## Appendix A – Catalog Description

The Master of Science in Cybersecurity is a professional science degree program designed to meet the needs of the computing industry and associated organizations. The program is a blend of technical courses and business courses with a capstone project. The objective of the program is to train an expertly skilled workforce to fulfill the imminent needs of the emerging and evolving cybersecurity industry. The program is designed to prepare those with strong background in computer science for management positions in cybersecurity such as the manager of the information security department, the director of risk assessment and compliance, the chief information security officer, the director of it security, and project managers of security related projects

Throughout the program, students will be exposed to real-world problems/cases, leading-edge technologies, managerial/interpersonal skills, ethics and governance knowledge, and problem solving skills.

The rigorous program is taught in the evenings and on weekends to accommodate the working student. The program design is a cohort model that requires students to go through the program together over a five-semester period with a predetermined course sequence. It is a non-thesis degree program requiring a rigorous "Internship or Semester-In-Residence" project as culminating experience.

Each student will be guided and evaluated by an Advisory Committee that will be made up of university faculty, program instructors, and industry mentors, as well as program advisors. *This program is offered through the Office of Extended Learning.*

### Admission Requirements and Application

Admission requirement and application include the general admission to graduate studies at CSUSM. Program specific admission considerations are as follows:

- 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, 3) TOEFL for international students, and 4) the statement of purpose and recommendation letters. Those not meeting the minimum GPA, GRE or TOEFL should not apply
- Admission to the program requires an undergraduate degree in Computer Science including upper-division courses in operating systems, networks and software engineering. Applicants with a baccalaureate degree in a related field with a minor or equivalent work/certification experiences may 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 when applying. Minimum GRE required:
    - Verbal 143
    - Quantitative 155
- Analytical Writing 3.5 (this will also satisfy the Graduate Writing Assessment Requirement.)
- 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 bachelors degree from a post-secondary institution where English was the principal language of instruction.

Applicants must submit:

- The program application form.
- The statement of purpose outlining the reason or pursuing the degree.
- GRE scores.
- TOEFL score if required.
- One set of transcripts from all colleges/universities attended.
- Two recommendation letters on a provided form.

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.

**Degree Requirements and Courses**

The Master of Cybersecurity requires thirty-eight (38) semester hours of coursework. Students must complete a set of courses and the culminating experience project with a 3.0 GPA and earn at least a "C" (2.0) in each course.

**Six Required Technical Side Courses Total: 21 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)** |
| **MCS 610 Offensive Security & Penetration Testing** | **(4)** |
| **MCS 611 Intrusion Detection and Investigation** | **(4)** |

**Five Required Business Side Courses Total: 12 units**

| | |
|---|---|
| **MGMT 521 Principles of Organizational Behavior and Leadership for Security Management** | **(2)** |
| **MIS 522 Information Systems and Security Management** | **(2)** |
| **MIS 621 Secure System Governance, Regulation, and Compliance** | **(3)** |
| **MIS 622 Technology Assessment and Security Risk Management** | **(3)** |
| **MCS 660 Communication in a Technical Industry** | **(2)** |

**Culminating Experience Total 5 units**

| | |
|---|---|
| **MCS 680A Semester in Residence Project Writing Workshop** | **(1)** |
| **MCS 680B Internship/Semester in Residence/Project** | **(4)** |

A student who has obtained a waiver for a required course may enroll in **MCS 697 Directed Studies** upon consent of the instructor.

**Continuation**

Graduate 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

**Advancement to Candidacy**

The student will advance to Master's Degree candidacy upon the completion of MCS680A and approval of a Project Abstract by the student's Advisory Committee. The Advisory Committee is made up of a program faculty member, an industry mentor, and the Program Director.

**Culminating Experience**

In lieu of a thesis, the candidate must successfully complete a culminating 16-week "Semester Internship/Residency Project" in MCS 690B, resulting in a final written report with an oral defense. Student projects address and affect a real-world problem in the cybersecurity industry demonstrating students' ability to integrate principals of science and technology with fundamental business practices. The type of experience and the nature of the project vary depending upon the student's current situation, employment, and right-to-work status. A project report must be submitted, defended, and approved at the end of the Internship or Semester-In-Residence. In unusual circumstances where project requirements are not completed, defended, and approved at the end of MCS 690B, the student may complete the requirements within six months under the guidance of the advisory committee. In such cases, enrollment in MCS 699 is required.

Appendix B

# MS Cybersecurity
# Curriculum Map

| PSLO | Courses | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | MCS 510 | MCS 511 | MCS 512 | MATH 503 | MCS 610 | MCS 611 | MIS 522 | MGMT 521 | MIS 612 | MIS 622 | MCS 680 |
| 1a) Building a security schema and developing an infrastructure | I | I | I | I | R | R | R | | | | A |
| 1b) Developing security practice methodologies to scrutinize threats and identify defenses within a constantly-changing environment | I | I | I | I | R | R | R | | | | A |
| 2a) Structuring team dynamics, project management, and response to change | | | | | | R | R | R | | R | A |
| 2b) Identifying economic and regulatory issues | | | | | | R | | R | R | R | A |
| 2c) Analyzing risks and operationalizing security decisions | | | | | | R | R | R | R | R | A |

I = Introduced; R = Reinforced; A = Advanced level application

Appendix B1

# *Masters of Science in Cybersecurity*
# *Comprehensive Assessment Plan*

| *a* | *b* | *c* | *d* | *e* | *f* | *g* | *h* | *i* | *j* |
|---|---|---|---|---|---|---|---|---|---|
| **ULOs* | *PSLOs* | *Courses (Where SLOs are assessed)* | *Assessment activities (to measure each SLO)* | *Suggested assessment tools* | *Assessment schedule – how often SLOs will be assessed* | *How will data/ Findings be reported?* | *Designated personnel to collect, analyze, and interpret student learning outcome data* | *Program data/ findings dissemination schedule* | *Anticipated closing the loop strategies* |
| | 1a) Building a security schema and developing an infrastructure | MCS 611 | Examinations and report project | Common exam and rubric | Year 1 (Biennial schedule) | Exam and /or rubric scores will be aggregated, reviewed by team; reported to program faculty; annual reports to Academic Programs | Course instructor, program faculty | Semester following assessment activity | Program faculty will determine if change is needed; implement change in following year; re-measure the following year |
| | 1b) Developing security practice methodologies to scrutinize threats and identify defenses within a constantly-changing environment | | | | | | | | |
| | 2a) Structuring team dynamics, project management, and response to change | MIS 622 | Examination and projects | Common Exam and rubric | Year 2 (Biennial schedule) | Exam and /or rubric scores will be aggregated, reviewed by team; reported to program faculty; annual reports to Academic Programs | Course instructor, program faculty | Semester following assessment activity | Program faculty will determine if change is needed; implement change in following year; re-measure the following year |
| | 2b) Identifying economic and regulatory issues | | | | | | | | |
| | 2c) Analyzing risks and operationalizing security decisions | | | | | | | | |

*Campus-wide Learning outcomes for graduate programs (GLOs) are in development.

## Appendix C: Courses for the Degree Total: 38 units

### Six Required Technical Side Courses for MS Cybersecurity Total: 21 units

**MATH 503 Cryptography (3)**

Outcomes:

After completing this course students will be able to:

1. Identify basic structures of cryptographic algorithms from a mathematical and computer scientific viewpoint.
2. Recognize fundamental cryptographic protocols.
3. Identify common flaws in cryptographic regimes.

Course Description:

Fundamentals of protecting confidentiality, integrity and availability of information in computer systems. This course covers the fundamentals of cryptographic concepts and methods. Several encryption/decryption algorithms will be discussed. The topics include an introduction to the mathematics behind cryptography including number theory, group theory, and probability theory; cryptographic algorithms including classical methods, symmetric key systems, public key systems, hash functions, digital signatures and certificates; cryptanalysis and attacks; and access control including authentication and authorization. Assignments include programming labs to apply public keys, dictionary attacks, digital signatures, and certificates.

3 units lecture only

**MCS 510 Security in Computer Networks (3)**

Outcomes:

Upon successful completion of the course, students will be knowledgeable of the practical elements of networks security and related design. They will be able to:

1. Recognize design and analysis of network security architectures, protocols, and services in both wired and wireless networks.
2. Identify network security standards, their functionality and limitations.
3. Identify network attacks and analyze defense techniques against them.

Course Description:

Theoretical and practical aspects of security in computer networks, including wired and wireless networks. Topics will include: the basic concepts of communication networks and an introduction to TCP/IP architecture, the fundamental techniques and protocols used to insure secure communications, the common attacks and defenses, and the vulnerability assessment of network systems. Students will learn various aspects of security in computer networks, and the best techniques and tools against network attacks.

Prerequisite:

MATH503 Cryptography

3 units lecture only

**MCS 511 Secure Features in Operating Systems (3)**

Outcomes:

Upon successful completion of the course, students will be able to:

1. Identify fundamental security features in a modern operating system
2. Analyze threats behind operating system security
3. Identify vulnerabilities of a computer system
4. Identify the appropriate tools for applying OS security.

Course Description:
An overview of the current security of most commercial operating systems and examines the fundamental concerns of security in modern operating systems. Analysis of the operating systems model for computer system security criteria as it pertains to overall system vulnerability is covered. Based upon the security requirements and general architecture of secure operating systems publically available security enhanced operating systems are examined and evaluated.
3 unit lecture only

**MCS 512 Development of Secure Software (4)**
Outcomes:
Upon successful completion of the course, students will be able to:

1. Develop secure software
2. Identify security issues in current programming languages
3. Develop defensible applications using secure coding
4. Perform risk assessment and secure code analysis of existing systems

Course Description:
Introduction to the development of secure software during all phases of the software development life cycle. An emphasis is placed upon the secure code implementation and the most common pitfalls and security bugs found in programming languages, such as C/C++, Java, PHP and Perl. Risk assessments, threat modeling and secure code analysis of existing systems are also considered one of the primary topics. Hands-on exercises will be required in laboratory sessions. .
3 units lecture and 1 unit lab.

**MCS 610 Offensive Security & Penetration Testing (4)**
Outcomes:
Upon successful completion of the course, students will be able to:

1. Define and use the terms used in penetration testing.
2. Describe the steps in penetration testing.
3. Choose the right penetration technique for a given situation.
4. Choose the right penetration tools for a given situation.
5. Describe the required content of a report after penetration testing.

Course Description:
Introduction to the latest penetration testing techniques. Students will understand the fundamentals of penetration testing by learning the terms, tools and procedures used in the field. Topics will include: pre-engagement interactions, intelligence gathering, threat modeling, vulnerability analysis, exploitation, post exploitation, and reporting. Methodologies for web applications will be covered. Students will learn to choose the best techniques and tools for situations they will encounter. Hands-on exercises will be required in laboratory sessions.
Prerequisite:
All four MCS 500 level courses: 510, 511, 512, 513
3 unit lecture and 1 unit lab

**MCS 611 Intrusion Detection and Investigation (4)**
Outcomes:
Upon successful completion of the course, students will be able to:

1. Identify and apply network and protocol architectures

2. Describe the characteristics of common network attacks
3. Evaluate network traffic using open source tools
4. Analyze attack scenarios and report results

Course Description:
Uses current events and case studies to investigate threats against computers and networked systems. Covers principles and techniques of intrusion detection such as network traffic analysis, packet analysis, application protocol layer for common protocols (HTTP, SMTP, DNS, etc) and log analysis. Evaluates the use of intrusion detection tools and services. Emphasis is placed on investigation, analysis and outcome reports.

Prerequisite: All four MCS 500 level classes: 510, 511, 512, 513
3 unit lecture and 1 unit lab.

**Five Required Business Side Courses for MS Cybersecurity Total: 12 units**

**MGMT 521 Principles of Organizational Behavior and Leadership for Security Management (2)**
Outcomes:
Students will be able to:
1. Distinguish between the main concepts and theories of Organizational Behavior (OB) and Leadership.
2. Apply key OB and Leadership concepts to real world situations in cybersecurity.
3. Analyze organizational situations in terms of OB and Leadership theories and concepts.
4. Recognize OB and Leadership related traits and perspectives.

Course Description:
Covers the key topics in organizational behaviors and leadership seeking to explain people's behavior and experiences in various types of organizations, as well as how to effectively lead people to accomplish shared goals. Explores how research and knowledge of these topics can be applied in managing information systems and security related projects specifically, and in organizations more generally. Issues in contractual negotiations and effective communication inside organizations will also be addressed.
Prerequisite: N/A
2 units lecture only

**MIS 522 Information Systems and Security Management (2)**
Outcomes:
Students will be able to:
1. Identify information systems and key business strategies
2. Describe the principles of information technology security.
3. Analyze data value in business context
4. Describe the components of information security management and how the elements interact
5. Evaluate different methods for access control
6. Evaluate and justify security technology selections and designs.
7. Identify appropriate strategies to assure confidentiality, integrity, and availability of information.

Course Description:
Overviews the fundamental principles and components of information systems. Introduces the concepts and topics of Information Technology Security and Risk Management at the organizational level. Studies drivers and the requirements for information security, the integration of security into the systems design process, and life cycle of information security management.
Prerequisite: N/A

2 units lecture only

**MIS 621 Secure System Governance, Regulation, and Compliance (3)**
Outcomes:
Upon successful completion of the course, students will be able to

1. Identify the role of an information systems security (ISS) policy framework.
2. Analyze how security policies help mitigate risks and support business.
3. Identify components and basic requirements for creating a security policy framework.
4. Identify different methods, roles, responsibilities, and accountabilities of personnel, along with the governance and compliance of security policy framework.
5. Recognize ISS policies associated with the user domain, IT infrastructure, risk management and incident response teams (IRT).
6. Analyze social, legal and ethical issues represented by information technology environments.

Course Description:
Covers the fundamentals of developing business cases for information security (assurance) governance. Studies the development and implementation of IT strategies to integrate assurance functions to improve security, and ensure the preservation of the organization and its ability to continue to operate. Offers a comprehensive view of information security policies in business context and the psychology of implementation. Provides insight into governance, privacy, regulator mandates, business drivers, legal issues.
Prerequisite: MGMT 521 and MIS 522
3 units Lecture only

**MIS 622 Technology Assessment and Security Risk Management (3)**
Outcomes:
Upon successful completion of the course, students will be able to

1. Analyze and communicate appropriate financial, economical, and business models to assess technology investment decisions
2. Describe the fundamental concepts of Risk Management and Risk Management Life Cycle
3. Identify Risk Management Artifacts in an organizational environment
4. Conduct a Business Impact Assessment and develop a Security Risk Management plan
5. Compare the difference between qualitative and quantitative risk analysis methods and apply appropriate methods to the right situation
6. Describe the procedure for periodical security risk review

Course Description:
Examines variety of quantitative models, including financial, economic and business models, to analyze real managerial problems for technology assessment and investment that affect all types of institutions. Introduces the concept of risk and risk management and discusses up-to-date methods for both qualitative and quantitative risk analysis. Focuses on training future information technology or security managers to make better risk decisions.
Prerequisite: MGMT 521 and MIS 522
3 units Lecture only

**MCS 660 Communication in a Technical Industry (2)**
Outcomes:
Students will be able to:

1. Identify and analyze the rhetorical situation (communicative purpose, topic, goal, audience, method of delivery)

2. Create and deliver oral and/or visual presentations that clearly convey concise and precise messages designed for specific audiences.

Course Description:
Provides insight and practice in the forms of communication between technical and non-technical audiences including presentations, proposals, organizational reporting/reports, and other communication demands found in industry. Students will differentiate between objectives of the various communication purposes and understand key steps and ingredients for effective communication. Emphasizes basic skills for both written and oral communication and provides practice of these principles.
*Enrollment is restricted to students who have been admitted to the Master of Cybersecurity Program.*

**Culminating Experience Total 5 units**

**MCS 680A Semester in Residence Project Writing Workshop (1)**
Outcomes:
Students will
1. Research and develop a proposal starting with generating project ideas to multiple revisions of written proposal.
2. Create the components included in a written research proposal resulting in complete draft.

Course Description:
Provides the student with tools and a focused pathway to develop and complete their Semester in Residence Project. This process is imperative to the student's ability to produce a comprehensive final project, defense, and future industry presentations.
*Enrollment is restricted to students who have been admitted to the Master of Cybersecurity Program. This class cannot be repeated.*
Prerequisite: Completion of all 500 level classes.

**MCS 680B Internship/Semester in Residence/Project (4)**
Outcomes:
Students will be able to:
1. Develop an industry-based Semester-in-Residence project in one semester (spring, year 2) on a full-time basis.
2. Defend a Semester-in-Residence project with the guidance of an SIR Advisory committee.
3. Orally communicate the Semester-in-Residence project at year-end Master of Science in Cybersecurity Symposium.

Course Description:
Provides industry experience under the guidance of a project committee consisting of a faculty member, an industry member and the Program Director. The student will establish/accomplish goals, communicate work/project progress, acquire broad organization insight, and demonstrate core competencies required for the degree. The experience will culminate in a written project document and an oral presentation to fellow students, faculty, and company representatives on assigned work and project. The student will be required to complete an electronic submission of their Executive Summary to the library.
*Enrollment is restricted to students who have been admitted to the Master of Cybersecurity Program.*
Prerequisite: MCS 680A and Advancement to Candidacy.

**MCS 699 A/B/C/D/E/F Semester-in-Residence Project Extension (1/2/3/4/5/6)**

Course Description:

Registration is limited to students who have received a grade of Report in Progress (RP) in MCS 680B and who expect to use the facilities and resources of the University/Industry to work on or complete the project. May not be repeated more than two times. Graded Credit/No Credit. Enrollment Requirement: prior registration in MCS 680B with an assigned grade of Report in Progress (RP). Units may not be applied to the required units for the Master's degree.

*Enrollment is restricted to students who have been admitted to the Master of Science in Cybersecurity program or have obtained consent of the Program Director.*

**Alternative Course Which Can Be Taken In Place Of A Waived Required Course**

**MCS 697 A/B/C/D/E/F Directed Studies (1/2/3/4/5/6)**

Course Description:

Industrial or Academic research directed or sponsored by Industry and a PSM faculty. Enrollment is limited to students who have Graduate Standing and who expect to use the facilities and resources of Industry or the University. May be repeated one time. Graded Credit/No Credit. Units may be applied to the required units for the Master's degree.

*Enrollment restricted to students who have obtained consent of instructor.*

*Enrollment is restricted to students who have been admitted to the Master of Science in Cybersecurity program or have obtained consent of the Program Director.*

## Appendix C2: Master of Cybersecurity Program Course Schedule- Fall 2015

**All Courses are Required. Directed Study is offered as requested.**

| Year | Semester | Course Title | Instructor | No. of Units |
|---|---|---|---|---|
| 1 | Fall | MATH 503 - Cryptography | Sharif | 3 |
| | | MIS 522 – Information Systems and Security Management | Fang | 2 |
| | | MCS 660- Communication in a Tech Industry | Metzger | 2 |
| | Spring | MGMT 521 – Principles of Organizational Behavior and Leadership for Security Management | Kohles | 2 |
| | | MCS 510 – Security in Computer Networks | Majd | 3 |
| | | MCS 511 – Secure Features in Operation Systems | Springer | 3 |
| | Summer | MIS 621 – Secure Governance, Regulation, and Compliance | Sun | 3 |
| | | MCS 512 Development of Secure Software | Springer | 4 |
| 2 | Fall | MIS 622 – Technology Assessment and Security Risk Management | Fang | 3 |
| | | MCS 610 – Offensive Security & Penetration Testing | TBD | 4 |
| | | MCS 680A SIR Writing Workshop | | 1 |
| | Spring | MCS 680B- Internship/ Residency & Project | | 4 |
| | | MCS 611 – Intrusion Detection and Investigation | Macklin | 4 |
| | | | Total Units | 38 |

# Master of Science in Cyber Security

**5 Year Rolling Budget**

Program cost: $794/unit * 38 units = $30,172
$839/unit * 38 units = $31,880

| | FY 15/16 | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 |
|---|---|---|---|---|---|
| **Tuition** | $ 794 | $ 794 | $ 839 | $ 839 | $ 839 |
| **Target Number Participants** | 25 | 25 | 25 | 25 | 25 |
| **Units Taught in Program** | 15 | 15 | 15 | 15 | 15 |

| | | | | | |
|---|---|---|---|---|---|
| **Tuition** | $ 794 | $ 794 | $ 839 | $ 839 | $ 839 |
| **Target Number Participants** | 25 | 25 | 25 | 25 | 25 |
| **Units Taught in Program** | 23 | 23 | 23 | 23 | 23 |

| | FY 15/16 | FY 16/17 | FY 17/18 | FY 18/19 | FY 19/20 |
|---|---|---|---|---|---|
| **Revenue** | | | | | |
| Tuition | $ 297,750 | $ 754,300 | $ 771,175 | $ 797,050 | $ 797,050 |
| Attrition | $ - | $ (30,172) | $ (30,172) | $ (30,172) | $ (30,172) |
| **Total Revenue** | $ 297,750 | $ 724,128 | $ 771,175 | $ 797,050 | $ 797,050 |
| **Direct Expenses** | | | | | |
| TT Faculty Program Director | $ 41,666 | $ 100,000 | $ 103,000 | $ 106,090 | $ 109,273 |
| IST | $ 12,500 | $ 30,000 | $ 30,900 | $ 31,827 | $ 32,782 |
| Instructors | $ 19,809 | $ 63,829 | $ 65,744 | $ 67,716 | $ 69,748 |
| Faculty Payroll benefits | $ 48,708 | $ 44,725 | $ 46,067 | $ 47,449 | $ 48,873 |
| Semester in Residence Committee Membe | $ - | $ 10,000 | $ 10,000 | $ 10,000 | $ 10,000 |
| Library Resources | $ 11,600 | $ 11,600 | $ 11,600 | $ 11,600 | $ 11,600 |
| Professional Affiliation Conference | $ 1,125 | $ 1,125 | $ 1,125 | $ 1,125 | $ 1,125 |
| Office Supplies | $ 500 | $ 500 | $ 500 | $ 500 | $ 500 |
| Professional Memberships | $ 1,500 | $ 2,500 | $ 2,500 | $ 2,500 | $ 2,500 |
| Postage & Copying | $ 75 | $ 75 | $ 75 | $ 75 | $ 75 |
| Promotion, Advertising & Print | $ 4,000 | $ 4,000 | $ 4,000 | $ 4,000 | $ 4,000 |
| **Total Direct Expenses** | **$ 141,483** | **$ 268,354** | **$ 275,511** | **$ 282,882** | **$ 290,475** |
| **Operating Income/Margin** | **$ 156,267** | **$ 455,774** | **$ 495,664** | **$ 514,168** | **$ 506,575** |
| **Indirect Expenses** | | | | | |
| CSU/CSUSM, FAS, IITS | $ 54,640 | $ 128,341 | $ 136,063 | $ 140,516 | $ 140,971 |
| CoBA $254/unit fee | $ 25,400 | $ 63,500 | $ 63,500 | $ 63,500 | $ 63,500 |
| CoBA @ 5% of class gross | $ - | $ - | $ - | $ - | $ - |
| CSM @ 5% of class gross | $ 10,918 | $ 27,790 | $ 28,409 | $ 29,365 | $ 29,365 |
| EL Costs @ 30% of Revenue | $ 89,325 | $ 226,290 | $ 231,353 | $ 239,115 | $ 239,115 |
| | $ 180,283 | $ 445,921 | $ 459,324 | $ 472,496 | $ 472,951 |
| **Total All Expenses** | **$ 321,766** | **$ 714,275** | **$ 734,835** | **$ 755,378** | **$ 763,426** |
| **Net Profit/Loss** | **$ (24,016)** | **$ 9,853** | **$ 36,340** | **$ 41,672** | **$ 33,624** |
| % Net Margin | -8% | 1% | 5% | 5% | 4% |
| **Loss Carry Forward View** | $ (24,016) | $ (14,163) | $ 22,177 | $ 63,849 | $ 97,473 |

Assumptions:

1) Start date for Faculty/Director and IST is Aug 1 according to Rikka.
2) Delay purchase of Library recommemdations until Director arrives.
3) CSU/CSUSM/IITS 15.5% based on revenue; FAS is 6% of Direct Expenses.
4) COBA instruction for 10 credit units (MIS 522, MIS 621, MIS 622 & MGMT 521.)
5) COBA gains $254 Professional Fee/unit rather than 5% of revenue.

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:** October 1, 2014

**To:** Dr. Rika Yoshii

**From:** Dr. Jennifer Fabbi
Dean, Library

**Subject:** Library Review of the Proposal for Master of Science in Cybersecurity

Thank you for the opportunity to respond to the proposal for a Professional Science Masters Degree in Cybersecurity. The following information reviews the current capacity and describes probable needs of the CSUSM Library to support this program. Talitha Matlin, currently the STEM Librarian, has reviewed the program proposal.

**Existing Collections**
Collections relevant to the proposed program would be housed with the CSUSM Kellogg Library, or more likely, virtually accessible through the Library website The California State University at San Marcos (CSUSM) Library (http://biblio.csusm.edu). CSUSM has no branch or satellite libraries on or off campus. The CSUSM Library currently has monographs and journals to support undergraduate/graduate programs in Computer Science and Business, which also appear to be relevant to significant aspects of the PSM in Cybersecurity program. Relevant current holdings include:

- Safari eBooks collection (over 9,500 programming ebooks, with 150+ titles related to Network Security)
- Science Direct books and journals related to Network Security and General Computer Science
- Wiley General & Introductory Computer Science, Information Science, and Computing journal collections
- Business Source Premier database (topical coverage includes general business, marketing, management, MIS, POM, accounting, finance, and economics)
- EBSCO Host Military & Government Collection (format includes academic periodicals and general interest magazines)

**Additional Needed Collections**
The proposal states that many (if not all) of the students will be working professionals. While many of the students may have access to materials through their employers/internship sites,

the CSUSM Library needs to ensure equal access to relevant, industry-standard literature for the entire cohort. Although there will be a relatively small number of students enrolled in the program (25 students per cohort, with 2 cohorts running simultaneously after the first year) and the Library does have strong inter-library loan/resource sharing services, some increase to the monograph acquisitions would be needed in order to ensure a substantive collection is immediately available to students and faculty.

The Library does subscribe to some of the major databases that would be used by students and faculty in the PSM Cybersecurity program. However, as the Computer Science/IT-related offerings provided through the College of Science and Mathematics and Extended Learning continue to grow and increase in number, the resulting expansion in topical scope and increase in FTES places additional pressures and demands on the existing information resources.

To keep up with the continued growth and advancement of Computer Science/IT-related programs at CSUSM, we strongly recommend the following resources be added in order to provide an enriching educational experience and to maintain excellence in the research activities of faculty and students:

| **Core Resources** | **Notes** | **Cost** |
|---|---|---|
| Monographs (physical or electronic) | Titles related to general cybersecurity/encryption | $1,000 (annually) |
| Association for Computing Machinery Digital Library | Journals and conference proceedings from the Association for Computing Machinery, the accrediting body for Computer Science programs | $6,182 (annually) |

| **Highly Recommended Resources** | **Notes** | **Cost** |
|---|---|---|
| IEEE Xplore Digital Library Journals and Proceedings Collection | One of the premier resources for scientific and technical content | $4,463 (annually) |

Faculty may, at any time, contact the librarian assigned to the Cybersecurity PSM regarding suggestions for additions to the collection. Further, reports, assessment, and other analysis of library collections in all subjects are done in response to program review, by the library liaison.

**Reference and instruction by subject specialist librarians**

A Cybersecurity PSM program bears some topical overlap to Computer Science and Business. Currently, Talitha Matlin is the subject specialist for the College of Science and Mathematics and Ann Fiegen is the subject specialist for the College of Business Administration. Given this portfolio of subjects, these librarians will serve as liaisons to the Cybersecurity PSM program, with Talitha Matlin (STEM Librarian), acting as the primary contact.

These librarians have provided online and in-class instruction to students in the aforementioned fields. Most relevant to the PSM programs is online instruction through course guides and online tutorials; these librarians would provide this type of instruction as part of their liaison responsibilities for the Cybersecurity PSM program.

In addition, as students will be required to submit a Project-in-Residence as their culminating experience, they will need to work closely with Carmen Mitchell, Institutional Repository Librarian, in their second year. Ms. Mitchell consults and assists graduate students in the areas of intellectual property, copyright, fair use, and electronic thesis/project submission.

Basic information about the library's collections and services follows in the table below.

| | |
|---|---|
| Library holdings | http://biblio.csusm.edu/external/about-the-library/collection-overview |
| Circulation | http://biblio.csusm.edu/external/policies/books-%2526-media-borrowing-policies |
| Inter-library loan services | http://biblio.csusm.edu/interlibrary-loan-borrowing-policies |
| Reference/Research help | https://biblio.csusm.edu/research-assistance |
| Information Literacy Program | http://biblio.csusm.edu/about/departments/337/info |
| E-thesis, project, and dissertation submission | http://biblio.csusm.edu/guides/subject-guide/193-CSUSM-ETD-Submission-Guide/ |

The Library looks forward to continued collaboration with those working on the proposed Cybersecurity PSM program and is happy to provide further information. It is essential that the program proposers continue discussions with the Library as the program is approved to ensure that students and faculty have sufficient information resources at the inception of the program. Please contact me when budget discussions begin with Extended Learning in order to begin this process.

cc: Ann Fiegen
Katherine Kantardjieff
Jill Letchewski
Talitha Matlin
Carmen Mitchell
Hua Yi

**Appendix E MEMORANDUM FROM IITS**

DATE: September 24, 2014

To: Budget and Long Range Planning Committee

From: Bill Ward
Interim Dean, Instructional Information Technology Services/CIO

Subject: IITS Comments for CyberSecurity

Thank you for the opportunity to provide additional comments for the program proposal for CyberSecurity. As this description is written, the program states that there are some courses that will require special computer lab technology and on-campus support from IITS. This program understands that computer labs are impacted so will use these resources during the evenings. However, special configuration of these lab classes will be necessary to protect the campus production network. In addition, some classes will need server and firewall technologies.

After reading all course descriptions it is apparent that the CyberSecurity program is going to need a special computer lab configuration and technology support to develop and maintain the lab environment during the course Although technology requirements for the courses are not yet specific, IITS can likely provide the special infrastructure needed (switches, firewalls, virtual servers, cable infrastructure) since our feeling is that this could benefit stateside computer science and MIS courses as well. We estimate the cost of the program once lab work starts will be ½ a staff person. The budget figure I would use is $30,000 per year. The technical staff is required for server setup and maintenance and (unless the courses use a dedicated lab) work must be done before and after each class session to provide the isolated network environment needed for coursework. There will also be technical staff needed to program various network technologies in order to mimic what students would encounter in the real world.

To effectively support any proposal that includes new courses and new faculty we have the following guidelines.

- Any new course must comply with the CSU Accessibility Technology Initiative (ATI) guidelines for instructional materials: "New courses and new course content, including instructional materials and instructional websites, will be designed and authored in a manner that incorporates accessibility." An instructional developer will meet with the faculty member designing the new course to review specific accessibility guidelines and ensure that the course content is in compliance with the ATI. Typical issues include captioning multimedia, adding image tags to PowerPoint, using styles in Word, and naming links appropriately in the LMS or website. Analyzing the

instructional materials and training how to make these items accessible could take a minimum of 3 hours of instructional development time.

- New faculty members are usually not familiar with our Learning Management System (LMS) or the multimedia options we offer. Therefore, they are highly encourage to attend workshops or request an orientation by contacting ids@csusm.edu to become familiar with all of the options that Academic Technology Services has available to support their teaching. This training can range from 1 hour to 20 plus hours depending on the interactive content, media integration and whether the course is flipped, hybrid, or fully online.
- It is understood that these courses are live lecture based but if in the future Online courses are planned it should be noted that they are labor-intensive to develop. The Instructional Developer team provides one-on-one and professional development opportunities to prepare faculty to develop quality online courses. It is suggested that faculty teaching online meet with the IDS team one semester in advance of teaching the course.
- Multimedia resources including video studios, Mediasite studio, and videoconferencing rooms are supported Monday through Friday, 8 am to 5 pm. Funds need to be identified for additional support for programs with support needs outside of this schedule.

## Appendix F Email from Academic Programs on Pilot Programs

I am hoping that a response to this e-mail will suffice.

Regarding pilot status, here are the criteria that must be met:

### Pilot-Program Criteria

Pilot degree programs must meet all of the following six criteria:

1. The proposed program could be offered at a high level of quality by the campus within the campus's existing resource base, or there is a demonstrated capacity to fund the program on a self-support basis.

2. The proposed program is not subject to specialized accreditation by an agency that is a member of the Association of Specialized and Professional Accreditors, or it is currently offered as an option or concentration that is already recognized and accredited by an appropriate specialized accrediting agency.

3. The proposed program can be adequately housed without a major capital outlay project. Major capital outlay construction projects are those projects whose total cost is $610,000 or more (as adjusted pursuant to Cal. Pub. Cont. Code §§ 10705(a); 10105 and 10108).

4. It is consistent with all existing state and federal law and Trustee policy.

5. It is either a bachelor's or master's degree program.

6. The proposed program has been subject to a thorough campus review and approval process.

These come from the CO (I am attaching the full version of the procedure for your information). You are correct that there is one other program being proposed as a pilot – the MS in Kinesiology. We do not yet have approval for that yet,

Regarding your question about when we are allowed to use pilots, that is a conversation that needs to happen with the Provost/Vice Provost. We do not have a policy or procedure on campus to determine when it is appropriate to use one of our pilot slots. Having said that, I will raise this issue and get back to you.

I hope this helps.

Regards,

Regina