned for meeting those requirements. The system security plan also delineates responsibilities and expected behavior of all individuals who access the system. The system security plan should be viewed as documentation of the structured process of planning adequate, cost-effective security protection for a system. (An example of a government-based IA security plan may be found at: Security plan example.) This is an example and not intended to replace an existing institution security plan.

Overall Point Value: 6 pts mandatory/9 pts maximum

6a. Security Plans

- Provide links or attachments to the high-level IS Security Plan(s) for the institution to show how it practices institutional security. IS Security Plan must include how the Information System infrastructure of the institution is protected and how the plan is implemented, not just policies on use of the system.

(2 pts mandatory)

6a. Institutional Information System Security Plan and Implementation

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Security PLAN - Links/Attachments

(Add rows as necessary)

6b. Security Officer – Provide Name and Job Description

- Provide the name, title and job description for the individual responsible for the institution IS program. If there is a committee to oversee IS security, please explain duties and implementation.

(2 pts mandatory)

6b. Security Officer

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Name (or Committee)	Title	Attachment: Job Description (Duties)

(Add rows as necessary)

6c. Implementation of Cyber Security Practice

- Provide evidence of how the institution implements IS Security plan through awareness, training and tutorials, log in security banners, user acknowledgements, on- line help and good security practice guides. (e.g., Students, faculty and staff are required to take computer based training or on-line tutorials; a security banner statement is present on institution or department computers; security related help screens are available; students are provided with a guide on good security practices, etc.)
- Provide screen shots, links to mandatory training, good password practices, etc.

(1 pt per example/2 pts mandatory/5 pts maximum)

6c. Implementation of Cyber Security Practice

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Security Plan Implementation	Links/Attachments (Screen Shots)
Awareness training/tutorials	
Login Security Banners	
User Acknowledgments	
On-line Security Help	
Good Security Practice Guide(s)	
Mandatory Training	
Good Password Practice	
Other	

(Add rows as necessary)

Criterion 7. Cyber Outreach/Collaboration *Beyond* the Institution

The institution must demonstrate how Cyber Defense practices are extended beyond the normal boundaries of the institution. Show how CD concepts developed at the Institution are shared with others or how industry theory and practice are incorporated into curriculum.

Overall Point Value: 18 pts mandatory/30 pts maximum

7a. Faculty Involvement in Sharing Expertise

- Provide evidence of how the institution shares Cyber related curriculum and/or faculty with other schools, to include K-12 schools, other community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge within the last 3 years
- Identify specific materials/faculty provided, to whom the material was provided, when and for what purpose. Any additional supporting documentation of this exchange, such as emails, formal meeting notes, links to material on accepting parties' website, etc. is encouraged
- Identify shared faculty (e.g., Faculty on Cybersecurity curriculum development committee). The institution should specifically state its contribution to the shared effort, (e.g. If faculty is on a curriculum development committee, what was the intuition's/faculty's specific contribution?)

(1 pt per event/1 pt mandatory/5 pts maximum)

7a.1 Sharing Materials

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Material Shared	With Whom	Links/Attachments

(Add rows as necessary)

AND / OR

7a.2 Sharing Faculty

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Faculty Shared	On What Project/Dept/Committee	Links/Attachments

(Add rows as necessary)

7b. Transfer of Credit – 4-year institutions

- Provide evidence of **Articulation/Transfer** agreements with 4-year institutions offering a concentration or cybersecurity (or related field) degrees/areas of study/track or certificates
- Identify specific cyber courses that are accepted at partner institutions and a crosswalk of the accepted courses. Examples include, (but are not limited to): statewide transfer agreements, articulation agreements, college in the high school, dual credit, running start, credit for prior learning, credit for military training or occupation

(1 pt per agreement/3 pts for statewide agreement/1 pt mandatory/5 maximum)

7b.1 Agreement Citations (4-year)

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Articulation/Transfer	With Whom (Institution)	Links/Attachments

(Add rows as necessary)

AND / OR

7b.2 Courses Accepted at Partner Institutions

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Accepted Cyber Courses	For Dual Credit/Running Start/Prior Learning/Mil or Occupation Training	Links/Attachments (w/ crosswalk)

(Add rows as necessary)

7c. Transfer of Credit or Partnerships - High School

- Provide evidence (e.g., MOA, dual-credit, college in high school, running start, lecture series, curriculum/faculty sharing, etc.) of agreements with high schools (cyber related or technical pre-requisite and not just general pathway programs) to facilitate awareness and training for faculty, administration or students.

(1 pt per agreement/3 pts for statewide agreement/1 pt mandatory/5 maximum)

7c. High School Agreements to Facilitate Awareness and Training

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Type of Agreement with High Schools	With Whom	Link/Attachment

(Add rows as necessary)

7d. Support/Participation to the CAE Community

- Provide evidence that the applying institution has participated in CAE events such as: CAE Symposium, CRRC workshops for candidate institutions, CAE Tech Talk/Forum used in classroom (1pt = 3 uses), collaboration on grants with CAE institutions. Provide emails, attendance roster, etc.
- Provide evidence of faculty collaborating with current CAE institutions on research, grants, course development, etc. Provide documenting information.
- Reviews/mentor/advisor, etc.

(1 pt per event/1 pt mandatory/5 maximum)

7d. Support/Participation to the CAE Community

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Type of Event	For Whom	Link/Attachment

(Add rows as necessary)

7e. Community Outreach – Activities Outside of Student/Campus Events

- Provide evidence of faculty/employee sponsorship or oversight of cyber events for the community at large. Events could include cyber awareness and education for local schools, adult education centers, senior centers, camps, first responders and the surrounding community
- Examples of events could be, but are not limited to, computer "check-up" days, protecting personal information in cyber space, workshops for senior citizens on Internet safety, or preventing and recovering from a "virus" (senior centers, K-12, camps, etc.) Provide fliers, emails, web announcement, etc.

(1 pt per event/1 pt mandatory/5 pts maximum)

7e. Community Outreach Events

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Type of Event	With Whom	Link/Attachment

(Add rows as necessary)

7f. Business/Industry Collaboration

- Explain involvement (internships for students, identifying needs of business partners for course content, job fairs, guest speakers, etc.)
- Provide evidence on how the institution partners with companies and other employers to identify Cyber Defense needs of potential employers and encourage student internships
- Provide evidence on how the institution works with employers and students to support placement for Cyber related jobs
- Provide evidence of obtaining input on curriculum to meet industry needs

(1 pt per collaboration/1 pt mandatory/5 pts maximum)

7f. Business/Industry Collaboration - Communication – Connection

Use the following self-check list to assure that all required information is provided in the Justification, Links, and/or Attachment boxes of the NIETP database tool:

Type of Collaboration	With Whom	Link/Attachment

(Add rows as necessary)

V. Reference - Summary of Criteria and Points

0. **Letter of Intent and Endorsement (0 pts awarded, but must provide - mandatory)**

1. **Cyber Defense Curriculum Path (Overall Point Value: 10 pts mandatory)**
    a. **Cyber Defense Program of Study (5 pts mandatory)**
    b. **Student Participation in Curriculum Path (5 pts mandatory)**
    c. **Curriculum Program Path Identification (0 pts awarded, but must provide - mandatory)**
    d. **NICE Framework Crosswalk (0 pts awarded, but must provide - mandatory)**

2. **Student Skill Development and Assessment (17 pts mandatory, up to 27 pts)**
    a. **Courses Required for Student Scholarly Skills Development (1 point per course/at least 3 different courses/3 mandatory/5 pts maximum)**
    b. **Scholarly Skills Development Requirements for Cyber Defense students (1 pt per paper/project/etc./from at least 3 different courses/4 pts mandatory/5 pts maximum)**
    c. **Courses Requiring Lab Exercises (1 pt per course/at least 3 different courses/3 pts mandatory)**
    d. **Students Assessed by: Lab assignments/Hands on Activities (1 pt per lab assignment/from at least 3 different courses/5 pts mandatory)**
    e. **Student participation in cyber competitions. (1 pt per competition /1 pt mandatory/5 pts maximum)**
    f. **Cybersecurity Practitioners/Industry Partnerships (1 pt per partnership/1 pt mandatory/4 pts maximum)**

3. **"Center" for Cyber Education (10 pts mandatory/13 pts max)**
    a. **Services the "Center" provides (8 pts mandatory)**
    b. **Cyber "Center" external board of advisors (2 pts mandatory/5 pts maximum)**

4. **Cyber Faculty Qualifications and Courses Taught (10 pts mandatory/15 pts maximum)**
    a. **Head of the Cyber Program of Study (5 pts mandatory)**
    b. **Designated Alternate and Additional Faculty (1 pt each/1 pt mandatory)**
    c. **Faculty Cybersecurity Qualifications (1 pt each/1 pt mandatory)**
    d. **Cyber Defense Presentations (1 pt per presentation/5 pts maximum)**
    e. **Faculty support to Cyber Student activities, Clubs, Competitions, etc. (1 pt per item/1 pt mandatory)**

5. **Cyber Defense is a Multidisciplinary Practice at the Institution (7pts mandatory/15 pts maximum)**
    a. **Cyber Defense Concepts Taught in Other Fields of Study (1 pt per course/3 pts mandatory/5 pts maximum)**
    b. **Non-Cyber Defense Courses Encourage Papers, Projects or Test Questions in CD topics (1 pt each/3 pts mandatory/5 pts maximum)**
    c. **Professional Development Courses (1 pt per course/5 pts maximum)**

6. **Institutional Security Plan (6 pts mandatory/9 pts max)**
    a. **Security Plans (2 pts mandatory)**
    b. **Security Officer – provide name and job description (2 pts mandatory)**
    c. **Implementation of Cyber Security Practice (1 pt per example/2 pts mandatory/5 pts maximum)**

7. **Cyber Outreach/Collaboration Beyond the Institution (18 pts mandatory/30 pts max)**
    a. **Faculty Involvement in Sharing Expertise (1 pt per event/1pt mandatory/5 pts maximum)**
    b. **Transfer of Credit – 4-year institutions (1 pt per agreement/3 pts for statewide agreement/1 pt mandatory/5 maximum)**
    c. **Transfer of Credit or Partnerships - High School (1 pt per agreement/3 pts for statewide agreement/1 pt mandatory/5 maximum)**
    d. **Support/participation to the CAE Community (1pt per event/1pt mandatory/5 maximum)**
    e. **Community Outreach – Activities outside of student/campus events (1 pt per event/1 pt mandatory/5 maximum)**
    f. **Business/Industry Collaboration (1 pt per collaboration/1 pt mandatory/5 pts maximum)**

CYBERSECURITY EDUCATION
SOLUTIONS FOR THE NATION

National CyberWatch Center
Prince George's Community College
Room 129B
301 Largo Road
Largo, MD 20774

www.nationalcyberwatch.org