CALIFORNIA STATE POLYTECHNIC UNIVERSITY, POMONA

ACADEMIC SENATE

ACADEMIC PROGRAMS COMMITTEE

REPORT TO

THE ACADEMIC SENATE

AP-012-223

New Minor in Cyber Security

Academic Programs Committee **Date: 10/11/2023**

Executive Committee
Received and Forwarded **Date: 10/11/2023**

Academic Senate **Date: 10/18/2023**
First Reading
11/08/2023
Second Reading

BACKGROUND:

The minor in Cyber Security from the Department of Computer Science is intended to help undergraduate students develop cyber security skills and knowledge. The minor consists of a series of courses that are designed to provide students with both the theoretical background and the practical skills necessary to compete for jobs in the cyber security field. The minor program will 1) offer a core foundation in cyber security that allows students to contribute to their communities at large in a responsible and ethical manner; and 2) engage students to work effectively as individuals or as team members in the professional practice of cyber security and show an understanding of contemporary cyber security issues.

RESOURCES CONSULTED:
Department Chairs, all colleges
Associate Deans, all colleges
Dr. Drew Hwang, Chair of the Computer Information Systems Department
Dr. Halima El-Naga, Chair of the Electrical and Computer Engineering Department
Ashley Ly, Senior Curriculum Specialist and Lead, Academic Programs Office

DISCUSSION and RECOMMENDATION:

The Computer Science department proposed this new minor in Cyber Security. The minor is 36 units with 29 units of core courses, 6 units of elective courses, and 1 required unit of a Capstone project in Cyber Security. The proposed minor program offers a core foundation in cyber security and trains students in competencies to use the different cyber security methods, techniques, and tools to solve cyber security problems. Specifically:

(1) Core courses allow students to gain the fundamental knowledge set and skills that are essential for any cyber security professional. These include: an understanding of networking, script programming, cryptography, threats, and countermeasures.

(2) The elective courses will enable students to gain advanced and specialized skills in cyber security, including: data privacy, machine learning to solve cyber security problems, wireless and mobile security, and reverse engineering and software security.

(3) The capstone course will guide the students to conduct a project and apply the cyber security knowledge and skills to solve practical problems.

Three new courses have been developed for the minor: Software Security and Reverse Engineering (CS 4670), Data Privacy and Security (CS 5510), and Machine Learning for Cyber Security (CS 5520). All new courses have been approved in Curriculog. The minor is designed for undergraduates; however, two of the new courses are graduate-level courses for those students who are prepared for more challenging coursework. After consultation with the Academic Programs Office, the committee is satisfied that the minor will be accessible to undergraduate students. Undergraduate students can

enroll in graduate-level courses (with a permission number); however, the students will not be able to count the graduate-level courses towards their undergraduate *and* graduate degrees. The graduate-level courses are offered within the electives for the minor so students could choose not to enroll in the graduate-level courses and still be able to earn the minor.

All department chairs and associate deans were consulted. Concerns were raised by two departments: Electrical and Computer Engineering (ECE), and Computer and Information Systems (CIS), both of which have expertise and interests pertaining to cyber security.

Some of ECE's concerns focused on the specific content of the minor and some of the courses within it, and whether those courses adequately meet the needs of cyber security professionals. CS faculty elaborated on the nature and purpose of the courses, to the satisfaction of the AP Committee. After further reflection the ECE department dropped this objection.

An additional concern from ECE regarded the possibility that the minor will compete with their Computer Engineering major. However, this is a minor program, not a major, so the AP Committee is confident that very few Computer Engineering students will reconsider their major on the basis of a minor, particularly since ECE is already an impacted department. Upon further reflection, the ECE department likewise dropped this objection.

CIS expressed concerns about (1) a single department using a name that applies to expertise found in many departments and (2) the minor having a substantial number of core computer science classes, with only a handful of cyber security-specific courses.

The AP Committee considered these concerns and nonetheless supports the minor, for two reasons: First, it is right and proper that a minor might also include disciplinary foundations that may be applicable to several related fields. Indeed, if a computer science department offered cyber security training without foundations, the minor would be deficient and not suitable for approval. While this minor certainly does not provide the depth of cyber security training that a major would provide, this is a minor rather than a major. And this minor still has 4 required classes with significant cyber security content and 2 more electives in cyber security.

Second, the AP Committee believes that when multiple departments have expertise in an interdisciplinary topic, it is appropriate for any or all of those departments to name that topic in their programmatic offerings. Several years ago, when considering AP-011-189, a Master's program in Information Security that elicited a similar controversy between the same departments, the AP Committee wrote in its report:

> *…the AP Committee strongly believes that if a topic is studied by people in multiple departments then multiple departments should be able to offer programs focused on that topic and label their programs accordingly. This opinion was*

> *reinforced by input from multiple AP Committee members with expertise in interdisciplinary fields.*

That report was subsequently adopted by the Academic Senate, and the reasoning remains compelling and applicable in this dispute.

There was some discussion of whether a future minor program, whether from ECE or CIS, might have a similar name and elicit confusion among students. The AP Committee, however, believes that this issue is addressable for two reasons. First, the name “Information Security” elicited similar concerns about being overly broad, yet the CS department has found an alternative broad name for the same field. We are confident that if ECE wishes to offer a similar program they can likewise find a broad name that is not yet taken, and that CIS can aptly call any future minor program “Information Security” (as they do for their graduate program). Second, while students might be confused by certain labels, that confusion is most perilous when they are applying to college and not yet on campus trying to select a major without access to people who can explain it. Minors are only declared once students are on campus and have access to people who can help explain the content of the program.

Finally, we note that the CS department indicates future plans that will hopefully give multiple departments a stake in the success of this minor, thus mitigating concerns about departments claiming something that others have expertise in. Specifically, the CS department hopes to expand the interdisciplinary nature of the minor once it is established and bring in coursework from other departments. If this plan is successful, the minor has the potential to provide enrollment growth opportunities for multiple departments, rather than detract from enrollments.

The Academic Programs Committee recommends approval of the Cyber Security Minor.