KU Alignment with PUPR's Program of Study

Rose A. Luna Rivera
Master in Computer Science
Advisor: Alfredo Cruz, Ph.D.
Polytechnic University of Puerto Rico
Graduate Project EXPO, October 2025

Abstract *– Academic institutions have the chance to become recognized as a Center of Academic Excellence (CAE). This recognition demonstrates that the institution meets the standards for cybersecurity curriculum. The requirements for receiving the CAE recognition are regularly updated. The most recent update was from January 2025. As part of the recognition process, the academic institution must align the degree's courses with a certain number of Knowledge Units (KUs). Additionally, the institution must choose between two categories: technical core and non-technical core. This project mapped and aligned PUPR's Master of Science in Computer Science with a specialization in Cybersecurity with these designation requirements, specifically the KUs. The process was carried out by using the courses of the said program, their syllabuses, the textbooks used in each course, and the KUs' learning outcomes and their corresponding topics. This project aimed to align the educational program with the two categories: technical core and non-technical core. The result reflected favorably for the academic institution.*

Key Terms *– CAE-CD, Cybersecurity Curriculum, Knowledge Units, Mapping.*

INTRODUCTION

The National Centers of Academic Excellence in Cybersecurity (NCAE-C) is a program managed by the National Security Agency (NSA). It is partnered with various federal agencies [1] [2]. The purpose of the NCAE-C program is to build a cybersecurity educational initiative in collaboration with educational entities. As a result, cybersecurity curriculum standards are established, and students are encouraged to develop competencies and pursue professional development.

Academic institutions must apply for NCAE-C and choose from three designations: Cyber Defense, Cyber Research, and Cyber Operations. By receiving one of these designations, the academic institution demonstrates that it meets the desired characteristics of a Center of Academic Excellence (CAE) and offers a high-quality cybersecurity education [1] [2].

The application for the National Center of Academic Excellence in Cyber Defense designation (NCAE-CD or CAE-CD) has two separate processes: the Program of Study (PoS) validation and then the CAE-CD Designation [3]. The PoS is a defined series of elements that leads to the completion of a degree, certification, or other specified set of outcomes as defined by the institution. As part of the PoS validation, the academic institution must provide a Knowledge Unit (KU) alignment. A KU is a thematic grouping that encompasses multiple related outcomes and learning outcomes [3]. A KU alignment is the process of documenting how the KUs and their outcomes and topics are aligned to the relevant courses in the PoS.

Depending on the nature of the PoS (Associate, Bachelor's, Master's, or Doctoral), the courses must cover a set of specific KUs. For master's degree programs, the PoS must align to three (3) Foundational KUs, five (5) Core KUs, seven (7) Optional KUs, and an additional seven (7) KUs for thesis or its equivalent. Regarding the Core KUs, the academic institution must choose between the Technical Core and the Non-Technical Core when seeking PoS validation.

The Polytechnic University of Puerto Rico (PUPR) in San Juan offers a Master of Science in

Computer Science with a specialization in Cybersecurity [4]. Since 2009, PUPR has been recognized as a Center of Academic Excellence in Information Assurance Education (CAE/IAE) and has successfully received re-designation. Thanks to this designation, this institution has helped many students pursue graduate studies in cybersecurity, thereby preparing them to work with the Federal Government and other federal institutions and agencies [5].

Problem

The Cybersecurity industry is extremely volatile and constantly changing. Threats are growing and evolving, and cybersecurity practices are continually adapting to meet these challenges. Academic institutions should do their best to help cybersecurity students stay current with all this new information and trends. For this reason, and other reasons unbeknownst to us, the PoS validation and NCAE designation are periodically updated. As a result, the KUs' learning outcomes and topics are likely to change. The latest and current designation requirements are valid through the end of December 2025. In January 2026, another requirements document will go into effect.

The last requirements document found was from 2020. The differences in the KUs' learning outcomes and topics are mostly minor but should not be overlooked. For the majority of the KUs in the current document, some learning outcomes have been added, and several topics have been introduced as well. A handful of learning outcomes and topics were removed. Additionally, five KUs are completely new. This change in requirements can be beneficial or harmful for the academic institution. Although highly unlikely, there is a chance that this change could remove certain KUs, outcomes, or topics that some institutions depend on to meet the minimum requirements. On the positive side, academic institutions may add KUs that were not previously mapped, thus enhancing their PoS.

When seeking re-designation, the institution must verify that its PoS is still aligned with the KUs and modify its mapping to include the new learning outcomes and topics if they align with the course. This is important to follow, as it will ensure that the PoS offered by the institution remains qualified to prepare students for the cyber workforce.

Project Goals

The objective of this project is to map the courses of PUPR's Master of Science in Computer Science with a specialization in Cybersecurity to the CAE-CD designation requirements of 2025 to ensure that the PoS still aligns with the current KUs. The changes from the last version to this one were also noted. This will not only ensure that the PoS still meets the current designation requirements, but it will also reveal how each designation requirements document changes and updates for the better. By demonstrating that PUPR's PoS still optimally meets the designation requirements, it will be proven that the institution offers a high-quality education. Furthermore, it will support the fact that students pursuing this degree will be well-suited for the cybersecurity workforce.

As mentioned above, the academic institution must choose between the Technical and the Non-Technical for the Core KUs when seeking validation. Currently, PUPR's PoS is validated for the Non-Technical Core. The reason for this is that the courses naturally and seamlessly align with the five (5) Non-Technical Core KUs. This project attempts to create two NCAE-CD mappings: one where the PoS is aligned with the Technical Core KUs, and another one where the PoS is aligned with the Non-Technical Core KUs. This demonstrates how efficiently PUPR prepares its students with a wide variety of knowledge and tools that will help them in their professional journey and development.

Relevance and Significance

Threats are continually finding new ways to inflict harm on their victims. Cybersecurity professionals must be vigilant for any new information that can help them create a more secure and robust digital environment. They must stay

current to properly protect valuable assets and information from harm. For this reason, academic institutions should do their part in forming students with the best knowledge and preparation. Smith highlighted the importance of higher education in offering cybersecurity courses and degrees [6]. He emphasizes the increase in cyber threats as more organizations digitalize their data. Consequently, this creates a top-priority need for cybersecurity professionals. As he observes the evolution of cyber threats and the cybersecurity industry, he notes how higher education institutions are adapting. According to Smith, the four countermeasures that the institutions are implementing to equip students with cybersecurity skills include preparing programs focused entirely on cybersecurity; forming partnerships with leading industries to offer students internships, co-ops, and job opportunities; incorporating cybersecurity courses into other curricula; and inviting students to collaborate with those from different disciplines.

Capitol Technology University also emphasizes the importance of incorporating cybersecurity into higher education [7]. They support students in pursuing a cybersecurity degree and also support the practice of offering cybersecurity courses to students in non-related fields. A topic that Capitol Technology University mentioned is the importance of continuing education and professional development. As the field of cybersecurity continually evolves, professionals must stay current with the latest cybersecurity trends and tactics. Another point recommended by Capitol Technology University for universities was to seek designations such as NCAE-C. By receiving the NCAE-C, the academic institution demonstrates that its high-quality program is well-equipped to prepare students to become more than competent for the cybersecurity workforce.

Osman explains the role of higher education in preparing students for the cybersecurity workforce [8]. As the cybersecurity industry is expected to continue growing, Osman emphasizes the need for universities to quickly adapt their curricula, whether by incorporating cybersecurity courses across various disciplines, offering dual-track programs, or updating academic content as technologies evolve. He recommends that universities should co-design their curriculum alongside industry partners, cybersecurity firms, and government agencies. This ensures that the curriculum meets industry standards and prepares students for real-world challenges and demands.

The National Initiative for Cybersecurity Education (NICE) Workforce Framework and the Department of Defense Cyber Workforce Framework (DCWF) are two examples of government frameworks. The NICE Workforce Framework is a resource developed by the Department of Homeland Security (DHS) and the National Institute of Standards and Technology (NIST) [9]. This framework provides a common guideline that describes the expectations of work and workers in the cybersecurity field [10]. The DCWF leverages the NICE Workforce Framework. Similar to this framework, DCWF outlines the work performed by various cybersecurity roles [11]. Although the primary aim of these frameworks is to benefit employers, academic institutions can also greatly benefit from them. These frameworks encompass a range of tasks, knowledge, and skills organized by work roles. Universities may use this as a basis for some of their cybersecurity course offerings.

The CAE-CD KUs are tailored to provide students with the necessary knowledge and skills established in both frameworks, the NICE Workforce Framework and the DCWF [12]. This means that by receiving the CAE-CD designation, the academic institutions indirectly use the workforce frameworks as the basis for their courses and PoS. The designation requirements for the CAE-CD are periodically adjusted. As these modifications occur, the academic institutions must be aware of the updates and differences between the last designation requirements and the current ones.

Review of Literature

The CAE Cyber Defense (CAE-CD) designation is awarded to educational entities that are regionally accredited and offer degrees related to cybersecurity. This includes degrees such as majors, minors, and/or certificates at undergraduate and graduate levels. To receive this designation, the academic institutions must apply, and their PoS must meet all requirements. The primary purpose of this program, NCAE-C, is to advocate for high-quality academic programs of higher learning that will support students in their preparation for the cyber workforce.

As part of the application process, the academic institution must demonstrate that its PoS content aligns with the relevant KUs. This alignment will demonstrate whether the program of study has the necessary materials in terms of quantity and form. Master's degree programs have to align three (3) Foundational KUs, five (5) Core KUs, seven (7) Optional KUs, and seven (7) KUs for Thesis and/or Institutional Equivalent.

The KUs criterion is the foundation for the CAE-CD PoS Validation. This is because it establishes the scope and rigor for the curriculum and the targeted work roles as described in the DCWF or the NICE framework. The KUs are carefully developed to help graduates meet the expectations set by the NCAE-C community.

PROCESS

This section outlines the materials needed to achieve the objective of the project.

KU Mapping

The KU mapping serves as the foundation of the entire project. The KU mapping involves comparing each KU learning outcome and topic with the course objectives and topics. To track this, an Excel document is used. The top row of the spreadsheets lists all courses in separate columns that belong to the PoS. In the first column are, in separate rows, the name of the KU, its description, its learning outcomes, its topics, vocabulary related to the KU, related knowledge units, and the related DCWF and/or NICE framework work role(s). Each KU has its own sheet with its own information.

Each group has been assigned a different tab color and an abbreviation. Foundational KUs are assigned the color red and added "-F" at the end (e.g., "Cybersecurity Fundamentals" is to CSF-F); Technical Core are blue and added "-TC" (e.g., "Basic Cryptography" is BCY-TC); Non-Technical Core are green and added "-NTC" (e.g., "Cyber Threats" is CTH-NTC); and Optional are purple and added "-O" (e.g., "Advanced Algorithms" is AAL-O).

KU Alignment

When a course is mapped to a specific number of learning outcomes and topics, it is considered aligned with the corresponding KU. Two separate documents are used to track the KU alignment. The first document lists every KU learning outcome and topic mapped to the course, regardless of whether they are aligned or not. For each course, the document has the course title, the list of mapped KUs, a table containing the course objectives, the KU and its learning outcomes, and a list of the topics mapped to the course. The second document contains only the KUs that are aligned to the course. The format of this second document is identical to that of the first one.

METHODOLOGY

This section explains the strategy conducted to complete the project.

KU Mapping and Alignment

The mapping process is as follows. Starting with the first KU in Excel, which is CSF-F, the syllabus of the first course is reviewed (CECS 6005 – *Principles of Information Security*), and the listed objectives and course outline with the KU learning outcomes and topics are compared. Whenever both coincide, it is marked on the Excel document. Upon finishing the syllabus, the search for learning outcomes and topics is continued by reviewing the course's book(s), using the table of contents,

chapter objectives, chapter summaries, and index. After completing this check-up with the first course, the same process repeats with the next course: first, review the syllabus and then the book(s), all while marking the topics and outcomes that match. Once all 14 courses and 23 books are completed, the entire process is repeated with the next KU until all 73 KUs are mapped.

The result of this process is how the courses map to each and every KU. However, this does not represent the actual KU alignment. The reason for this is that the course must map to most of the KUs' topics so it can then be considered as aligned. It should be mapped with at least 75% of the outcomes and topics. Given this, for each KU, the number of outcomes and topics that would equal 75% of the total is calculated. When 75% equals a decimal, it is rounded down, and the resulting number is used as the base. For example, the total number of topics of CSF-F is 25. Seventy-five percent (75%) of 25 is 18.75. Of course, it is impossible for the number of topics to equal 18.75, so instead, it is counted as 18.

Column Dominance

When selecting which courses to include in the CAE-CD designation, column dominance is applied. As defined in Game Theory, a strategy is a strictly dominant strategy for player *i* if and only if their strategy dominates all the other strategies [13]. For example, let's assume that one course, course *i*, is aligned to a total of 3 KUs. Then, another course, course *f*, is aligned with the same 3 KUs but also includes an additional 2 KUs. In this case, course *f* dominates course *i*. Thus, we have no need for course *i* and it may be "dissolved" or not considered for the final alignment.

Choosing between Technical Core and Non-Technical Core

For the CAE-CD, the education entity must align the PoS courses to five (5) core KUs, which are either Technical or Non-Technical, depending on the nature of the program. The five (5) Technical Core KUs include: Basic Scripting and Programming (BSP); Basic Networking (BNW); Network Defense (NDF); Basic Cryptography (BCY); and Operating Systems Concepts (OSC). The five (5) Non-Technical Core KUs include: Cyber Threats (CTH); Policy, Legal, Ethics and Compliance (PLE); Security Program Management (SPM); Security Risk Analysis (SRA); and Cybersecurity Planning and Management (CPM). The academic institution must choose between these two groups and align the courses of the PoS with the selected group of KUs.

RESULTS

Upon concluding the process explained above, the goal of the project is achieved. The results, explained in this section below, reflect the quality of the institution's PoS.

KU Mapping

For the purpose of this project, the KU mapping refers to the KUs that coincide with at least one topic or outcome in a course, not the KUs that are aligned with the courses. For the KU alignment, in the context of this project, the course must meet most of the KU's learning outcomes and topics.

Out of 73 KUs, only six remained unmapped. This means that all other 67 KUs' learning outcomes and topics align with the courses offered by the PoS at some point.

Although the course CECS 7950 (*Project for MCS*) is aligned with the seven (7) additional KUs that cover Thesis and/or institutional equivalent, as will be shown in the next section, it is also aligned to an Optional KU: Independent/Directed Study/Research (IDR-O). This KU does not have specific learning outcomes or topics. It is intended to address emerging Cybersecurity technologies and issues [12]. This KU aims for emerging Cybersecurity topics. However, it does not list any learning outcomes or topics that must be aligned with a course. The academic institution outlines the topics and objectives, and then the review committee decides if the course receives the credit.

KU Alignment

The KU mapping is used to create the KU Alignment by following the process outlined below. For each KU, the number of learning outcomes and topics that are equal to most of them, as in 75% of outcomes and topics, is calculated. Only those courses that meet, as a minimum, this resulting number are considered to be properly aligned with the KU. Therefore, of the 67 mapped KUs, 47 are properly aligned with the courses of the PoS. This leaves 6 unmapped KUs and 20 partially aligned KUs. For most cases, an exceedingly small number of outcomes and topics were mapped to only one or a few courses. In some cases, no KU outcomes were mapped, but instead, only one or two KU topics were covered by a course. The results of the KU alignment are covered below.

Foundational

The Foundational KUs that must be aligned to the courses are Cybersecurity Fundamentals (CSF), Cybersecurity Principles (CSP), and IT Systems Components (ISC). The four (4) aligned courses to these KUs are CECS 6005, CECS 7230, CECS 7570, and CECS 6015. *Table 1* illustrates the alignment of the KUs with the courses.

Table 1
Foundational KU Alignment

	Foundational		
	CSF	**CSP**	**ISC**
CECS 6005	X	X	X
CECS 7230		X	
CECS 7570	X	X	
CECS 6015			X

Only one course must be chosen to complete the alignment for a single KU. There are multiple ways to mix and match the course selection. Three options are found. The first case would be selecting only CECS 6005 since it aligns with all three KUs. The second option would be to select CECS 7570 and CECS 6015, as the first aligns with two foundational KUs (CSF and CSP), while the latter aligns with the third KU (ISC). The third and final option would be to select CECS 7570, CECS 7230, and CECS 6015. These three cover the three foundational KUs: CSF, CSP, and ISC, respectively. It is worth noting that this last option is unnecessary given that CSP is aligned to CECS 7570 and CECS 7230. Since none of the other courses align with CSF, CECS 7570 cannot be removed. However, CECS 7230 can be removed as its only alignment is already covered by another course that is "bigger" in terms of alignment. This leaves only two options for the final alignment: one option with only CECS 6005 and another option with CECS 7570 and CECS 6015. Applying the column dominance, the best option would be the first one: CECS 6005 for CSF, CSP, and ISC.

Technical Core

As mentioned above, the five (5) Technical Core KUs are: Basic Scripting and Programming (BSP); Basic Networking (BNW); Network Defense (NDF); Basic Cryptography (BCY); and Operating Systems Concepts (OSC). There are five (5) courses that align to these KUs: CECS 6005, CECS 6605, CECS 7230, CECS 7570, and CECS 6015. Refer to *Table 2* to see the mapping of the five (5) technical core KUs and the five (5) courses.

Table 2
Technical Core KU Alignment

	Technical Core				
	BCY	**BNW**	**BSP**	**NDF**	**OSC**
CECS 6005		X			
CECS 6605			X		
CECS 7230	X			X	
CECS 7570	X	X			X
CECS 6015		X			

There are three possible options. The first option includes the courses CECS 7230, CECS 6005, CECS 6605, CECS 7230, and CECS 7570. The second option includes CECS 7230, CECS 6015, CECS 6605, CECS 7230, and CECS 7570. Lastly, the third option would include CECS 7230, CECS 6605, and CECS 7570. Given that these last three courses are the only ones that align with certain KUs, they cannot be removed. Since these courses align with all Technical Core KUs, it is unnecessary to add another course. Thus, the third option is the best option.

Non-Technical Core

The five (5) Non-Technical core KUs are: Cyber Threats (CTH); Policy, Legal, Ethics and Compliance (PLE); Security Program Management (SPM); Security Risk Analysis (SRA); and Cybersecurity Planning and Management (CPM). The PoS has four courses that align to these KUs: CECS 6005, CECS 6230, CECS 7570, and CECS 6015. The alignment of these five (5) KUs and four (4) courses is depicted in *Table 3*.

Table 3
Non-Technical Core KU Alignment

	Non-Technical Core				
	CTH	**CPM**	**PLE**	**SPM**	**SRA**
CECS 6005	X	X			X
CECS 6230		X			
CECS 7570	X	X	X		X
CECS 6015		X		X	X

There are four ways to align the courses with the Non-Technical KUs. The first way is aligning the courses CECS 6005, CECS 6230, CECS 7570, and CECS 6015. The second solution is using the courses CECS 6005, CECS 7570, and CECS 6015. The third option includes the courses CECS 7570, CECS 6230, and CECS 6015. For the fourth and last possible way, only the courses CECS 7570 and CECS 6015 are used. The situation for this case is similar to the situation in the previous section. The courses CECS 7570 and CECS 6015 align with two KUs (PLE and SPM, respectively) where no other course aligns as well. This makes either of the courses impossible to remove. As shown in *Table 3*, these two courses also cover the rest of the Non-Technical core KUs, making them perfect to complete this mapping while applying column dominance.

Optional

Table 4 shows the courses that were aligned to ten (10) Optional KUs. Specifically, in this table are the courses that were not used for Foundational, Technical, and Non-Technical KUs. The reason for this is to have a final alignment with a wide variety of courses, instead of choosing fewer courses that align with many KUs.

The ten (10) Optional KUs are ALG, CSE, DST, DVF, DFS, HOF, ITC, MEF, NWF, and PRI. To these KUs, six (6) courses are aligned: CECS 6010, CECS 6030, CECS 7235, CECS 7237, CECS 6045, and CECS 6046.

Table 4
Optional KU Alignment

	Optional									
	ALG	**CSE**	**DST**	**DVF**	**DFS**	**HOF**	**ITC**	**MEF**	**NWF**	**PRI**
CECS 6010	X		X							
CECS 6030							X			
CECS 7235				X	X	X		X	X	
CECS 7237				X	X	X		X	X	
CECS 6045		X								X
CECS 6046								X		

Choosing the courses and KUs for the final optional alignment can be a bit tricky, but it is possible. From the ten (10) Optional KUs, only seven (7) are needed. Out of these 10 KUs, five (5) are related to Forensics. Ideally, it is best to use a variety of KUs, rather than choosing only the forensics ones and aligning them with the forensics courses. The remaining 5 KUs, which are not related to Forensics (ALG, DST, ITC, CSE, PRI), are chosen. Only two more KUs are needed to complete the 7 Optional KUs required for designation. Since the project aims for variety, DFS and MEF from the forensic KUs are chosen. Both KUs are aligned with the courses CECS 7235 and CECS 7237, and, additionally, MEF is also aligned with CECS 6046. The result of this selection is shown in *Table 5*.

Table 5
Optional KU Alignment after selecting the 7 KUs

	Optional						
	ALG	**CSE**	**DST**	**DFS**	**ITC**	**MEF**	**PRI**
CECS 6010	X		X				
CECS 6030					X		

CECS 7235				X		X	
CECS 7237				X		X	
CECS 6045		X					X
CECS 6046						X	

Thesis and/or Institutional Equivalent

For the CAE-CD designation, Master's degree programs may include a Thesis or equivalent, such as a graduate project course, a graduate experiential learning course, or a graduate practicum. PUPR's PoS offers a Graduate project course, CECS 7950. This course aligns with the seven (7) additional KUs that are dedicated to a Graduate thesis, dissertation, or equivalent. This mapping is illustrated in *Table 6*.

Table 6
Thesis and/or Institutional Equivalent Alignment

	Additional or Graduate Thesis/Dissertation/Equivalent						
	7 KUs for Graduate Project Course						
CECS 7950	X	X	X	X	X	X	X

Observations

During the process of selecting courses and KUs for the final alignment, several observations were noted. Curiously, two courses are aligned with a single KU, each one. The courses CECS 6230 (*IT Operations*) and CECS 6046 (*Electronic Discovery & Digital Evidence*) are aligned with Cybersecurity Planning and Management (CPM-NTC) and Media Forensics (MEF-O), respectively. In terms of the KU alignment, the courses CECS 6230 and CECS 6046 could be dissolved since the KUs aligned for these courses are also aligned to other courses that are aligned to even more KUs. Thus, applying column dominance, the other courses have the upper hand. The course CECS 7230 (*Network Security*) could be dissolved; however, it's the only course that is aligned with Network Defense (NDF-TC). Lastly, the courses CECS 7235 (*Computer Forensics*) and CECS 7237 (*Advanced Computer Forensics*) can be merged together as they both cover the same exact KUs.

The differences between the 2020 KUs and the 2025 KUs are primarily rephrased versions of existing learning outcomes and topics. There is also a significant number of learning outcomes and topics that have been added, as well as a smaller number that have been removed. No KU was removed; however, there are five (5) new KUs: Business Continuity and Disaster Recovery (BCD-O), Cyber-Physical Systems (CPS-O), Independent/Directed Study/Research (IDR-O), Pre-OS Boot Environment (PBE-O), and Threat Intelligence (THI-O).

Final Alignment

The courses best suited for the CAE-CD designation are organized into two tables. *Table 7* shows the Master Technical CAE-CD mapping, and *Table 8* shows the Master Non-Technical CAE-CD mapping. These two final alignments were completed by applying column dominance and focusing on a wide variety.

Table 7
Master Technical CAE-CD Mapping

	Master Technical CAE-CD								
	CECS 6005	**CECS 6010**	**CECS 6030**	**CECS 7235**	**CECS 6605**	**CECS 7230**	**CECS 7570**	**CECS 6045**	**CECS 7950**
CSF	X						X		
CSP	X						X		
ISC	X								
BCY						X	X		
BNW	X						X		
BSP					X				
NDF						X			
OSC							X		
ALG		X							
CSE	X							X	
DST		X							
DFS				X					
ITC			X						
MEF				X					
PRI								X	
7 KUs for Project Course									X
									X
									X
									X

									X
									X
									X

Table 8
Master Non-Technical CAE-CD Mapping

	Master Technical CAE-CD							
	CECS 6005	CECS 6010	CECS 6030	CECS 7235	CECS 7570	CECS 6015	CECS 6045	CECS 7950
CSF	X				X			
CSP	X				X			
ISC	X					X		
CTH	X				X			
CPM	X				X	X		
PLE					X			
SPM						X		
SRA	X				X	X		
ALG		X						
CSE	X						X	
DST		X						
DFS				X				
ITC			X					
MEF				X				
PRI							X	
7 KUs for Project Course								X
								X
								X
								X
								X
								X
								X

DISCUSSION

With a total of 14 courses, PUPR's PoS offers a wide variety of topics. Thus, it achieves an extensive and varied alignment of KUs. Despite the selection of courses for the final alignment in this project, it is still possible to continue mixing and matching with different courses, including those not chosen for the Optional KUs (Foundational, Technical, and Non-Technical). This results in numerous possibilities for the final alignment, each with different reasons behind it. It is worth noting that this heavily depends on the person creating this final alignment and their opinion on what would be best for the alignment.

For the purpose of this project, it is preferred not to consider the courses used in Foundational, Technical, and Non-Technical and give a higher priority to the other courses. This results in a wider variety of courses, KU alignment, and a broader range of topics covered. Of course, "more" does not always mean "more," and having too many different things can result in poor outcomes. However, it is essential for students to explore and learn various topics. This will help them develop personally and professionally. By acquiring a diverse range of knowledge, they will develop unique skills, regardless of where they choose to work. Not only this, but a variety of courses will also enable students to explore different potential work areas within the cybersecurity industry. Therefore, they will have an easier time discovering which area(s) of cybersecurity they prefer and which one(s) they do not, and thus, enhancing their professional development.

FUTURE WORK

As mentioned before, the designation requirements are periodically changing. It would be interesting to see how these requirements change in January 2026 and how they would affect PUPR's PoS. Future projects would involve finding out if there are new KUs to which any course may be aligned. With the new designation requirements, an even more optimal final alignment could be achieved. Nonetheless, it's essential to stay current with these requirements to ensure the academic institution is offering high-quality education.

A short investigation related to "Skills Needs Gap Analysis in Puerto Rico in the areas of AI, Data Science, Cybersecurity, and AI/Machine Learning" was conducted during this project. A possible future project could include a skills gap analysis of the alumni of PUPR's PoS. To complete this, a questionnaire would be prepared and sent to the alumni, asking about their skills and other relevant information. These results would be compared with the course objectives of the PoS and the DoD's Cyber Workforce Framework (DCWF) and NIST's National Initiative for Cybersecurity Education (NICE) framework. The result of this

will give an even deeper insight into the quality of PUPR's PoS.

CONCLUSION

The goal of this project was to align the courses of PUPR's Master of Science in Computer Science with a specialization in Cybersecurity with the KUs that form part of the CAE-CD designation requirements. To accomplish this, all 14 courses were mapped with all 73 KUs. This was done by comparing the course's objectives and the topics covered in the books with the KUs' learning outcomes and topics. Once the mapping was completed, the next step was to properly align the courses with the KUs. The final stage was to select which courses would fulfill the designation requirements for the CAE-CD. The results of this project demonstrate the preparation of PUPR's PoS. The Non-Technical CAE-CD supports and demonstrates the institution's current designation. Meanwhile, the Technical CAE-CD confirms that PUPR is also qualified to receive this designation.

This project emphasizes the importance of the CAE-CD designation. As cyber threats and issues continue to grow, incoming cybersecurity professionals must possess the necessary skills and knowledge to adapt to this growth. With this designation, the academic institutions are proving their PoS is of high quality. The CAE-CD designation serves as evidence that the institution is well-equipped and capable of preparing students competent for the cyber workforce. Students graduating from these institutions are talented, skilled, and proficient.

REFERENCES

[1] Defense Information Systems Agency (DISA). (n. d.). *National Centers of Academic Excellence in Cybersecurity (NCAE-C)* [Online]. Available: https://www.cyber.mil/ncae-c/.

[2] National Security Agency (NSA). (n. d.). *National Centers of Academic Excellence in Cybersecurity* [Online]. Available: https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/.

[3] Application Process and Adjudication Rubric (APAR) and Cyber Defense Working Group (CDWG). (2024, July). *National Centers of Academic Excellence in Cybersecurity NCAE-C 2024 Designation Requirements and Application Process for CAE-Cyber Defense (CAE-CD* [Online]. Available: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_designation_requirements.pdf.

[4] Polytechnic University of Puerto Rico (PUPR). (n. d.). *Master of Science in Computer Science with a specialization in Cybersecurity* [Online]. Available: https://pupr.edu/master-computer-science/.

[5] Polytechnic University of Puerto Rico (PUPR). (2024). *Information Assurance and Security* [Online]. Available: https://pupr.edu/information-assurance-and-security/.

[6] M. Smith. (2023, June 26). *Cyber security: How higher ed aims to meet the rising demand* [Online]. Available: https://www.apporto.com/cyber-security-how-higher-ed-aim-to-meet-the-rising-demand.

[7] Capitol Technology University. (2024, June 6). *The Importance of Higher Education in Cybersecurity Studies* [Online]. Available: https://www.captechu.edu/blog/importance-of-higher-education-cybersecurity-studies.

[8] T. M. Roydean Osman. (2025, July 15). *The Role of Higher Education in Building a Cyber-Resilient Workforce* [Online]. Available: https://cybersecurityasia.net/building-cyber-resilient-workforce/.

[9] NIST. (2025, March 10). *NICE Framework History* [Online]. Available: https://www.nist.gov/itl/applied-cybersecurity/nice/nice-framework-resource-center/about/nice-framework-history.

[10] NICCS. (2025, August 28). *NICE Workforce Framework for Cybersecurity (NICE Framework)* [Online]. Available: https://niccs.cisa.gov/tools/nice-framework.

[11] Chief Information Officer. (n. d.). *Framework* [Online]. Available: https://dodcio.defense.gov/Cyber-Workforce/DCWF/.

[12] A. Becker et al. (2024). *National Centers of Academic Excellence in Cybersecurity (NCAE-C) - Cyber Defense (CAE-CD) Knowledge Units* [Online]. Available: https://dl.dod.cyber.mil/wp-content/uploads/cae/pdf/unclass-cae-cd_ku.pdf.

[13] MIT OpenCourseWare. (2012). *Economic Applications of Game Theory | Chapter 4: Dominance* [Online]. Available: https://ocw.mit.edu/courses/14-12-economic-applications-of-game-theory-fall-2012/0136e76dcd45a6f1d7b386c563452ff0_MIT14_12F12_chapter4.pdf.