CALIFORNIA STATE UNIVERSITY SAN MARCOS
NEW PROGRAM PROPOSAL – P Form Signature

For Academic Programs Office Use Only		
R.E.	Catalog	File

COLLEGE ☐ CHABSS ☐ CoBA ☐ CoEHHS ☒ CSM

TITLE OF PROGRAM Cybersecurity – Technologies Discipline CSIS

This form is the signature sheet for new programs and new options/concentrations/emphases/tracks within existing programs. For all changes to existing programs (other than addition of new options/concentrations/emphases/tracks), use the Form P-2.

Check one:
- ☐ New Undergraduate Major or New Graduate Degree — Attach a completed New Program Template
- ☐ New Option/Concentration/Emphasis/Track
- ☐ New Minor
- ☐ New Teaching Credential
  (☐ New Option/Concentration/Special Emphasis, ☐ Teaching Credential and ☐ Minor) — Attach a completed New Option/Concentration/Special Emphasis, Teaching Credential and Minor
- ☒ New Certificate — Attach a completed New Certificate Template

Does this proposal impact other disciplines? ☐ Yes ☒ No If yes, obtain signature(s).
Any objections or concerns should be stated in writing and attached to this form. Please check the box to indicate whether a memo has been attached.

Term and Academic Year of intended implementation (e.g. Fall 2016): Fall 2017

CS — ✓ Support ___ Oppose
Discipline #1
Signature ☐ Date 12/5/17

Chemistry — ✓ Support ___ Oppose
Discipline #2
Signature ☐ Date 12/5/17

Industrial — X Support ___ Oppose
Discipline #3
Signature ☐ Date 12/5/17

Physics — ✓ Support ___ Oppose
Discipline #4
Signature ☐ Date 12/12/17

MATH — ✓ Support ___ Oppose
Discipline #5
Signature ☐ Date 3/13/18

RECEIVED
MAR 13 2018
BY:

RP
Trucker
PS

P-FORM PREPARATION

1a. Ali Ahmadinia — Originator (Please print) — 04.06.2017 — Date

1b. _____ — Librarian Liaison for Library Report+ — Date

1c. _____ — IITS Liaison for IITS Report+ — Date

PROGRAM/DEPARTMENT-LEVEL REVIEW

2. _____ — Program/Department - Director/Chair* — 4/10/17 — Date

COLLEGE/SCHOOL-LEVEL REVIEW

3. _____ — College/School Curriculum Committee* — 11/27/17 — Date

REVIEW (Signatures must be obtained by proposer)

4a. _____ — Vice President for Student Affairs* — 12/4/17 — Date

4b. _____ — Dean of Library* — 12/13/17 — Date

4c. _____ — Dean of Information and Instructional Technology Services* — 12/21/17 — Date

4d. _____ — Vice President for Finance and Administrative Services* — 11/29/2017 — Date

4e. _____ — Dean of Graduate Studies (if applicable) * — 12/11/17 — Date

COLLEGE/SCHOOL-LEVEL RECOMMENDATION

5. _____ — College/School Dean/Director* — 11/27/2017 — Date

UNIVERSITY-LEVEL REVIEW

(May not begin until all signatures numbered 1-5 have been obtained.)

6a _____ — University Curriculum Committee^ — Date

6b. _____ — Budget and Long-Range Planning Committee^ — Date

FACULTY APPROVAL

7 _____ — Academic Senate — Date

UNIVERSITY-LEVEL APPROVAL

8 _____ — Provost — Date

9 _____ — Date to Chancellor's Office

+ Please contact the liaisons at the beginning of the process and allow sufficient time for the liaisons to prepare the resource implication report. Upon completion of the report liaisons will sign.

* May attach a memo on program impact on the unit and the ability of the unit to support it.

^ Attach a memo summarizing the curricular and/or resource deliberations.

o summarizing the curricular and/or resource deliberations.

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, 2018

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, Assistant Professor, Ph.D., 2006, Computer Science, Developed and taught courses in computer system security

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.

California State University
SAN MARCOS

Kellogg Library California State University San Marcos 333 S. Twin Oaks Valley Road San Marcos, CA 92096-0001
Tel: 760.750.4330 **Fax:** 760.750.3318 jfabbi@csusm.edu

Date: December 5, 2017

To: Laurie Schmelzer

From: Dr. Jennifer Fabbi
Dean, University Library

Subject: Library Review of the Proposal for Certificate in Cybersecurity - Technologies

Thank you for the opportunity to respond to the proposal for a certificate of advanced study in Cybersecurity – Technologies. Talitha Matlin, currently the STEM Librarian, has reviewed the program proposal. The capacity and probable needs of the CSUSM Library to support this program is identical to the Library's response for the Professional Science Masters Degree in Cybersecurity in 2014. At this time, the most critical resource (a subscription to the Association for Computing Machinery Digital Library) has been acquired.

cc: Katherine Kantardjieff
Lauren Magnuson
Talitha Matlin

California State University
SAN MARCOS

Instructional & Information Technology Services ~ Office of the Dean & Chief Information Officer

DATE: December 21, 2017

TO: Laurie Schmelzer
College of Science & Mathematics

FROM: Kevin Morningstar, Dean & Chief Information Officer

SUBJECT: IITS Comments Related to Program Proposal for
Cybersecurity Professional Science Masters (Extended Learning)

IITS has reviewed the program proposal related to the expansion of the existing Cybersecurity Professional Science Masters. The following factors were considered relative to the established technology resources and support services provided by Instructional and Information Technology Services.

1. The proposal did not indicate any new courses will be developed requiring Instructional Development.
2. Proposal did not indicate any additional demand for classroom/labs use as the proposal noted "[t]his certificate program will use open seats in the existing Cybersecurity Professional Science Master's program".
3. No specific Information Technology needs or services were noted throughout the proposal as it is assumed that existing resources for the current program are sufficient.

FINDING

IITS fully supports the expansion of the Cybersecurity Professional Science Masters with this new certificate option. No additional long term technical support, hardware resources, or operational impacts to IITS were identified including Instructional Design Services.

Given the information available, IITS projects that there are adequate existing staff and technology resources available to support the program as documented.