REPORT TEMPLATE
FOR A
NATIONAL CENTER OF ACADEMIC EXCELLENCE IN CYBER DEFENSE (NCAE-CD)

CAE-CD Designation APPLICATION
PRE-SUBMISSION REVIEW (PSR)

**Referenced Requirements, Figures and Appendices can be found in the June 2021 Draft of the**

[***CAE Cyber Defense (CAE-CD) Program Guidance - 2021***](https://public.cyber.mil/ncae-c/documents-library/)

**REPORT TEMPLATE
FOR A
NATIONAL CENTER OF ACADEMIC EXCELLENCE IN CYBER DEFENSE (NCAE-CD) DESIGNATION APPLICATION
PRE-SUBMISSION REVIEW (PSR)**

**Purpose:**

This document is provided as a tool to assist Pre-Submission Reviewers from the **CAE National Resource Center** at Whatcom Community College in the completion of a ***Pre-Submission Review Report*** for institutions applying for CAE-CD Designation by the **National Centers of Academic Excellence in Cybersecurity (NCAE-C)** Program Management Office.

**How to use this template:**

The template is provided as a Microsoft Word document for ease of editing. The reviewer should make a copy of this document for each institution being reviewed.

The template is created to act as a checklist which the reviewer can use to verify that all the application requirements have been met by the applying institution. This is done by using a color-coding scheme and by providing comments (described below) on changes/corrections which need to be completed by the institution to have a successful application.

This template uses the CAE-CD APPLICATION – CAE-C DESIGNATION CRITERIA as identified in the ***June 2021*** draft of the *National Centers of Academic Excellence in Cybersecurity - CAE 2020, Proposed Designation Requirements and Application Process* document prepared by the *Application Process and Adjudication Rubric (APAR) Working Group (WG).* This document can be found at:

[***CAE Cyber Defense Education (CAE-CD) Program Guidance - 2021***](https://www.ncyte.net/images/downloads/CAE-CD/20210608_CAE2021_Proposed_CAE-CD_Designation_Requirement.pdf)

*([https://www.ncyte.net/images/downloads/CAE-CD/20210608\_CAE2021\_Proposed\_CAE-CD\_Designation\_Requirement.pdf)](https://public.cyber.mil/ncae-c/documents-library/)*

 **Color Coding Scheme of Requirements:**

The use of a color-coding scheme provides an easy way for the reviewer to identify issues with a Requirement to the applying institution.

The Requirements have been placed in a two-column table. The first column is copy of the requirement as presented in the document referenced above. The second column is used by the reviewer to identify the severity of the issues, if any, which were identified.

The color scheme is as follows:

|  |  |
| --- | --- |
| Green – No issues were identified for the Requirement. |  |
| Yellow – Issues were identified which would not result in the application failing approval but should be corrected before submission. |  |
| Red – Issues were identified which would most likely result in an application not being approved. |  |

**Requirement Justification and Reviewer Comments:**

In addition to the color coding of requirements, space is provided for the reviewer to copy/paste the contents of the Justifications PDF and for Reviewer Comments.

***Justification Comments:***

* *If a Justifications file is provided, check for and identify errors (i.e. spelling, grammar, punctuation, acronyms which need to be spelled out, etc.) and any content that needs clarification.*
* *Explain any errors found.*
* *If a Justifications file was not provided enter ’Justifications not provided’. If no comments or corrections were identified enter ‘No comments/corrections identified’.*

***Reviewer Comments:***

* *The Reviewer Comments section is where the reviewer will explain any issues identified as Yellow or Red in the requirements table, as well as any issues identified with the Justification.*
* *If no comments or corrections were identified enter ‘No comments/corrections identified’.*

**Sample Letters and Program of Study (PoS) Review Comments:**

The template contains a copy of a *Sample Report Submission Letter*. The reviewer will use this letter to provide General Comments the institution should consider when completing the application. This is where the reviewer can identify any major issues identified by the review which the reviewer wants to emphasize to the institution.

The reviewer should also recommend whether the application is ready for submission.

The *Program of Study (PoS) Reviewer Comments* is where the reviewer can provide an overview of the review findings and identify any major issues identified by the review which the reviewer wants to emphasize to the institution. It also has a brief explanation of the review process that should be used when reviewing the application.

***The ‘Sample Report Submission Letter’ and the ‘Program of Study (PoS) Reviewer Comments’ should be amended as appropriate by the reviewer.***

National Center

of Academic Excellence

in Cyber Defense

(NCAE-CD) Designation Application

PRE-SUBMISSION REVIEW (PSR) Report FOR

***[Add Institution Name Here]***

Table of Contents

**Report Submission Letter3**

**CAE Designation Review Comments4**

**Recommended CAE Designation Application Changes5**

***Sample Report Submission Letter***

**Pre-Submission Reviewer Report For**

**Awesome Cybersecurity College (ACC)**

December 7, 2021

After reviewing the CAE Designation Application of Awesome Cybersecurity College (ACC), I believe ACC’s application is ready for submission, pending consideration of my comments and suggested changes.

SAMPLE

I believe ACC has demonstrated that it has a strong cybersecurity program, and the Bachelor of Science in Cybersecurity fulfills all the requirements for ACC to apply for CAE-CD Designation during the current submission cycle.

My reviewer comments regarding ACC’s CAE Designation Application are provided as part of this report. I would especially like to recognize the excellent job ACC did in documenting Criteria 9: Outreach for their institution.

I want to commend Mr. Al Heitkamper, ACC’s Point of Contact (POC), on the quality of his application and I feel confident that ACC’s application for CAE-CD Designation will be approved.

Please let me know if you have any questions regarding this report.

Sincerely,

Al Heitkamper

***Sample CAE Designation Review Comments***

**CAE Designation Reviewer Comments**

**Review Findings Overview**

After reviewing the CAE Designation Criteria (see **Review Process** below) of Awesome Cybersecurity College (ACC) I believe that ACC, after completing the recommended changes, will meet the CAE Designation requirements.

That said, I need to emphasize that this determination is based on my review process and that a final Peer Reviewer may raise other questions regarding the application.

**Review Process**

Below is a list of steps I took during this review:

* Reviewed each CAE Designation Criteria Requirement to ensure that the required information was provided.
	+ Verified that links, attachments, and/or justifications were provided for each Criteria Requirement.
* Opened and reviewed all attachments to verify that they are current and active.
* Navigated to any hyperlinks provided to verify that they are current and active.
* Reviewed the CAE Designation Criteria justifications, file names and hyperlinks for clarity, grammar, and spelling.

SAMPLE

**General Comments regarding CAE Designation Criteria**

Some things you can do to make the final reviewer’s job easier are:

* Name files and links to indicate what they contain or represent.
* Explain in your justification how the files/links relate to the Criteria Requirement you are justifying.
* Try not to make the reviewer search for information that supports the requirement.
* Do your best to help the reviewer get to know your institution.

Remember that the less a Peer Reviewer must look for support information outside your application, the faster and smoother the application review will go.

**Color Coding Scheme of Requirements**

The color scheme is as follows:

|  |  |
| --- | --- |
| Green – No issues were identified for the Requirement. |  |
| Yellow – Issues were identified which may not result in the application failing approval but should be corrected before submission. |  |
| Red – Issues were identified which would most likely result in an application not being approved. |  |

**Recommended CAE-CD Designation Application Changes**

The following criteria form the necessary documentation to demonstrate that the institution has the necessary resources, capacity, and processes to be a successful CAE-CD, and in the case of re-designation that it is also involved in the CAE-C program. All of the criteria are required of all CAE-CD applicants, both initial and at redesignation.

**Note: Referenced Figures and Appendices can be** **found in the June 2021 Draft of the:**

[***CAE Cyber Defense (CAE-CD) Program Guidance - 2021***](https://www.ncyte.net/images/downloads/CAE-CD/20210608_CAE2021_Proposed_CAE-CD_Designation_Requirement.pdf)

**Criteria 1: Accreditation**

The academic institution must be regionally accredited, as outlined by the Department of Education [(http://ope.ed.gov/accreditation/)](http://ope.ed.gov/accreditation/), to hold any CAE-C designation.

**Requirement:**

|  |  |
| --- | --- |
|  |  |
| 1. Provide URL at the academic institution’s domain to demonstrate that the academic institution is regionally accredited at the time of application.
 |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 2: Institution Commitment**

The letter of intent and endorsement, signed by the Provost or Higher, demonstrating that the institution is aware of the expectations and responsibilities associated with the CAE-C program. The letter must express institutional commitment to excellence in the cybersecurity field and support of the program the institution is submitting for CAE-C designation, identify the CAE point of contact (POC) from the institution, state institutional support of an official Cybersecurity Center within the institution, identify regional accreditation information, and list the program(s) of study supporting the requested designation. Submission of this letter acknowledges minimum participation expectations including: submission of an Annual Report or annual update of application data in the application tool; attendance at the CAE Community Symposium each year; regular communication with the CAE PMO, the CAE Community, and the CAE Regional Hubs (CRH); and active participate in the CAE Community and support of the CAE-Cybersecurity programs. This letter must be submitted early in the process to demonstrate that the institution supports the application, executive leadership acknowledges and supports the CAE program, and the institution is committed to meeting all required criteria throughout the life of the designation.

**Requirements (All needed):**

|  |  |
| --- | --- |
|  |  |
| ***2a. Provide a letter of intent and endorsement to participate in the CAE-C program (in PDF, do not mail) that:*** |  |
| 1. Written on official institution letterhead, signed by the Provost or higher and addressed to:

***National Security Agency*** ***Attn: CAE Program Director*** ***9800 Savage Road*** ***Ft. Meade, MD 20755-6804***  |  |
| 1. Identify regional accreditation information.
 |  |
| 1. Express institutional commitment to excellence in the cybersecurity field.
 |  |
| 1. Identify and provide institutional support of an established “Center” for Cybersecurity within the institution.
 |  |
| 1. Identify the CAE Point of Contact (POC) from the institution.
 |  |
| 1. Identify the name of a designated CAE Institutional Accounts Administrator (A person who oversees the CAE accounts across the institution - one who is authorized to switch POCs, activate new users, etc.).
 |  |
| 1. List the program(s) of study supporting the requested designation.
 |  |
| ***2b. Provide acknowledgement to follow the minimum participation expectations of a CAE-C:*** |  |
| 1. Submission of an Annual Report with all required information.
 |  |
| 1. Attendance at either (or both) the CAE Principal's Meeting and CAE Community Symposium each year.
 |  |
| 1. Regular communication with the CAE PMO, the CAE Community, and the CAE Regional Resource Center, including responding to email, offers input and suggestions for workshops, programs, program decisions, etc.
 |  |
| 1. Active participation in the CAE Community and support of the CAE-C program, including acting as a mentor or application reviewer, participation on working groups, supporting program initiatives, briefing or lecturing for the Tech Talks or CAE Forum webinars, and so on.
 |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 3: Evidences of Sound Cybersecurity Posture and Plan**

Institutions shall have a sound institutional cybersecurity posture and plan including a dedicated official to oversee its implementation to provide an overview of the institution’s ability to protect critical information and systems processing that information at the institution. The institution must demonstrate that they have the proper cybersecurity resources including a dedicated official, such as the CISO or CIO, with formal responsibility for the institution's cybersecurity posture and plan, that the cybersecurity posture and plan is maintained and functionally appropriate to mitigate cyber-attacks to the institutional information assets, and that the institution has a formal cybersecurity awareness program.

**Requirements (All needed):**

|  |  |
| --- | --- |
|  |  |
| 3a. Provide a signed letter on official letterhead from the officer assigned with direct responsibility for institutional cybersecurity, attesting to the fact that the institution has a sound cybersecurity posture and plan in place (in PDF) |  |
| 3b. Provide the name, title, and job description for the individual responsible for the institution cybersecurity program |  |
| 3c. Provide six separate examples of how the institution implements its cybersecurity plan through awareness, training and tutorials, log in security banners, user acknowledgements, online help and good security practice guides (e.g. Students, faculty and staff are required to take computer based training or online 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.) (in six separate PDFs). |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 4. Established “Center” for Cybersecurity**

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 current and visible within the institution and the external community at large. The “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 CAE-C program as a whole. This board provides a connection between the program(s), “Center”, college/department, and the local community. The external board of advisors can be shared with other programs in the college/department.

**Requirements (All needed):**

|  |  |
| --- | --- |
|  |  |
| ***4a. Provide URL at the academic institution’s domain to demonstrate that the academic institution has an established Website for the “Center” for Cybersecurity including:*** |  |
| 1. The “Center” Website (URL) is visible within the institution and the external community at large
 |  |
| 1. Center POC is noted on the “Center” Website
 |  |
| 1. Information about the cybersecurity PoS(s)
 |  |
| 1. Faculty members
 |  |
| 1. Links to student cybersecurity activities available to students at the institution and beyond
 |  |
| 1. News that include both internal and external cybersecurity news. Internal news should highlight cybersecurity activities and efforts at the institution and/or other cybersecurity activities of students and faculty representing the institution. External cybersecurity news should highlight up-to-date trending cybersecurity information
 |  |
| 1. Link to the institutional security resources and awareness
 |  |
| 1. Up-to-date links to key cybersecurity resources for students such as cyber competitions
 |  |
| 1. Documentation on the Industry Advisory Board
 |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 5: Affirmation of the CAE Core Values and Guiding Principles**

CAE-C at the academic institutions are characterized by several common attributes including academic excellence and institutional excellence. These attributes are built upon a foundation of ethical behavior, a sharing environment, and a willingness to lead by example. These form the core values and guiding principles of the CAE-C program. Applicant institutions will affirm their commitment to the CAE Core Values as part of the Designation application, and expected to follow the Guiding Principles indicated on each of the three Core Values ***(not to be submitted, affirmed only)***.

**5a. The Ethical Behavior Core Value:** The academic institution must encourage and support ethical behavior by students, faculty, administrators, and professional staff. It is expected that academic institutions with CAE-C Designation will have in place all the Guiding Principles noted below.

**Guiding Principles**

* The academic institution has appropriate systems, policies, and procedures that reflect the 20 support for and importance of ethical behavior for students, faculty, administrators, and 21 professional staff in their professional and personal actions.
* The academic institution has in place published policies and procedures to support legal and ethical behaviors.
* The academic institution has systems, policies, and procedures that provide appropriate 25 mechanisms for addressing breaches of ethical behavior
* The academic institution has in place systems for detecting and addressing breaches of ethical 27 behaviors, or other mechanisms to deter academic misconduct, such as honor codes, plagiarism 28 detection tools, and disciplinary systems to manage inappropriate behavior.

**5b. The Share Core Value:** The institution enables an environment in which students, faculty, administrators, professional staff, and practitioners can share, interact, and collaborate with others in the cybersecurity field.

**Guiding Principles**

* The academic institution has appropriate mechanisms for facilitating collaboration between 34 institutions, both CAE and non-CAE institutions.
* The academic institution has appropriate mechanisms to share resources, instructional material, 36 faculty, and/or facilities between institutions, both CAE and non-CAE institutions.
* The academic institution engages students, faculty, administrators, professional staff, and 38 practitioners in practices of successful information/resources sharing or joint events.

**5c.** **The Lead by Example Core Value:** The institution demonstrates a commitment to address, engage, 40 and respond to current and emerging cybersecurity issues in the classroom, the institution itself, and outside the institution.

**Guiding Principles**

* The institution leads multidisciplinary cybersecurity activities and/or programs.
* The institution leads cybersecurity outreach activities.
* The cybersecurity program functions are conducted as part of an institutional and/or college/departmental effort, beyond a single isolated professor’s efforts. This can include connection to the institutions mission, vision and strategic plans.

|  |  |
| --- | --- |
|  |  |
| 5a. Box checked to affirm that applying institution follows all the Ethical Behavior Core Value Guiding Principles. |  |
| 5b. Box checked to affirm that applying institution follows all the Share Core Value Guiding Principles. |  |
| 5c. Box checked to affirm that applying institution follows all the Lead by Example Core Value Guiding Principles. |  |

***Justification for Selected Requirement(s):***

* *Not applicable*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 6: Sustainability**

Sustainability of programs at the academic institution is an important component of the CAE-C program. Having full-time permanent faculty members associated with the “Center” and PoS Validated program(s) are needed to run the continuous improvement aspects of the program as well as elements such as outreach and ensure the continuous commitment to the CAE-C program Core Values at the institution. Having these fulltime permanent administration personnel, POC (who may be a faculty member as well), and faculty members identified in the application is part of assuring that the institution has the necessary resources, capacity, and processes for the cybersecurity program(s) to be successful.

**Requirements (All needed):**

|  |  |
| --- | --- |
|  |  |
| 1. Identify the administrative head of academic unit housing the established “Center” for Cybersecurity (Dean, Associate Dean, Department Chair, etc.) including name, phone number, e-mail address, and indicate the number of year(s) the individual has been working full-time for the academic institution.
 |  |
| 1. Provide CV of the administrative head of academic unit housing the established “Center” for Cybersecurity (in PDF).
 |  |
| 1. Identify the Point-of-Contact (POC) for the established “Center” for Cybersecurity (Department chair, faculty lead, CAE POC, etc.) including name, phone number, e-mail address, and indicate the number of year(s) the individual has been working full-time for the academic institution.
 |  |
| 1. Provide CV of the established “Center” for Cybersecurity POC and indicate year the individual joined the academic institution (in PDF).
 |  |
| 1. Identify the alternate POC for the established “Center” for Cybersecurity including name, phone number, e-mail address, and indicate the number of year(s) the individual has been working full-time for the academic institution.
 |  |
| 1. Provide CV of the established “Center” for Cybersecurity alternate POC (in PDF).
 |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 7: Professional Development**

Professional development for faculty and students at the academic institution is an important component of the CAE-C program. Ongoing access to working professionals and practitioners during their time in a CAE-C program is needed by both faculty and student in order to maintain and improve the program as well as a crucial component of elements such as outreach, industry and government connections, awareness of the quality of the faculty and students at the institution, etc. There are many formats for such professional development opportunities, but the obvious elements are guest lecturers working in cybersecurity industry and government, internship opportunities for students, joint events with the institutional career development and student job placement center focused on cybersecurity, etc. Faculty development maybe in the form of encouragement and time release and/or financial support to attend and participate in cybersecurity training, professional certifications, relevant conferences, faculty exchange program with industry and/or government, summer research programs for faculty, and/or other events are critical. Identifying these professional development opportunities for faculty and students in the application is part of assuring that the institution has the necessary resources, capacity, and processes for synergistic success. The established “Center” for Cybersecurity at the institution is the likely sponsor for these activities or shared with the department/college it is housed at. What is important is that these activities are available to faculty and students, while occurring regularly during the academic year.

**Requirement:**

|  |  |
| --- | --- |
|  |  |
| 1. Provide six separate examples of professional development opportunities provided to faculty and students over the past three years. Evidence files can be fliers, posters, letters, attendance records, or other evidence of professional development for faculty and students (in six different PDFs).
 |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 8. Cybersecurity Academic Integration**

The institution shall demonstrate that cybersecurity is not treated as an isolated discipline and cybersecurity concepts are also integrated into additional degree programs within the institution outside the PoS(s) applied for or previously validated. For example: healthcare students learning about privacy and patient data protection, or accountants learning about data backup and protection, or students in law school and/or criminal justice learning about privacy laws and cyber-crime. Courses in this criterion cannot be courses in the applied for or previously validated PoS.

**Requirements (All needed):**

|  |  |
| --- | --- |
|  |  |
| 8a. Identify the course and academic unit (department/college/etc.) at the institution where students from non-validated PoS (or non-PoS(s) applied for validation) are exposed to cyber concepts. |  |
| 8b. Provide three different syllabi of courses where cyber modules clearly highlighted from other departments/colleges. Combine the syllabus, guidelines (i.e. what students are asked to do) of the work, and one sample student work into a single file for each of the three courses (In three PDFs). |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 9. Outreach**

One of the core values of the CAE-C program is sharing of cyber defense expertise. The institution must demonstrate how cyber defense practices are extended beyond the normal boundaries of the institution. Outreach activities help show how cyber defense concepts developed at the institution are shared with others or how industry theory and practice are incorporated into curriculum. Moreover, outreach activities allow the cybersecurity program to engage with business and industry to provide pathways for graduates while maintaining an appropriate curriculum to place graduates into those jobs. Examples of outreach and collaboration include:

* Participation in CAE events such as: CAE Community Symposia, CAE Regional Hubs (CRH) workshops for candidate institutions, CAE Tech Talks/Forums used in classroom, collaboration on grants with CAE-C institutions.
* Faculty members collaborating with current CAE-C institutions on research, grants, course development, etc.
* Faculty and/or staff participating as CAE reviewers/mentors/advisors, etc.
* Faculty and/or staff participating on FBI affiliated InfraGard [(https://InfraGard.org/)](https://infragard.org/) as members, and/or chapter board and/or sector chiefs, USSS Electronic Crime Task Forces, DHS Regional Domestic Task Forces, and/or other national, regional, state, and/or local cybersecurity working groups, task forces, and leadership positions.
* Faculty and/or staff sponsorship or oversight of cybersecurity 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, presentations on 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.).
* Involvement with industry (internships for students, identifying needs of business partners for course content, job fairs, guest speakers, etc.).
* Institution partners with companies and other employers to identify cybersecurity needs of potential employers and encourage student internships.

**Requirements (All needed):**

|  |  |
| --- | --- |
|  |  |
| 9a. Provide evidence of how the institution has shared cyber related curriculum and/or faculty with other schools, to include K-12 schools, community colleges, technical schools, minority colleges/universities to advance cyber defense knowledge within the last three years. Identify specific materials 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 (in PDF). |  |
| 9b. Provide evidence (three) that the applying institution has participated in CAE events such as: CAE Community Symposium, CRRC workshops for candidate institutions, CAE Tech Talk/Forum used in classroom, collaboration on grants with CAE institutions (Three separate PDFs). |  |
| 9c. Provide at least three evidences that faculty members from the applying institution has contributed to the CAE community such as: served as PoS Validation and/or CAE-C Designation mentors, reviewers, members of the CAE Working Groups, presented in CAE Community Symposiums, CRRC workshops, CAE Tech Talk/Forum (Three separate PDFs). |  |
| 9d. Provide evidence of faculty members collaborating with current CAE-C institutions on research, grants, course development, etc. (in PDF). |  |
| 9e. Provide evidence of faculty members/employee sponsorship or oversight of students for Cyber events for the community at large. Events could include Cyber awareness and education for local schools, adult education centers, senior centers, camps, first responder training and the surrounding community. |  |
| 9f. Provide evidence on how the institution works with employers and students to support placement for cyber related internships and jobs, such as via institutional Career Development Services (i.e. HandShake) and industry events on-campus (in PDF). |  |
| 9g. Provide evidence of obtaining input on curriculum to meet industry needs (in PDF). |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*

**Criteria 10. Transfer of Credit/Articulation Agreements**

Transfer of Credit/Articulation Agreements with other academic institutions are important and needed to demonstrate the pipeline in cybersecurity, in the context of offering a concentration and/or cybersecurity (or related field) degrees/areas of study/track and/or certificates. Agreements should be with community colleges, technical schools, minority colleges/universities, other colleges/universities, and/or with high schools (cyber-related or technical pre-requisites, not just general pathway programs). United States Military Academies are exempt (provide justifications).

**Requirement:**

|  |  |
| --- | --- |
|  |  |
| 1. Provide evidence that the institution awards credit in cybersecurity related courses and/or technical prerequisite courses from other academic institutions, community colleges, tech schools, etc. or through alternative means. Examples include but are not limited to: transfer agreements with community colleges, articulation agreements, statewide transfer agreements, articulation agreements, college in the high school, dual credit, running start, credit for prior learning, credit for military training or occupation, and/or membership in Transfer Evaluation Services (TES) (in PDF).
 |  |

***Justification for Selected Requirement(s):***

* *Justifications not provided.*

***Reviewer Comments:***

* *No comments/corrections identified.*