1. New Program Proposal Form

Form NP
NEW PROGRAM PROPOSAL FORM

Sponsoring Institution(s):	Southeast Missouri State University
Program Title:	Cybersecurity
Degree/Certificate:	Bachelor of Science
Options:	None
Delivery Site(s):	Cape Girardeau, Missouri
CIP Classification (provide a CIP code):	11.1003
Implementation Date:	Fall 2011
Cooperative Partners:	None
Expected Date of First Graduation:	Spring 2014

AUTHORIZATION

Dr. Ronald Rosati, Provost		
Name/Title of Institutional Officer	Signature	Date

Dr. Randall Shaw, Dean, School of Polytechnic Studies	573-651-5915
Person to Contact for More Information	Telephone

2. Need:

A. Student Demand:

i. Estimated enrollment each year for the first five years for full-time and part-time students

Form SE
STUDENT ENROLLMENT PROJECTIONS

Year	1	2	3	4	5
Full-Time	23	46	69	92	92
Part-Time	2	4	6	8	8
TOTAL*	25	50	75	100	100

2. In each case, an average of 12 credit hours per student is projected.

ii. Will enrollment be capped in the future?
Response: No.

B. Market Demand:

i. National, state, regional, or local assessment of labor need for citizens with these skills
Response: Jim Gosler, Sandia Fellow, NSA Visiting Scientist, and the founding Director of the CIA's Clandestine Information Technology Office, recently stated that "There are about 1,000 security people in the US who have the specialized security skills to operate effectively in cyberspace. We need 10,000 to 30,000." The U.S. Department of Labor, Bureau of Statistics, projects a 20% growth of jobs in this field nationally adding up to 135,500 jobs by 2018 and Missouri anticipates a 21% growth by 2018. Also, a November 11, 2010 search of indeed.com for cybersecurity jobs in Missouri provided ads for 46 different positions (http://www.indeed.com/q-Cyber-Security-l-Missouri-jobs.html). About half of those jobs were either in the St. Louis area or within 50 miles of there. Members of the Southeast Cybersecurity Advisory Committee, representing computer security and forensics interests for organizations in banking, health care, telecommunications, manufacturing, and law enforcement also report a regional need for cybersecurity professionals.

C. Societal Need:

i. General needs which are not directly related to employment
*Response: There is a definite need to "protect America's computers and networks from assault" (*Pittsburgh Tribune-Review*, September 6, 2010). Howard A. Schmidt, national cybersecurity coordinator and special assistant to President Barack Obama stated in a video message on November 8, 2010 to the attendees of 2010 IEEE International Conference on Technologies for Homeland Security: "We rely on cyber networks to control and manage transportation, electricity and banking, just to name a few parts of our critical infrastructure. Cybersecurity risks pose some of the most serious economic and national security challenges of the 21st century. Going forward, economic prosperity and*

our way of life depends on strong cybersecurity built on the backbone of resilient cyber infrastructure."

D. Methodology used to determine "B" and "C" above.

Response: 1) Discussions with government officials from the FBI, DEA, and Homeland Security working in cybersecurity in face-to-face meetings on October 18-20, 2010 in Washington, DC. 2) Meeting of the new Southeast Cybersecurity Advisory Board on October 22, 2010 in Cape Girardeau. They are individuals representing computer security and forensics interests for organization in the banking, health care, telecommunications, manufacturing and law enforcement fields. 3) U.S. Bureau of Labor Statistics website (http://www.bls.gov). 4) Various print and electronic articles.

3. Duplication and Collaboration: If similar programs currently exist in Missouri, what makes the proposed program necessary and/or distinct from the others at public institutions, area vocational technical schools, and private career schools?
Response: There is no duplication; similar programs do not currently exist in Missouri.

   Does delivery of the program involve a collaborative effort with any external institution or organization? *Response: No.* If yes, please complete Form CL.

4. Program Structure:

Form PS
PROGRAM STRUCTURE

A. Total credits required for graduation: 124 cr.

B. Residency requirements, if any: 30 cr. (General University Guidelines)

C. General education (total credits): 55 cr. (Univ. Studies req. w/2 five cr. Courses)

General education courses (specific courses OR distribution area and credits):
[See **Appendix A** for the names of all courses listed below.]

UI100	3	cr.	Artistic Exp	3	cr.	Polit. Sys	3	cr.
EN100	3	cr.	Literary Exp	3	cr.	Major Civ.	3	cr.
MA135	5	cr.	Oral Exp	3	cr.	UI3xx	3	cr.
PH120	5	cr.	Written Exp	3	cr.	UI3xx	3	cr.
MN220	3	cr.	Behav. Sys.	3	cr.	UI410	3	cr.
SW207	3	cr.	Living Sys.	3	cr.			Cr.

D. Major requirements (total credits): 69 cr.

MA223	3	cr.	TN425	3	cr.	MA464	3	cr.
IM102	3	cr.	TN565	3	cr.	CY2xx*	3	cr.
TN255	3	cr.	CS155	4	cr.	CY3xx*	3	cr.
ET245	3	cr.	CS265	4	cr.	CY3xx*	3	cr.
TN254	3	cr.	CS300	4	cr.	CY4xx*	3	cr.
TN275	3	cr.	CS440	3	cr.	CY4xx*	3	cr.
TN375	3	cr.	IS245**	3	cr.			Cr.
TN395	3	cr.	TN435	3	cr.			Cr.

* - It is proposed that there be a new subject code CY (for Cybersecurity) with five new courses, as outlined in Appendix B.

** - This is a proposed new course in web development (see Appendix C).

E. Free elective credits
(sum of C, D, & E should equal A): 0 cr.

F. Requirements for thesis, internship or other capstone experience: (UI410) 3 cr.

G. Any unique features such as interdepartmental cooperation: Department of Computer Science (18 cr.)
Department of Mathematics (6 cr)

6. Program Characteristics and Performance Goals: For collaborative programs, responsibility for program evaluation and assessment rests with the institution(s) granting the degree(s).

Form PG
PROGRAM CHARACTERISTICS AND PERFORMANCE GOALS

Institution Name: Southeast Missouri State University

Program Name: Bachelor of Science in Cybersecurity

Date: Fall 2011

(Although all of the following guidelines may not be applicable to the proposed program, please carefully consider the elements in each area and respond as completely as possible in the format below. Quantification of performance goals should be included wherever possible.)

Student Preparation

- Any special admissions procedures or student qualifications required for this program which exceed regular university admissions, standards, e.g., ACT score, completion of core curriculum, portfolio, personal interview, etc. Please note if no special preparation will be required.
  Response: No special preparation will be required.

  Characteristics of a specific population to be served, if applicable
  Response: Individuals seeking formal education and training to pursue careers in cybersecurity.

Faculty Characteristics

- Any special requirements (degree status, training, etc.) for assignment of teaching for this degree/certificate.
  Response: There are faculty members in Industrial and Engineering Technology (IET), Computer Science, and Mathematics that have experience related to cybersecurity. Also, IET is also presently searching for a full time faculty position in cybersecurity. Most of the new Cyxxx courses will be taught by this faculty member. Faculty teaching courses from Industrial and Engineering Technology, Computer Science, and Mathematics all have appropriate degrees and training in their respective areas of expertise in order to teach their respective supporting courses for this program.

- Estimated percentage of credit hours that will be assigned to full-time faculty. Please use the term “full-time faculty” (and not FTE) in your descriptions here.
  Response: It is anticipated that a majority of the courses in the major, i.e. more than 90% will be taught by full time University faculty.

- Expectations for professional activities, special student contact, teaching/learning innovation.
  Response: As expected of all faculty members at Southeast, faculty teaching in the proposed program will have expectation for professional development activities to keep them current in their respective fields of expertise.

Enrollment Projections

- Student FTE majoring in program by the end of five years:
  Response: FTE=100.0
- Percent of full-time and part-time enrollment by the end of five years:
  Response: Full Time=92%; Part Time=8%.

Student and Program Outcomes

- Number of graduates per annum at three and five years after implementation:
  Response: 3 Yr=5; 5 Yr=20

- Special skills specific to the program:
  Response: The program objectives of the Cybersecurity program is that upon graduation students will be able to:
  1. *Understand and be able to apply informational assurance fundamentals.*
  2. *Understand and be able to apply computer forensics fundamentals.*
  3. *Assess, implement, maintain, and manage security needs of computer networks and telecommunication systems.*
  4. *Demonstrate proficiency in secure programming.*
  5. *Do one of:*
     a. *Enter the workforce as an entry-level cybersecurity professional.*
     b. *Be accepted into a graduate program related to cybersecurity.*
  6. *Understand the need for lifelong learning in their cybersecurity careers.*
  7. *Exhibit ethical and legal responsibilities of a cybersecurity professional.*
  8. *Demonstrate the ability to communicate effectively.*
  9. *Demonstrate critical thinking skills.*

  [The last two are university-wide objectives.]

- Proportion of students who will achieve licensing, certification, or registration:
  Response: N/A

- Performance on national and/or local assessments, e.g., percent of students scoring above the 50th percentile on normed tests; percent of students achieving minimal cut-scores on criterion-referenced tests. Include expected results on assessments of general education and on exit assessments in a particular discipline as well as the name of any nationally recognized assessments used.
  Response: N/A

- Placement rates in related fields, in other fields, unemployed:
  Response: Related Field=90% and Other Fields=10%

- Transfer rates, continuous study
  Response: N/A

Program Accreditation

- Institutional plans for accreditation, if applicable, including accrediting agency and timeline. If there are no plans to seek specialized accreditation, please provide reasons.
  Response: There is not yet an accrediting body for cybersecurity degree programs. However, the National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) program. The goal of this program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in information assurance (IA) and producing a growing number of professionals with IA expertise in various disciplines. Designation as a CAE/IAE is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation.

  Since an institution's focus on information assurance must have been in effect for at least two years prior to applying for recognition as a CAE/IAE center. Thus, the plan is for Southeast to make such an application in the fall of 2013.

Alumni and Employer Survey

- Expected satisfaction rates for alumni, including timing and method of surveys
  Response: Surveys will be conducted of graduates within six months of graduation from the fall and spring terms requesting their input, among other things, on their satisfaction with the quality of the program. This will be followed up by an every three year follow-up of these graduates to assess the effectiveness of the program in preparing them for their careers.

- Expected satisfaction rates for employers, including timing and method of surveys.
  Response: Surveys will be conducted of employers of graduates every three years requesting their input on quality of the program and its graduates. The Southeast Cybersecurity Advisory Committee, that meets twice per year, will also provide input during the meetings.

7. Accreditation: If accreditation is not a goal for this program, provide a brief rationale for your decision. If the institution is seeking program accreditation, provide any additional information that supports your program.
   Response: There is not yet an accrediting body for cybersecurity degree programs. However, the National Security Agency (NSA) and the Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Information Assurance Education (CAE/IAE) program. The goal of this program is to reduce vulnerability in our national information infrastructure by promoting higher education and research in information assurance (IA) and producing a growing number of professionals with IA expertise in various disciplines. Designation as a CAE/IAE is valid for five academic years, after which the school must successfully reapply in order to retain its CAE designation.

   Since an institution's focus on information assurance must have been in effect for at least two years prior to applying for recognition as a CAE/IAE center. Thus, the plan is for Southeast to make such an application in the fall of 2013.

8. Institutional Characteristics: Please describe succinctly why your institution is particularly well equipped or well suited to support the proposed program.
   Response: The Department of Industrial and Engineering Technology is well suited to provide the Bachelor of Science in Cybersecurity degree because of the excellent faculty and facilities associated with the department, as well as faculty and facilities in the collaborating departments. In addition to this, almost all courses associated with the proposed program (except for six new additional courses) are currently available and being offered at the university.

9. Any Other Relevant Information: *Response: None*

Appendix A

Program Requirements with Course Names

Dept of Industrial & Engineering Technology
Program Proposal for
BS DEGREE IN CYBERSECURITY

University Studies (55 Credit Hours)

UI100 First Year Seminar	3
Artistic Expression	3
Literary Expression	3
Oral Expression	3
EN 100 English Composition	3
Written Expression	3
Behavioral Systems	3
Living Systems	3
Political Systems	3
Development of a Major Civilization	3
MA135 Pre Calculus (Logical Systems)	5
Economic Systems (MN220)	3
Social Systems (SW207)	3
Physical Systems (PH120)	5
UI3xx	3
UI3xx	3
UI410 IET Senior Capstone	3

Major Courses (69 Credit Hours)

CS155 Computer Science I	4
CS265 Computer Science II	4
CS300 Computer Science III	4
CS440 Database	3
CY2xx Introduction to Cybersecurity (NEW PROPOSED)	3
CY3xx Information Security and Assurance (NEW PROPOSED)	3
CY3xx Information Security in System Administration (NEW PROPOSED)	3
CY4xx Web Application Security (NEW PROPOSED)	3
CY4xx Computer Forensics (NEW PROPOSED)	3
ET245 Logic Circuits	3
IM102 Technical Communications	3
IS245 Web Development & Security (NEW PROPOSED)	3
MA223 Elementary Probability & Statistics	3
MA464 Mathematical Cryptography	3
TN254 Network Communications	3
TN255 Microcomputer Maintenance & Troubleshooting	3
TN275 Network Fundamentals	3
TN375 Network Routing Protocols and Concepts	3
TN395 Server Maintenance & Troubleshooting	3
TN425 Wireless Communications & Mobile Data Networks	3
TN435 Network Security	3
TN565 Network Management	3
TOTAL	**124**

Appendix B

New Cybersecurity Core Courses

New Cybersecurity Core Courses
November 17, 2010

On pages 3-7 are outlines for five proposed new courses:
CY 2xx Introduction to Cybersecurity
CY 3xx Information Security and Assurance
CY 3xx Information Security in System Administration
CY 4xx Web Application Security
CY 4xx Computer Forensics
[Note: The registrar has said that the CY prefix has not been used to date and can be used here.]

Page 2 has a table mapping these courses to the Cybersecurity program objectives.

Among the steps involved in developing those courses and the rest of the proposed Cybersecurity curriculum:

- Research into existing undergraduate computer security programs;
- Phone conversations and email exchanges with several of the "Top 10" universities in preparing cybersecurity professionals, from a list provided by President Dobbins;
- A visit to several organizations (FBI, DEA, DHS and SANS Institute) in Washington, D.C. on October 18-20; and
- A meeting with Southeast's new Cybersecurity Advisory Board on October 22.

Specific References:

- The following SANS (SysAdmin, Audit, Network, Security) Institute course descriptions (http://www.sans.org/security-training/courses.php):
  - SEC301 Intro to Information Security
  - SEC401 SANS Security Essentials Bootcamp Style
  - SEC408 Computer Forensic Essentials
  - SEC508 Computer Forensics, Investigation, and Response
  - SEC542 Web Application Penetration Testing and Ethical Hacking
  - DEV422 Defending Web Applications Security Essentials
  - DEV532 Essential Secure Coding in ASP.NET
  - LEG523 Legal Issues in Information Technology and Information Security
- *Computer Security: Art and Science* by Matt Bishop (Pearson Education, 2003, 10th prntg.)
- Telecon with University of Missouri-Columbia cybersecurity faculty – October 1, 2010
- Discussions with various organizations in Washington, DC area – October 18-20, 2010
- Rough draft of notes from Cybersecurity Advisory Board meeting – October 22, 2010

Committee on National Security Systems (CNSS) standards covered:

- NSTISSI 4011 National Training Standard for Information Systems Security (INFOSEC) Professionals
- NSTISSI 4013 National Information Assurance Training Standard for Systems Administrators (SA)

[Meets NSA Center of Academic Excellence in Information Security Education requirements]

Program Objectives

The program objectives of the Cybersecurity program is that upon graduation students will be able to:

1. Understand and be able to apply informational assurance fundamentals.
2. Understand and be able to apply computer forensics fundamentals.
3. Assess, implement, maintain, and manage security needs of computer networks and telecommunication systems.
4. Demonstrate proficiency in secure programming.
5. Do one of:
   c. Enter the workforce as an entry-level cybersecurity professional.
   d. Be accepted into a graduate program related to cybersecurity.
6. Understand the need for lifelong learning in their cybersecurity careers.
7. Exhibit the ethical and legal responsibilities of a cybersecurity professional.
8. Demonstrate the ability to communicate effectively.
9. Demonstrate critical thinking skills.

[The last two are university-wide objectives.]

Map of Cybersecurity Core Courses to Program Objectives

Cybersecurity Program Objective # → Courses ↓	1	2	3	4	5	6	7	8	9
CY 2xx Introduction to Cybersecurity	X	X				X	X		
CY 3xx Information Security and Assurance	X			X		X			X
CY 3xx Information Security in System Administration	X		X		X	X	X	X	X
CY 4xx Web Application Security	X			X		X			X
CY 4xx Computer Forensics		X			X	X	X	X	X

CY 2xx Introduction to Cybersecurity

Prerequisite: TN 275 (Network Fundamentals)

Credit Hours: 3

Proposed Introduction Date: Fall 2012

Course Description:
Broad introduction to the field of cybersecurity. Information assurance terminology, issues, policies and secure system design. Computer forensics investigation, collection and analysis of data, and methodology.

Course Objectives: At end of this course, a student should be able to:

1. Understand basic information assurance terminology.
2. Implement computer security policies.
3. Demonstrate how secure computer systems are designed.
4. Identify basic computer forensic terminology.
5. Utilize the basic methodology of a computer forensic investigator.
6. Perform some basic forensic investigation using up-to-date software tools.

Contents:

- Information Assurance (about 10 weeks)
    - Basic components (confidentiality, integrity, availability)
    - Threats (disclosure, deception, disruption, usurpation)
    - Human issues (organizational, people)
    - Access control
    - Security policies
    - Design of secure systems
- Computer Forensics (about 5 weeks)
    - Fraud, insider threats, industrial espionage, phishing
    - The computer forensic investigator
    - Collecting and analyzing data from computer systems
    - Fundamental steps of the in-depth computer forensic methodology
    - Windows Digital Forensics (Windows XP through Windows 7 and Server 2008)
    - Computer forensic tools

CY 3xx Information Security and Assurance

Prerequisites: CY 2xx (Introduction to Cybersecurity) and
CS 300 (Computer Science III) and
TN 435 (Network Security)

Credit Hours: 3

Proposed Introduction Date: Spring 2013

Course Description:
Essential components and features of an information security system. Methods of system attacks, intrusion detection and prevention. Business and operational issues in information security. Information assurance and trust. Design and construction of secure systems.

Course Objectives: At end of this course, a student should be able to:

1. Apply the fundamentals of intrusion detection and prevention.
2. Identify business and operational issues in information assurance.
3. Demonstrate how secure systems are built, including the software engineering issues involved.

Contents:

- Review of CY 2xx information assurance material
- Intrusion Detection and Prevention
  - Host-based
  - Network-based
- Honeypots
- Methods of attacks
- Business and Operational issues
  - E-commerce
  - Risk management
  - Cost-benefit analysis
  - Supply chain management
- Operations security
- Assurance and trust
- Building secure systems
  - Review of software engineering fundamentals from CS 300 (lifecycle, development models)

CY 3xx Information Security in System Administration

Prerequisites: CY 3xx (Information Security and Assurance) and MA 464 (Cryptography)

Credit Hours: 3

Proposed Introduction Date: Fall 2013

Course Description:
Securing information through cryptographic and other means of access control. Security in administration of both Windows- and Linux-based systems. Legal and policy issues.

Course Objectives: At end of this course, a student should be able to:

3. Implement security access control mechanisms.
4. Identify the security issues involved in Windows family of operating systems.
5. Identify the security issues involved in the Linux operating system.
6. Understand the fundamentals of information technology security law and policy.

Contents:

- Security access control
  - Cryptographic (e.g. SSL)
  - Non-cryptographic (e.g. steganographic)
- Windows system security
  - Overview of the Windows family
  - The security infrastructure
  - Permissions and user rights
  - Security policies and templates
  - Service packs, patches, and backups
  - Securing network services
  - Auditing and automation
- Linux system security
  - Overview (command line, virtual machines)
  - OS security
  - Security tools
  - Maintenance, monitoring and auditing
- Fundamentals of IT security law and policy

CY 4xx Web Application Security

Prerequisites: CY 2xx (Introduction to Cybersecurity) and
IS 245 (Web Development and Security – to be proposed by computer science)

Credit Hours: 3

Proposed Introduction Date: Spring 2014

Course Description:
Development of secure web-based systems. Security mitigation strategies and secure coding. Penetration testing. Security in systems using advanced web technologies.

Course Objectives: At end of this course, a student should be able to:

1. Develop and implement information assurance mitigation strategies throughout the web application development cycle.
2. Understand fundamental language-independent security strategies.
3. Implement security strategies in the .NET environment.
4. Implement, manage and protect Web applications.
5. Understand the basic principles of the Open Web Application Security Project.
6. Correctly perform penetration testing on a Web application.

Contents:

- Mitigation strategies (infrastructure, architecture, and coding perspectives)
- Programming language-independent security strategies
- Secure coding in .NET
- Implementing, managing or protecting Web applications
- Open Web Application Security Project **(**OWASP**)**
    - OWASP Top 10 Project
- Penetration testing
- Web 2.0 technologies (AJAX and web services)

CY 4xx Computer Forensics

Prerequisites: CY 2xx (Introduction to Cybersecurity) and
CY 3xx (Information Security in System Administration)

Credit Hours: 3

Proposed Introduction Date: Spring 2014

Course Description:
Implementation of computer forensic methodology. File system analysis in Windows. Response techniques, evidence acquisition, timeline analysis, extraction and recovery of files and data. Dealing with as-yet-unknown malware.

Course Objectives: At end of this course, a student should be able to:

1. Understand how to perform in-depth file system analysis.
2. Implement file system analysis on a Windows operating system.
3. Understand how computer forensics should be performed when responding to an incident.
4. Acquire memory and other types of computer evidence.
5. Recover files and data previously inaccessible.
6. Perform a timeline analysis on a file system.
7. Locate previously-unknown malware on a computer system.

Contents:

- Review of CY 2xx computer forensics material
- In-depth file system analysis
- Windows NTFS, FAT, exFAT dissection
- Computer forensics for incident responders
- Memory acquisition
- Live response techniques
- Complex evidence acquisition
- File system timeline analysis
- Low level extraction/recovery of data and files
- Indicators of compromise, hash sets, and fuzzy hashing
- Intermediate registry analysis
- Shadow volume/restore point examinations
- Super timeline analysis
- Finding unknown malware using memory, artifact, and file system analysis

Appendix C

IS 245 Course Syllabus

Approved by Department of Computer Science faculty, November 11, 2010

Approved by College of Science and Mathematics College Council, November 17, 2010

Southeast Missouri State University

Department of Computer Science Course No. IS 245
Title of Course: Web Development and Security Revision
New 11/2010

I. Catalog Description and Credit Hours of Course:
Advanced web page programming used to develop professional, secure web pages. Browser/server interaction, directory management, evaluation of web site impact on communication, understanding, and accessibility, web site security. (3)

II. Prerequisite (s): IS130 or CS155 or CS177 with a minimum grade of 'C' or permission of the instructor.

III. Purposes or Objectives of the Course:
Upon the successful completion of this course, the student will be able to:
A. Develop web pages that follow World Wide Web Consortium (W3C) recommendations using HTML/XHTML, CSS, and Javascript code.
B. Understand browser/server interaction and directory management.
C. Evaluate web site impact on communication, understanding, and accessibility.
D. Develop secure web sites.

IV. Expectations of Students:
A. Students are expected to successfully complete all assignments and pass all quizzes and tests.

V. Course Content or Outline (Indicate number of class hours per unit or section):

A.	Introduction to Web Development	1 hour
B.	Browser/Server Interaction	1 hour
C.	Website Directory Management	2 hours
D.	Editing, Testing and Validating Web Pages	1 hour
E.	Evaluating Website Impact on Communication, Understanding and Accessibility	2 hours
F.	Programming Web Page Content Using HTML/XHTML	10 hours
G.	Programming Web Page Format and Layout Using CSS	9 hours
H.	Programming Web Page Enhancements Using JavaScript	9 hours
I.	Building Secure Web Pages	10 hours
Total		**45 hours**

VI. Textbook(s) and/or Other Required Materials or Equipment:
A. Boehm, Anne. *Murach's HTML, XHTML, and CSS.* Mike Murach & Associates, Inc., 2010.

VII. Basis for Student Evaluation:

A.	Assignments	60%
B.	Tests	20%
C.	Quizzes	10%
D.	Final	10%