CALIFORNIA STATE UNIVERSITY
SAN MARCOS

Procedure for Submitting Proposals for New Certificates

1. Full and exact title of the Certificate program and level of the program (Certificate of Specialized vs. Advanced Study). Name and position of the person(s) submitting the proposed Certificate. Intended implementation date of the program.

Title: Cybersecurity – Technologies
Level: Advanced Study
Name:
Position:
Implementation date: Fall, 2019

2. List of the existing programs in the discipline(s) under which the new Certificate is to be offered.

This program will be offered by CSIS through Extended Learning, in partnership with the Cybersecurity Professional Science Masters.

3. List of the existing program(s) that may be affected by the proposed Certificate.

It may affect the Cybersecurity Professional Science Masters, but this certificate is proposed and managed by the same committee.

4. Purpose of the proposed Certificate, including specific academic objectives served, professional applications, potential student market, and a statement explaining the need for the Certificate in comparison to existing related majors, minors, and Graduate programs.

Purpose: There is a broad need for these skills. Demand for the information and skills provided by this certificate remains very high, yet many potential students are not prepared to embark on a full Master's program. Additionally, some career paths do not require a master's degree. Many organizations will support funding employee certification over a Master's program. Further, many potential students are technology-focused and do not intend for their careers to require understanding of risk, policy or the more organizational elements of cybersecurity.

Academic Objectives: This certificate is intended to provide students with knowledge, skills and experience sufficient for them to understand the security of systems of computers and networks, and implement or operate these securely. Please note that a complementary certificate, "Cybersecurity – Management, Risk & Governance", explores the

development and implementation of cybersecurity policy, governance and risk programs.

These two certificates cover most of the courses in the MS degree, however students need to take three more courses plus Semester-In-Residence project to complete their master degree. The selected courses in the certificate program are the pre-requisites of the remaining courses of the master program.

Professional Applications: This certificate will be used for security analyst positions in organizations which manage or develop technology projects.

Compared to existing programs: At present, the CSIS program teaches only one course with a focus on security. The Cybersecurity Master's program includes these courses as listed in Section 5.

5. List of the courses, by catalog number, title, and units of credit, as well as total units to be required under the proposed Certificate.

Math 503 Cryptography (3)
MCS 510 Security in Computer Networks (3)
MCS 511 Secure Features in Operating Systems (3)
MCS 512 Development of Secure Software (4)

6. Definition of the minimum level of competence to be demonstrated to earn the proposed Certificate, and a description of the means of assessing that competence (examination, practicum, field experience, etc.).

These courses require a combination of written and oral communication skills demonstrated by a series of papers and presentations. These, along with quizzes and other assessments are used to assign grades. Students must maintain a 3.0 GPA and earn at least a "C" (2.0) in each course.

7. Description of assessment strategies for waiver of lower division requirements (where applicable).

N/A

8. New courses to be developed. Include proposed catalog descriptions in the Certificate proposal. "C-forms" for these courses should accompany the proposed Certificate package for curricular review

N/A

9. List of all present faculty members, with rank, appointment status, highest degree earned, date and field of highest degree, and professional experience, who would teach in the proposed aggregate of courses.

Dr. Ali Ahmadinia, Associate Professor, Ph.D., 2006, Computer Science, Developed and taught courses in computer system security

Dr. Shahed Sharif, Associate Professor, Ph.D., 2006, Mathematics, Developed and taught courses in Cryptography
Dr. Tom Springer, Lecturer, Ph.D., 2014, Computer Science, Senior Software Engineering, Boeing
Dan Ostermiller, Lecturer, MSc, 1988, Senior Software Engineer, MITRE Corp, G2 Software
Teresa Macklin, Lecturer, JD, 2007, Law, Campus Chief Information Security Officer, Assoc. Dean, IITS

10. Instructional resources (faculty, space, equipment, library volumes, etc.) needed to implement and sustain the Certificate program.

This certificate program will use open seats in the existing Cybersecurity Professional Science Master's program. At present we do not anticipate creating new sections of these courses to meet demand for the certificate, however as this program is self-support, it does not require any funded resources.

Appendix A – Catalog Description

Program Overview

This certificate is intended to provide students with knowledge, skills and experience sufficient for them to understand the security of systems of computers and networks, and implement or operate these securely.

Please note that a complementary certificate, "Cybersecurity – Management, Risk & Governance", explores the development and implementation of cybersecurity policy, governance and risk programs. These two certificates cover most of the courses in the MS degree, however students need to take three more courses plus Semester-In-Residence project to complete their master degree. The selected courses in the certificate program are the pre-requisites of the remaining courses of the master program.

The PSM Cybersecurity students will automatically receive this certificate after successful completion of the courses required for this certificate.

Program Students Learning Outcomes

Upon completion of the program, students will be able to:

1. Explain network security protocols;
2. Recognize secure operating systems;
3. Explain how secure software is developed.
4. Recognize encryption algorithms.

Admission Requirements and Application

- Admission decisions will be made by the Admission Committee chosen by the Program Director in consultation with its faculty
- Admission decisions will be based on 1) undergraduate courses and GPA, 2) GRE scores, or resume, 3) TOEFL for some students **, and 4) the statement of purpose and recommendation letters.
- Admission to the program requires an undergraduate degree in computer science or closely related discipline, and should include upper-division courses in operating systems, networks and software engineering. Applicants with a baccalaureate degree in a related field may be able to meet prerequisites with equivalent work experiences in computer science and will be considered for conditional admission.
- Admission requires a minimum of 3.0 grade point average in the upper-division computer science courses and at least a 2.5 undergraduate GPA in the last 60 semester units (or last 90 quarter units) attempted.
- All applicants must submit general GRE scores, or resume when applying. Minimum GRE scores required are:
  - Verbal 143
  - Quantitative 155
  - Analytical Writing 3.5 (this will also satisfy the Graduate Writing Assessment Requirement)
- As an alternative to the GRE, applicants may submit a resume or CV showing work experience in Cybersecurity of technology field.

Applicants must submit:

1. The program application form.
2. The statement of purpose outlining the reason or pursuing the degree.
3. GRE scores, or resume.
4. TOEFL score if required.
5. One set of transcripts from all colleges/universities attended.
6. Two recommendation letters on a provided form.

- Applicants to the program will be subject to standard background checks in accordance with Defense Security Service reporting requirements.

Student candidates may apply at any time throughout the year. However, selection and admission will be completed by early May for the Fall semester start. Later applications will be considered, as spaces remain available. Feedback to applicants, but not final admission decisions, will be provided on a timely basis regardless of the time of application.

***All applicants must have a TOEFL score of 80 iBT or above (213 on the computer-based examination, 550 paper-based), or an IELTS score of 6.0, unless they possess a bachelor's degree from a post-secondary institution where English was the principal language of instruction.*

Certificate Requirements and Courses

The Cybersecurity – Technologies certificates requires students to complete the following set of courses. Students must maintain a 3.0 GPA and earn at least a "C" (2.0) in each course.

Required Courses Total: 13 units

Math 503 Cryptography (3)
MCS 510 Security in Computer Networks (3)
MCS 511 Secure Features in Operating Systems (3)
MCS 512 Development of Secure Software (4)

Continuation

Students must maintain an overall GPA of 3.0 and earn at least a C (2.0) in each course, except those taken for credit/no credit. Any student whose overall GPA falls below 3.0 for two consecutive semesters will be dropped from the program. A full-time student should be enrolled in the predetermined course schedule and credit hours each semester for the program