Alignment of AI Knowledge Units and Cybersecurity Competencies for PUPR's Programs of Study

Roberto Vivas Gotay
Master in Computer Science
Advisor: Dr. Alfredo Cruz, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project EXPO, February 2026

Abstract **–** *The rapid integration of artificial intelligence into cybersecurity practice has increased the need for precise, curriculum-level alignment between emerging artificial intelligence concepts and established national cybersecurity education frameworks. This master's degree project presents a structured alignment of Artificial Intelligence in Cybersecurity knowledge units with the proposed Master of Science in Computer Science curriculum at the Polytechnic University of Puerto Rico. Rather than designing new curricular content, this work analyzes existing and planned graduate courses to identify where artificial intelligence–enabled cybersecurity concepts are already embedded and how they can be formally documented to support accreditation and program evaluation requirements. In addition, competency statements were developed for cybersecurity-related courses and aligned with nationally recognized cybersecurity workforce frameworks to support workforce relevance. The results demonstrate that a curriculum-first alignment strategy can meet the expectations of the Artificial Intelligence in Cybersecurity program while preserving existing course structures. This approach provides a replicable framework for institutions seeking to integrate artificial intelligence considerations into graduate cybersecurity education without redesigning the curriculum.*

Key Terms **–** *AI Cyber Knowledge Units, Cybersecurity Education, Graduate Competencies, Workforce Development.*

INTRODUCTION

The increasing adoption of artificial intelligence (AI) across modern cybersecurity operations has introduced new challenges for higher education institutions tasked with preparing graduates for an evolving threat landscape. AI techniques are now routinely applied to malware detection, intrusion analysis, automated incident response, and security analytics, requiring cybersecurity professionals to possess not only traditional defensive skills but also foundational knowledge of AI concepts and their ethical, operational, and security implications. As a result, academic programs must ensure that their curricula remain aligned with national cybersecurity education standards while also incorporating emerging AI-related competencies.

In response to these developments, federal and academic initiatives such as the Artificial Intelligence Cybersecurity (AICyber) framework and the National Centers of Academic Excellence in Cyber Defense (CAE-CD) program have emphasized the importance of formally documenting knowledge units, learning outcomes, and competencies that reflect both cybersecurity fundamentals and AI-enabled security practices [1]. However, integrating these frameworks into existing graduate curricula presents practical challenges. Many programs already contain relevant technical content but lack explicit alignment artifacts that demonstrate compliance with accreditation and workforce development expectations.

This master's degree project addresses this gap by structuring the alignment of AICyber knowledge units with the planned graduate curriculum of the Polytechnic University of Puerto Rico [2]. Additionally, selected course-level competencies are mapped to CAE-CD cybersecurity knowledge units to support institutional accreditation efforts. Rather than proposing new courses or redesigning existing ones, this work focuses on identifying how current and planned coursework already supports AI-

relevant cybersecurity concepts and documenting those relationships in a manner consistent with CAE-CD and AICyber guidance.

By adopting a curriculum-first and competency-driven alignment approach, this project demonstrates how graduate programs can incorporate AI considerations into cybersecurity education without disrupting established academic structures. The outcomes of this study provide a practical framework for educational institutions seeking to strengthen their alignment with national cybersecurity and AI education initiatives while maintaining program coherence and academic rigor.

Related Work

Prior research related to this project spans three primary areas: the integration of artificial intelligence concepts into cybersecurity education, the use of formal knowledge unit frameworks for curriculum standardization, and competency-based approaches to cybersecurity workforce preparation. Together, these bodies of work establish the academic and institutional context that motivates the alignment-focused methodology adopted in this study.

Artificial Intelligence in Cybersecurity Education

The growing use of AI in cybersecurity has been widely documented in both academic literature and workforce development initiatives. Studies examining AI-enabled cybersecurity techniques often emphasize applications such as anomaly detection, malware classification, automated threat intelligence, and decision-support systems [1]. As these technologies mature, researchers have increasingly highlighted the need for cybersecurity professionals to understand not only how AI models are applied, but also their limitations, security risks, and ethical implications. This has led to calls for the explicit inclusion of AI-related learning objectives within cybersecurity curricula, particularly at the graduate level, where analytical depth and system-level understanding are expected. Educational research further indicates that simply embedding AI-related tools into coursework is insufficient without a structured pedagogical framework. Programs that lack formal documentation of AI learning outcomes risk misalignment with national education standards and difficulty demonstrating compliance during accreditation reviews. These findings support the need for structured alignment mechanisms, such as knowledge units and competencies, rather than ad hoc curricular additions.

Knowledge Unit Frameworks and Curriculum Standardization

Knowledge unit frameworks have long been used to standardize cybersecurity education and promote consistency across academic institutions. The National Centers of Academic Excellence in Cyber Defense (CAE-CD) program defines a set of cybersecurity knowledge units that institutions must demonstrate coverage of to achieve or maintain designation. These knowledge units serve as formal artifacts linking course content to nationally recognized cybersecurity competencies.

More recently, the Artificial Intelligence Cybersecurity (AICyber) initiative has emerged to address the intersection of AI and cybersecurity education. AICyber emphasizes identifying AI-relevant cybersecurity knowledge units that reflect emerging technical, operational, and ethical considerations. Unlike traditional cybersecurity frameworks, AICyber explicitly focuses on how AI both enables and challenges cybersecurity systems, requiring careful integration into existing curricula. The existing literature on curriculum mapping demonstrates that alignment with such frameworks is most effective when implemented at the course and competency levels, rather than through wholesale curriculum redesign. This approach allows institutions to preserve academic continuity while still producing the documentation necessary for accreditation and workforce alignment.

Competency-Based Cybersecurity Education

Competency-based education has become a central component of cybersecurity workforce development, particularly in programs aligned with federal and defense-oriented standards.

Competencies provide measurable statements of what students are expected to know and be able to do upon completion of a course or program. Prior studies emphasize that competencies are most effective when they are explicitly linked to course content, assessment methods, and recognized external frameworks.

In the context of CAE-CD accreditation, competency statements serve as a critical bridge between abstract knowledge units and practical educational outcomes. Research in this area highlights that well-defined competencies improve curriculum transparency, support continuous program assessment, and facilitate communication with external stakeholders, including accrediting bodies and employers.

Despite this, prior work also notes that many academic programs struggle to produce consistent, well-aligned competency documentation, particularly when incorporating emerging domains such as AI. This challenge reinforces the importance of structured alignment methodologies that map existing coursework to established frameworks rather than introducing entirely new instructional domains.

METHODOLOGY

This section describes the structured process for analyzing graduate course artifacts, mapping curriculum coverage to AICyber knowledge units, and validating cybersecurity workforce alignment in support of CAE-CD requirements.

Overview of the Alignment Methodology

This master's project follows a structured, artifact-driven alignment methodology designed to map graduate-level cybersecurity coursework to Artificial Intelligence Cybersecurity (AICyber) knowledge units and CAE-CD cybersecurity requirements. The methodology emphasizes documentation, traceability, and validation, rather than curriculum redesign, consistent with CAE-CD documentation and evaluation practices [3]. All alignment decisions are grounded in existing course syllabi, learning outcomes, topical coverage, and formally defined competency statements developed as part of this project.

Figure 1 provides a high-level overview of the alignment workflow employed in this study, illustrating the progression from curriculum artifact collection to final knowledge unit and competency validation.

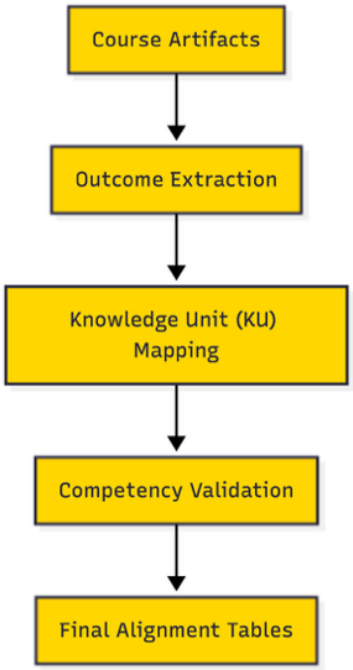


Figure 1
Curriculum-to-Knowledge Unit Alignment Workflow

Data Sources and Curriculum Scope

The primary data sources for this study consist of official graduate course documentation from the Master of Computer Science program at the Polytechnic University of Puerto Rico, including the proposed curriculum structure for the Area of Interest in Artificial Intelligence in Cybersecurity (AICyber) [2] [4]. These sources include course syllabi, catalog descriptions, learning outcomes, topical breakdowns, and assessment expectations. In addition, this project incorporates formally developed competency statements for selected courses, structured according to workforce-aligned templates. The scope of analysis includes cybersecurity, artificial intelligence, and AI-enabled cybersecurity courses relevant to AICyber and CAE-CD alignment. Courses without direct relevance to

these domains were excluded to maintain analytical focus. A complete listing of courses included in the study is summarized in *Table 1*.

Table 1
Graduate Courses Included in the Alignment Study for Competencies and Knowledge Units

Course Code	Course Title
CECS 6005	Principles of Information Security
CECS 6010	Advanced Design and Analysis of Algorithm
CECS 6027	Ethics in AI
CECS 6030	Computational Theory
CECS 6230	IT Operations
CECS 7235	Computer Forensics
CECS 6605	Advanced Database Systems
CECS 7230	Network Security
CECS 7237	Advanced Computer Forensics
CECS 7550	Artificial Intelligence
CECS 7570	Computer Security
CECS 6015	IT Auditing and Secure Operations
CECS 6017	Python Programming for AI and Data Analytics
CECS 6037	Threats in AI Security
CECS 6045	Law, Investigation, and Ethics
CECS 6046	Electronic Discovery & Digital Evidence
CECS 7717	Machine Learning
CECS 7727	AI for Cybersecurity
CECS 7950	Project for MCS
CECS 7951	Project Extension for MCS

Knowledge Unit Mapping Process

The alignment process was conducted in three successive layers: Knowledge Unit identification, course-level mapping, and program-level validation.

First, AICyber knowledge units were categorized into Cyber Foundational, AI Foundational, Core, and Optional groups, consistent with program-of-study requirements [5] [6]. Each graduate course was reviewed to identify explicit and implicit coverage of AICyber knowledge units as defined in the AICyber knowledge unit documentation [6].

Second, course-level mappings were documented in detailed alignment matrices, associating each course with one or more AICyber knowledge units. This process resulted in a comprehensive mapping artifact that captures both breadth and depth of coverage across the curriculum.

Figures 2, 3, and 4 illustrate the distribution of AICyber knowledge unit coverage across the graduate curriculum.

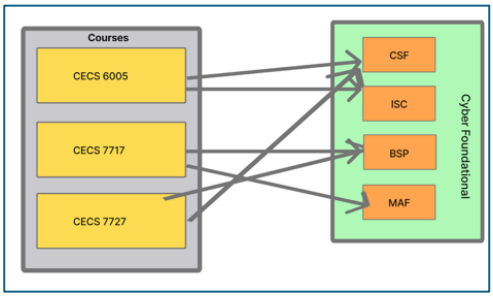


Figure 2
Final Alignment of Cyber Foundational (AICyber) Knowledge Units Across Graduate Courses

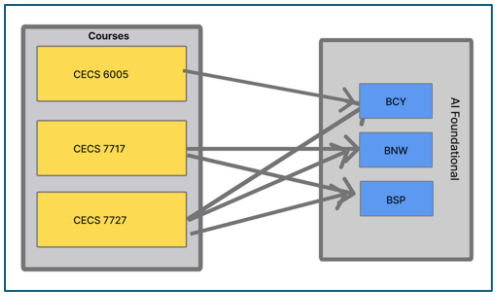


Figure 3
Final Alignment of AI Foundational (AICyber) Knowledge Units Across Graduate Courses

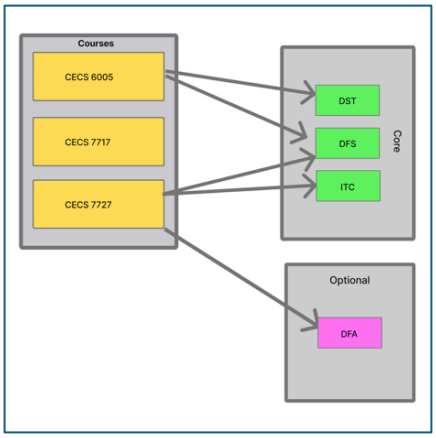


Figure 4
Final Alignment of AI Foundational (AICyber) Knowledge Units Across Graduate Courses

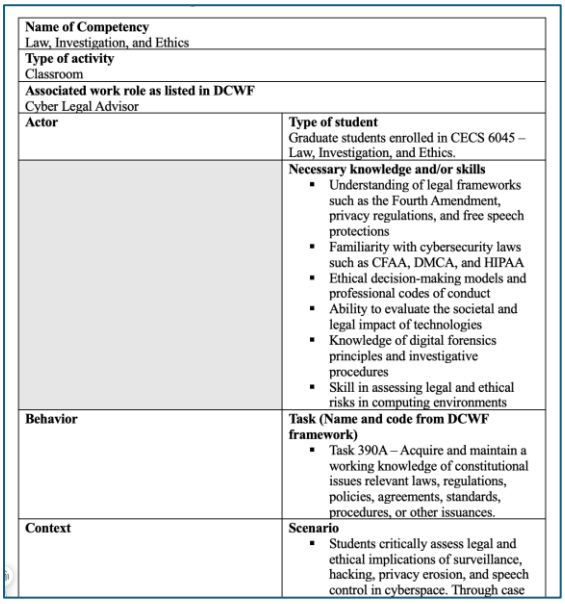
This mapping is fully documented in the detailed and final alignment artifacts developed for this project.

Competency Development and Workforce Framework Alignment

To support CAE-CD program requirements, course-level competency statements were developed only for cybersecurity-related courses within the graduate curriculum. This scope limitation reflects the fact that the NICE Framework and the Department of Defense Cyber Workforce Framework (DCWF) are cybersecurity-focused workforce models and are not intended for application to non-cyber or purely theoretical computer science courses.

The competency statements were written using a standardized template to ensure consistency, measurability, and traceability to instructional intent, in accordance with CAE-recommended competency development practices [7]. Each competency specifies expected student performance, assessment thresholds, and instructional context using an actor–behavior–context–degree–employability (ABCDE) structure [8].

Figure 5 shows the template used in Microsoft Word software.



Name of Competency Law, Investigation, and Ethics	
Type of activity Classroom	
Associated work role as listed in DCWF Cyber Legal Advisor	
Actor	**Type of student** Graduate students enrolled in CECS 6045 – Law, Investigation, and Ethics.
	Necessary knowledge and/or skills ▪ Understanding of legal frameworks such as the Fourth Amendment, privacy regulations, and free speech protections ▪ Familiarity with cybersecurity laws such as CFAA, DMCA, and HIPAA ▪ Ethical decision-making models and professional codes of conduct ▪ Ability to evaluate the societal and legal impact of technologies ▪ Knowledge of digital forensics principles and investigative procedures ▪ Skill in assessing legal and ethical risks in computing environments
Behavior	**Task (Name and code from DCWF framework)** ▪ Task 390A – Acquire and maintain a working knowledge of constitutional issues relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.
Context	**Scenario** ▪ Students critically assess legal and ethical implications of surveillance, hacking, privacy erosion, and speech control in cyberspace. Through case

Figure 5
Competency Template in Microsoft Word

Figure 6 demonstrates the other platform used for Competency Construction, called the Competency Constructor.

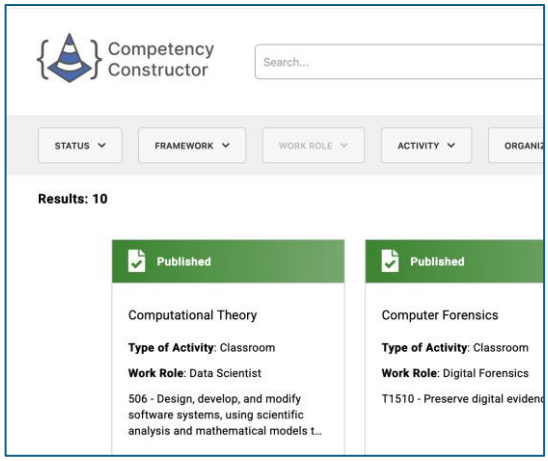


Figure 6
Competency Constructor Platform

Rather than mapping competencies to CAE-CD knowledge units, the developed competencies were aligned with recognized cybersecurity workforce frameworks, specifically the NICE Framework and the Department of Defense Cyber Workforce Framework (DCWF) [9] [10]. For each cybersecurity-related course, competencies were associated with relevant workforce work roles and task statements derived from the NICE Framework and the Department of Defense Cyber Workforce Framework (DCWF), consistent with CAE competency guidance [7] [9] [10]. This alignment provides workforce-oriented validation of course content while remaining consistent with CAE-CD expectations for demonstrating alignment with external frameworks and workforce relevance.

Table 2 summarizes representative competency-to-workforce framework alignments for selected cybersecurity courses.

Table 2
Cybersecurity Courses with Competencies Aligned

Course	Framework	Work Role
Advanced Computer Forensics	NICE	Digital Forensics
Advanced Database Systems	NICE	Database Administration

Computer Security	DCWF	Security Control Assessor
Electronic Discovery & Digital Evidence	DCWF	Cyber Crime Investigator
IT Auditing & Secure Operations	NICE	Technology Program Auditing
Law, Investigation, and Ethics	DCWF	Cyber Legal Advisor
Network Security	DCWF	Network Analyst
Final Project Course	DCWF	Research Development Specialist
Advanced Design and Analysis of Algorithms	NICE	Secure Software Development
Computational Theory	DCWF	Data Scientist
Computer Forensics	NICE	Digital Forensics
IT Operations	DCWF	Cyber Defense Infrastructure Support Specialist
Principles of Information Security	NICE	Systems Security Analysis

All competency artifacts are documented in the course-specific competency files developed as part of this project and serve as supporting evidence of workforce alignment for CAE-CD evaluation purposes.

Program-Level Validation and Dominance Analysis

The final phase of the methodology involved validating the completeness of alignment at the program level. Using the compiled course mappings, master alignment tables were constructed to evaluate whether the program satisfies AICyber program-of-study requirements, including minimum coverage of foundational, core, and optional knowledge units.

When multiple courses are aligned to the same knowledge unit, a row dominance principle was applied to identify primary contributors and reduce redundancy. This resulted in alternative final alignment configurations, each demonstrating compliance while highlighting different instructional emphases.

Figure 7 visualizes the step-by-step process of classifying and validating portions of the Row Dominance Validation Process.

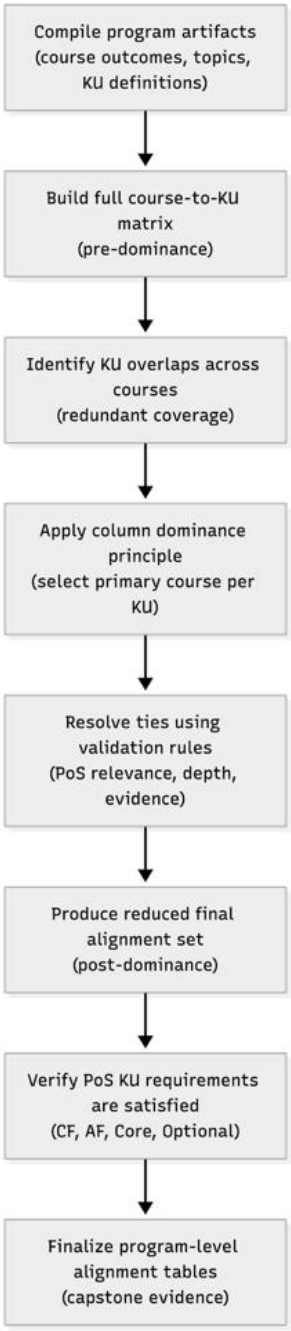


Figure 7
Row Dominance Validation Process

Methodological Rigor

This methodology prioritizes transparency and reproducibility. All alignment decisions are traceable to documented course artifacts and competency statements. By focusing on structured documentation rather than curricular modification, the approach supports accreditation review, curriculum assessment, and future program evolution without disrupting established academic structures.

RESULTS

This section presents the outcomes of the curriculum alignment process described in the Methodology. The results are organized into two parts: (1) final AICyber program-level knowledge unit alignment outcomes, and (2) cybersecurity workforce framework alignment outcomes derived from course-level competencies. Together, these results demonstrate compliance with the AICyber program-of-study requirements and the workforce-relevance expectations associated with the CAE-CD evaluation.

AICyber Program-Level Alignment Outcomes

The finalized alignment confirms that the Master of Computer Science curriculum with a specialization in Artificial Intelligence in Cybersecurity satisfies all required AICyber program-of-study knowledge unit categories [6]. Using the structured knowledge unit mapping process and subsequent program-level validation, the curriculum demonstrates coverage of Cyber Foundational, AI Foundational, Core, and Optional AICyber knowledge units.

Following the application of the row dominance principle, primary course contributors were identified for each knowledge unit to reduce redundancy while preserving required coverage. The resulting alignment ensures that each unit of knowledge needed is supported by at least one graduate-level course with sufficient depth and relevance. The final validated alignment is documented in the master alignment tables and visually supported by the row dominance validation workflow shown earlier.

Overall, the results show that the program meets AICyber structural requirements without the need for curriculum modification, confirming that existing and planned coursework already embeds AI-enabled cybersecurity concepts in a manner consistent with AICyber expectations.

Cybersecurity Workforce Framework Alignment Outcomes

In addition to knowledge unit alignment, workforce framework alignment results were derived from course-level competency development for cybersecurity-related courses only. Competencies were aligned with either the NICE Framework or the Department of Defense Cyber Workforce Framework (DCWF), depending on the course focus and intended workforce relevance.

The results indicate that multiple cybersecurity courses clearly define workforce roles across defensive operations, digital forensics, secure software development, cyber law, infrastructure support, and security analysis. These alignments demonstrate that the curriculum supports both technical and professional workforce preparation through documented learning outcomes and performance expectations.

Table 2 summarizes the cybersecurity courses for which competencies were developed and identifies the corresponding workforce frameworks and supported work roles. These results provide external validation of workforce relevance while remaining distinct from AICyber knowledge unit alignment activities.

DISCUSSION

The results of this study demonstrate that a curriculum-first alignment strategy can effectively integrate artificial intelligence considerations into graduate cybersecurity education without requiring structural changes to existing courses. By distinguishing between knowledge-unit alignment and workforce-competency alignment, this project provides a clear, defensible framework for meeting

both AICyber and CAE-CD expectations while preserving academic coherence.

Separation of Knowledge Units and Workforce Competencies

One of the key outcomes of this project is the explicit separation between AICyber knowledge unit alignment and workforce competency development. Knowledge units were used to evaluate curriculum coverage at the program level, ensuring that foundational, core, and optional AICyber requirements were satisfied. In contrast, competencies were developed only for cybersecurity-related courses and aligned with external workforce frameworks, namely NICE and the Department of Defense Cyber Workforce Framework (DCWF). This separation is consistent with CAE-aligned guidance that distinguishes curriculum-level knowledge unit coverage from workforce-oriented competency frameworks used for role and task validation [5]. This approach aligns with CAE guidance, which emphasizes competencies as task- and work-role–oriented constructs rather than curriculum-level knowledge unit descriptors [7].

This separation strengthens the alignment model by preventing the misapplication of workforce frameworks to non-cyber or theoretical courses while still demonstrating workforce relevance where appropriate. It also aligns with CAE-CD guidance, which emphasizes curriculum coverage and external validation without mandating a one-to-one mapping between competencies and knowledge units.

Impact of the Row Dominance Principle

The application of the row dominance principle played a critical role in validating program-level alignment. Rather than treating all course-to-knowledge unit mappings equally, dominance analysis identified primary contributors for each knowledge unit based on relevance and instructional depth. This approach reduced redundancy in the final alignment tables while maintaining full coverage of required AICyber categories.

From an accreditation perspective, this enhances clarity and defensibility by demonstrating intentional curriculum design rather than incidental overlap. For institutional review and future curriculum assessment, dominance analysis also provides a scalable mechanism for evaluating how changes to individual courses may affect overall program alignment.

Institutional and Accreditation Implications

The findings suggest that institutions pursuing AICyber and CAE-CD alignment can leverage existing curricula more effectively by focusing on documentation, validation, and structured mapping rather than course redesign [1]. The methodology presented in this project enables programs to generate alignment artifacts that support accreditation review, workforce relevance, and internal quality assurance without introducing unnecessary instructional disruption, consistent with CAE-CD evaluation guidance [5] [11].

Additionally, integrating the NICE and DCWF frameworks at the competency level provides external validation of workforce preparation while remaining flexible to future updates to national cybersecurity workforce models [9] [10]. This positions the program to adapt to evolving federal guidance without requiring substantial revisions to its academic structure.

Limitations

This study is limited to a single institution and a specific graduate program context. Alignment decisions were based on documented course artifacts and competency statements, which may not fully capture informal instructional practices or evolving course content. Furthermore, the alignment reflects the current state of AICyber knowledge units and workforce frameworks, both of which may become.

CONCLUSIONS AND FUTURE WORK

This master's degree project demonstrates that a structured, curriculum-first alignment approach can effectively integrate artificial intelligence considerations into graduate cybersecurity education

while maintaining consistency with established accreditation and workforce frameworks. By aligning existing and planned graduate courses with AICyber knowledge units and validating cybersecurity-focused coursework against workforce frameworks, this study provides a practical, replicable model for institutional alignment that does not require curriculum redesign.

The results confirm that the program satisfies all required AICyber program-of-study knowledge unit categories through documented course coverage and program-level validation. The application of the row dominance principle further strengthened the alignment by reducing redundancy and identifying primary course contributors, improving clarity and defensibility for accreditation and curriculum review purposes. In parallel, the development of cybersecurity-specific competencies aligned with the NICE Framework and the Department of Defense Cyber Workforce Framework (DCWF) demonstrated workforce relevance while respecting the scope and intent of these frameworks.

Collectively, these outcomes illustrate how academic institutions can balance emerging AI-enabled cybersecurity requirements with existing curricular structures. The methodology emphasizes documentation, traceability, and validation, offering a scalable pathway for supporting CAE-CD evaluation, internal program assessment, and future curricular evolution.

Future Work

Future extensions of this work include expanding the alignment framework to additional institutions or undergraduate programs to evaluate its generalizability across different academic contexts. As AICyber knowledge units and cybersecurity workforce frameworks continue to evolve, periodic reassessment of alignment artifacts will be necessary to maintain compliance and relevance. Future research may also explore integrating assessment data to quantitatively evaluate the effectiveness of aligned courses in achieving intended learning and workforce outcomes.

Additionally, further work could examine the applicability of similar alignment methodologies to adjacent domains where artificial intelligence intersects with other computing disciplines, such as software engineering, data science, and privacy engineering. Such efforts would support broader institutional strategies for integrating AI considerations into computing education while maintaining alignment with national standards and workforce expectations.

REFERENCES

[1] Towson University. (2024). *NSA CAE AI Workshop – Artificial Intelligence and Cybersecurity Education* [Online]. Available: https://wp.towson.edu/secured-lab/nsa-cae-ai-workshop-march-2024/. [Accessed: Feb. 3, 2026].

[2] Polytechnic University of Puerto Rico. (2025). *Master's Program in Computer Science* [Online]. Available: https://pupr.edu/master-computer-science/. [Accessed: Feb. 3, 2026].

[3] National Centers of Academic Excellence in Cybersecurity. (2025). *CAE-CD Document Library* [Online]. Available: https://www.cyber.mil/ncae-c/document-library. [Accessed: Feb. 3, 2026].

[4] Polytechnic University of Puerto Rico, "Proposed Master of Science in Computer Science Curriculum with Area of Interest in Artificial Intelligence in Cybersecurity (AICyber)," *Graduate School Curriculum Flowchart*, 2025.

[5] National Centers of Academic Excellence in Cybersecurity. (2024). *Artificial Intelligence and Cybersecurity Curriculum Guidance, unpublished document* [Online]. Available: https://docs.google.com/document/d/1K5DSnXWfrJilXuMTB5n8UOcSfLr1HbDx. [Accessed: Feb. 3, 2026].

[6] National Centers of Academic Excellence in Cybersecurity. (2024). *Cyber + AI Knowledge Units (AICyber), unclassified report* [Online]. Available: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cyber_ai_kus_stoneman.pdf. [Accessed: Feb. 3, 2026].

[7] V. Nestler and Z. Fowler, "CAE Approach to Competency," presentation, Careers Preparation National Center, funded by the National Centers of Academic Excellence in Cybersecurity (NSA Grant H98230-22-1-0329), Mar. 2024.

[8] Careers Preparation National Center, "Competency in Cybersecurity Education: A Handbook for Educators at NCAE-C Designated Institutions," Version 2, Mar. 2024.

[9] Cybersecurity and Infrastructure Security Agency. (2025). *NICE Cybersecurity Workforce Framework* [Online].

Available: https://niccs.cisa.gov/tools/nice-framework. [Accessed: Feb. 3, 2026].

[10] Department of Defense. (2025). *DoD Cyber Workforce Framework (DCWF)* [Online]. Available: https://www.cyber.mil/dod-workforce-innovation-directorate/dod-cyber-workforce-framework. [Accessed: Feb. 3, 2026].

[11] National Centers of Academic Excellence in Cybersecurity. (2025). *CAE-CD Designation Requirements, Version 2.0* [Online]. Available: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/20250623_CAE2025_CAE-CD_Designation_Requirements_Ver2.0.pdf. [Accessed: Feb. 3, 2026].