



TOPIC: Frostburg State University: Bachelor of Science in Secure Computing and Information Assurance

COMMITTEE: Education Policy

DATE OF COMMITTEE MEETING: March 28, 2012

SUMMARY: The proposed Bachelor of Science in Secure Computing and Information Assurance will augment current STEM programs and provide the student with an educational experience that is unique within the Western Maryland region. It will serve both the economic needs of the region and of the state of Maryland. This degree will address the recognized shortage of information security professionals in the region, the state, and the nation.

Earlier this month, the Governors of Maryland and West Virginia joined together to encourage the Navy to consolidate its information technology centers at Allegany Ballistics Laboratory (ABL) in the Eastern Panhandle of West Virginia, five minutes from Allegany County, Maryland. The advantages cited were proximity to Washington, D.C., the Navy owns ABL and maintains a significant presence there, and employee costs are lower than in the major metropolitan areas. The addition of a program in secure computing to FSU's other computer offerings can only enhance the chances for the success of this economic development effort.

The program also is primed to incorporate experiential education into the curriculum. The instructors of relevant courses have spent many years pursuing real-world experience as well as professional and academic credentials. The depth of the professional backgrounds of the instructors and their industry contacts will better prepare students for their futures as information assurance specialists, cyber forensics analysts, incident response experts, IT managers, corporate network managers, quality assurance specialists, and other cyber security and information assurance related careers.

The Secure Computing & Information Assurance degree will enhance Frostburg State University's computing specialization areas, attracting more students to the University. In turn, this will allow Frostburg State University to contribute a greater number of well-educated graduates toward filling the U.S. information assurance shortage.

ALTERNATIVE(S): The Regents may not approve the program or may request further information.

FISCAL IMPACT: No additional funding is necessary. The program will be supported through tuition and reallocated funds.

CHANCELLOR'S RECOMMENDATION: That the Committee on Education Policy recommend that the Board of Regents approve the proposal from Frostburg State University to offer the Bachelor of Science in Secure Computing and Information Assurance.

COMMITTEE RECOMMENDATION:

DATE:

BOARD ACTION:

DATE:

SUBMITTED BY: Irwin Goldstein (301) 445-1992 irv@usmd.edu



OFFICE OF THE PRESIDENT

JONATHAN C. GIBRALTER, PH.D.
101 BRADDOCK ROAD
FROSTBURG, MD 21532-2303
T 301.687.4111
F 301.687.7070

March 13, 2012

Dr. William E. Kirwan, Chancellor
University System of Maryland
3300 Metzerott Road
Adelphi, MD 20783-1690

Dear Dr. Kirwan:

Attached is a proposal for a Bachelor of Science in Secure Computing & Information Assurance to be offered by Frostburg State University beginning fall 2012. This program is FSU's response to the needs for the expansion of educational offerings and of the career pipeline identified by the Cyber Security Task Force that you chaired. We hope the presence of this program and its talented graduates will attract government agencies and private businesses with computer security concerns to Western Maryland. In fact, IBM recently opened a local office and is seeking security specialists.

And just last week, the Governors of Maryland and West Virginia joined together to encourage the Navy to consolidate its information technology centers at Allegany Ballistics Laboratory (ABL) in the Eastern Panhandle of West Virginia, five minutes from Allegany County, Maryland. The advantages cited were that this region is close to Washington, D.C., the Navy owns ABL and maintains a significant presence there, and employee costs are lower than in the major metropolitan areas. The addition of a program in secure computing to FSU's other computer offerings can only enhance the chances for the success of this economic development effort.

Please add consideration of this program to the agenda for the Board of Regents Educational Policy Committee meeting on March 28, 2012.

Sincerely,

A handwritten signature in black ink, appearing to read 'Jonathan C. Gibraltar', written in a cursive style.

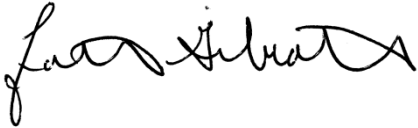
Jonathan C. Gibraltar
President

pc Stephen J. Simpson, Provost
Theresa Hollander, Associate Vice Chancellor for Academic Affairs
Joseph Hoffman, Dean, College of Liberal Arts and Sciences

UNIVERSITY SYSTEM OF MARYLAND INSTITUTION PROPOSAL FOR

X	New Instructional Program
	Substantial Expansion/Major Modification
	Cooperative Degree Program
X	Within Existing Resources (including tuition generated)

Frostburg State University
Institution Submitting Proposal
Bachelor of Science in Secure Computing and Information Assurance
Title of Proposed Program

Bachelor of Science		Fall 2012
Degree to be Awarded		Projected Implementation Date
070210		111003
Proposed HEGIS Code		Proposed CIP Code
Department of Computer Science and Information Technologies		Dr. Mary J. Gartner, Associate Provost
Department in which program will be located		Contact Name and Title
301.687.4284		mgartner@frostburg.edu
Contact Phone Number		Contact E-Mail Address
		March 13, 2012
Signature of President or Designee		Date

A. Mission

Describe how the program relates to the institution's approved mission.

Frostburg State University has provided paths to success for students for over 100 years. Founded in 1898 to prepare teachers, the institution today is a public, comprehensive, largely residential regional university offering a wide array of affordable programs at the undergraduate and graduate levels. The only four-year institution of the University System of Maryland west of the Baltimore-Washington corridor, the University serves as the premier educational and cultural center for western Maryland. At the same time, it draws its student population from all counties in Maryland, as well as from numerous other states and foreign countries, thereby creating a campus experience that prepares students to live and work in a culturally diverse world.

The role Frostburg State University plays in Western Maryland has never been more significant, and the future economic prosperity of the region depends on the University's growth and vitality. FSU is keenly aware of the importance of developing the highly educated and technologically competent workforce needed to meet the needs of today's knowledge economy. The University continues to develop and strengthen academic programs in response to the needs of businesses and industries in the region and the State. Major areas of undergraduate specialization are offered in education, business, science and technology (STEM) disciplines. The University is committed to continue to expand offerings in STEM-related fields through its partnerships and collaborations with community colleges, on-campus residential living programs, and new academic programming. Frostburg's membership in the Western Maryland Education Consortium (WestMEC), a network of universities, community colleges, county public school systems (Allegany, Garrett, and Washington), and economic development agencies, helps increase career readiness and workforce development in the region by promoting STEM education.

The University is a student-centered teaching and learning institution that emphasizes experiential education. Students are encouraged to apply and augment classroom learning through a wide range of experiential opportunities, including internships, volunteerism and leadership development activities, undergraduate research, and study abroad. <http://www.frostburg.edu/about/univ/missionstatement/>

The Bachelor of Science in Secure Computing & Information Assurance will augment current STEM programs and provide the student with an educational experience that is unique within the Western Maryland region. It will serve both the economic needs of the region and of the state of Maryland. This degree will address the recognized shortage of information security professionals in the region, the state, and the nation.

The program also is primed to incorporate experiential education into the curriculum. The instructors of relevant courses have spent many years pursuing real-world experience as well as professional and academic credentials. The depth of the professional backgrounds of the instructors and their industry contacts will better prepare students for their futures as information assurance specialists, cyber forensics analysts, incident response experts, IT managers, corporate network managers, quality assurance specialists, and other cyber security and information assurance related careers.

The Secure Computing & Information Assurance degree will enhance Frostburg State University's computing specialization areas, attracting more students to the University. In turn, this will allow Frostburg State University to contribute a greater number of well-educated graduates toward filling the U.S. information assurance shortage.

Need for the program, market demand, and employment statistics

The Department of Computer Science and Information Technologies has developed the Secure Computing & Information Assurance degree based on current and future market needs. Starting with a directive from the President of the United States, including the creation of the U.S. Cyber Command, many schools are beginning to develop a dedicated cyber security program. The B.S. in Secure Computing & Information Assurance at FSU will equip the successful student with the necessary theory and concepts to succeed in the field, while giving the practical experience necessary to quickly adapt to a potential employer.

Below are some of the factors that were considered during the development of this degree.

U.S. Bureau of Labor Projections

- The U.S. Bureau of labor predicts that computer specialists (in general) will continue to grow over the next 10 years with an eight percent change in the work force.
- “In addition, as cyber security becomes an increasingly important aspect of National defense, rapid growth will occur among information technology specialists, such as computer and information research scientists, who will be needed to devise defense methods, monitor computer networks, and execute security protocol.” <http://www.bls.gov/oco/cg/cgs041.htm>

Meeting the Needs of Maryland

- USM recently received a report from the Cyber Security Task Force (convened by Chancellor William E. Kirwan) which included several recommendations. FSU’s proposed program addresses the following recommendations:
 1. Enhance and extend educational offerings
(*This program will add a new B.S. degree to USM offerings and fill a much needed gap in technology education in Western Maryland.*)
 2. Strengthen research and support innovation and technology transfer in cyber security
 3. Expand the career pipeline
http://www.usmd.edu/newsroom/docs/USMCyberSecurity_final.pdf
- Jimmy DeButts from the *Baltimore Business Journal* reports that “in addition to the thousands of new cyber security jobs the state has seen sprout up in the past few years, another 15,000 cyber security positions could be added in the coming years.” This is due, in part, to the NAS and the new Cyber Command being located at Fort George G. Meade in Maryland.
<http://www.bizjournals.com/baltimore/print-edition/2011/11/18/protecting-marylands-cyber-security.html>

Industry Observations:

- “The U.S. government is currently on track to spend over \$79 billion for financial year 2011 on information security,” says Mike Meikle, CEO of the Hawthorne Group. “They are the largest customer for information security professionals at the present time.” Meikle maintains that the next greatest levels of need are within financial institutions and the utilities/energy sector.
<http://www.todaysengineer.org/2011/Aug/career-focus.asp>
- The Homeland Security Department has launched a number of programs this year designed to recruit, hire, train and retain a top-notch cyber security workforce.
http://wiredworkplace.nextgov.com/2011/06/dhs_seeks_cyber_pros.php
- The National Protection and Programs Directorate's [National Cyber Security Division \(NCSA\)](#) works collaboratively with federal, state and local governments; the private sector; academia; and international partners to secure the nation’s critical cyberspace and information technology

infrastructures through employing risk management and cyber incident preparedness, prevention, and response activities. To meet this cybersecurity mission, NCSD is looking for skilled individuals with experience in engineering, information security technology, computer science, and program and technical management. http://www.dhs.gov/xabout/careers/gc_1240512546017.shtm

- “Among the greatest concerns that impact both military and civilian realms is cybersecurity,” James G. Stavridis, Navy Adm., NATO’s supreme allied commander for Europe and commander of the U.S. European Command, told the Senate Armed Services Committee. “Today, we have a billion devices that are accessing the Internet,” he said. “Our economies are entangled in this Internet sea, and it’s an outlaw sea. Nothing exists in the norms of behavior. There is a military aspect to it, but it’s all of society. At some point, there needs to be a very global conversation on this challenge.”
- “Federal agencies have spent more on cyber security than the entire GDP of North Korea, who some have speculated is to be involved with some of these cyber attacks,” said Senator Thomas. L. Carper. “The issue of Cyber Warfare is not science fiction anymore. It’s reality.”
- With a cumulative market valued at \$55 billion (2010 – 2015), the U.S. Federal Cybersecurity market will grow steadily – at about 6.2% CAGR over the next six years. <http://www.marketresearchmedia.com/2009/05/25/us-federal-cybersecurity-market-forecast-2010-2015/>

Departmental Observations:

- There have been inquiries from students and parents about cyber security, computer security, network security, and information assurance at open house activities for the past several years. The development of this program addresses such requests from prospective students.
- With the success of the Information Technology degree, the department has a proven track record of growing a new program while maintaining student enrollment in established programs.
- Extensive research on other community colleges and university systems regionally and across the nation indicates a strong presence of cyber security degrees in many community colleges, but fewer dedicated degree programs at the university level. Further evidence of the lack of dedicated cyber security programs within the USM can be found in the “Report of the Cyber Security Task Force to the University System of Maryland.” UMUC does now offer baccalaureate and master’s programs and a number of specialized certificates.
- With the recent opening of a local office, IBM has indicated that they will be seeking security specialists in addition to individuals with SAP experience.

B. Characteristics of the Proposed Program

1. State the educational objectives of the proposed program.

Problem Solving and Critical Thinking. Solve problems by creating secure computing and information assurance environments, analyzing computing environments and implementing policies and practices to guarantee secure computing and information assurance environments. The student will be able to:

- Apply programming and system management techniques to address secure computing and information assurance problems.
- Perform critical analyses of the impacts of decisions.
- Participate in forensic analysis of hardware, software, and systems.

Communication and Interpersonal Skills. Use written, oral and electronic methods for effective communication. The student will be able to:

- Document all aspects of a system precisely and clearly.
- Document and communicate organizational secure computing and information assurance strategies, practices and policies.
- Use written, oral, and electronic communication to convey technical information effectively.
- Work cooperatively in teams and with others.

Ethical and Professional Responsibilities. Discern and articulate the impact of secure computing and information assurance on society. The student will be able to:

- Determine the economic and organizational effects of secure computing and information assurance on global society.
- Recognize important legal issues and demonstrate appropriate social responsibilities in secure computing and information assurance.
- Demonstrate an awareness of the codes of professional ethics in secure computing and information assurance.
- Plan for and ensure the security, privacy, and integrity of data.
- Recognize the need for continuing professional development.

2. Provide a brief narrative that addresses the adequacy of curriculum design and related learning outcomes. (See detailed instructions for REQUIRED content.)

As the discipline of computer science expands, so must our curriculum. It has been brought to the department's attention (by various sources at the University, state, and federal levels) that we need to match the growing needs of the "real world" with a degree in Secure Computing & Information Assurance at Frostburg State University. To answer this call, we have investigated similar programs throughout the University System of Maryland, Carnegie Mellon University, and other U.S. institutions and programs. Further, we have developed the Secure Computing & Information Assurance degree around ABET (Accreditation Board for Engineering and Technology) accreditation recommendations and have used ACM (Association for Computing Machinery) curricula as a framework for degree requirements. Secure Computing & Information Assurance is a new and unique major that must be differentiated from the Bachelor of Science in Computer Science.

We have developed new core, advanced, and elective courses to challenge our students and meet industry requirements. (See course descriptions appended to this proposal.) The curriculum development process will ensure that our students are prepared for productive interaction with other information assurance professionals who have graduated from similar information assurance programs.

To assess the student's synthesized knowledge of the content taught in the program, the student must take a capstone course during the last semester of her career at Frostburg State University. The capstone course will allow the student to demonstrate her understanding of the material by creating and maintaining a portfolio and successfully completing a degree exit exam. Upon completion of all course work with a grade of 'C' or better, the student will have completed a rigorous program; thus ensuring that the student has the confidence, skill set, and knowledge of an established information assurance professional. Finally, this program will equip the successful graduate with the proper qualifications to enable her to obtain a job in computing security, information assurance, cyber security, or a related field in any sector of business, government, or education. Surveys of graduates and their employers will measure the extent to which learning outcomes have been realized, and, as required, lead to revision of objectives and desired outcomes as the field changes and matures.

Requirements for Major in Secure Computing & Information Assurance

- You must earn a grade of C or better in all computer science, information technology, and secure computing courses to be applied towards major or minor requirements.
- You may receive credit by examination for the following courses: COSC 100, 101, 240.

1. Core Courses (25 hours):

COSC 101	The Discipline of Computer Science
SCIA 103	Foundations of Secure Computing and Information Assurance
SCIA 120	Introduction to Secure Computing and Information Assurance
SCIA 210	Introduction to Cyber Law
COSC 240	Computer Science I
COSC 241	Computer Science II
SCIA 340	Secure Databases
SCIA 489	Capstone Course

2. Required Advanced Courses (27 hours):

COSC 331	Fundamentals of Computer Networks
SCIA 325	Software Security Engineering
SCIA 335	Network Security
SCIA 360	Operating System Security
SCIA 370	Security Policy and Assessment
SCIA 460	Cloud Computing and Security
SCIA 470	Computer and Network Forensics I
SCIA 471	Computer and Network Forensics II
SCIA 472	Hacking Exposed and Incident Response

3. Other Required Courses (12-13 hours):

CMST 102/112	Introduction to Human Communication
ENGL 338	Technical Writing (<i>Core Skill 2</i>)
MATH 209/219	Elements of Applied Probability & Statistics (<i>Core Skill 3</i>)
or MATH 380	Intro. To Probability & Statistics
MATH 220	Calculus for Applications I
or MATH 236	Calculus I (<i>Core Skill 3</i>)

4. Electives (9 hours):

A minimum of 9 hours in at least three courses:

COSC 305	Computer Ethics
ITEC 442	Electronic Commerce
SCIA 425	Software Testing and Assurance
SCIA 435	Access Control
SCIA 480	Applied Cryptography
SCIA 485	Emerging Issues and Cyber Warfare
SCIA 491	Seminar in Secure Computing and Information Assurance
SCIA 494	Field Experience in Secure Computing and Information Assurance
SCIA 499	Individual Problems in Secure Computing and Information Assurance

Requirements for Minor in Secure Computing & Information Assurance

COSC 101	The Discipline of Computer Science
SCIA 103	Foundations of Secure Computing and Information Assurance
SCIA 120	Introduction to Secure Computing and Information Assurance
COSC 240	Computer Science I
SCIA 370	Security Policy and Assessment
<i>One additional Secure Computing & Information Assurance course at the 300 -level or above</i>	

3. Provide a brief narrative that addresses the demonstrable quality of program faculty.

Many courses in the Secure Computing & Information Assurance program can be taught by current faculty members in the Department of Computer Science and Information Technologies. However, because of the increase in course load, we do expect to hire four new faculty members (one each in years two (2013), three (2014), four (2015), and five (2016) for the new degree. In general, the department will seek individuals with expertise and experience in secure computing and information assurance in industry and in government. Specific areas of expertise sought include network security, policy and assessment, computer and network forensics, cloud computing, operating system security, database security, information security law and software engineering security. The following are current faculty members who are qualified to teach some of the courses for the Secure Computing & Information Assurance degree:

H. Amthauer, Ph.D. (Computer Science, University of Kansas, 2008)
M. Chitsaz, Ph.D.; M. S. (Agronomy, with minor in Statistics, North Dakota State University, 1983; Computer Science, Morehead State University, 1986)
M. Flinn, D.Sc. (Information Systems and Communications, Robert Morris, 2009)
B. Rinard, Ph.D. (Computer Science, West Virginia University, 1997)
B. Wentz, D.Sc. (Information Technology, Towson University, 2010)
W. Xu, Ph.D. (Information Technology, University of North Carolina, Charlotte, 2010)
X. Zheng, Ph.D. (Computer Science & Engineering, University of South Carolina, Columbia, 2007)

4. Describe the student audience to be served by the program; include enrollment estimates.

The program's intended audience is a student who desires a broad background in Secure Computing & Information Assurance. We expect the program to attract six new full-time students during the first year in addition to any students who might be transferring from other programs. As the program becomes better known and the need for secure computing and information assurance specialists continues to increase, it is expected that the number of new students will increase by an additional 12-13 full-time students each year for the next several years. We are projecting 18 full-time students in year two; an additional 12 students in year three (total = 30 full-time); and an additional 15 full-time students in year four (total = 45). At that time, we estimate that there will continue to be in excess of 60 new full-time students in the program from year five on. This estimate is based upon interest shown at open houses, market demand and employment forecasts as presented in the "need for the program" section of this document.

5. Describe the manner in which this program will enhance students' technology fluency.

The Secure Computing & Information Assurance program will support all of the Secure Computing & Information Assurance learning goals. By its very nature, graduates of this program will be fluent in current security technologies and have the corresponding skills required to be successful in technical security careers.

6. Assure that library resources are adequate by including the following statement:

The president assures that institutional library resources meet new program needs.

Since FSU is part of the University System of Maryland, we have access to many of the most widely used computer science resources over the Internet in addition to FSU's own collection and database subscriptions.

7. Assure that facilities are adequate by including the following statement:

The president assures that institutional facilities meet new program needs.

As of fall 2012, the Department of Computer Science and Information Technologies has the fundamental facilities to start a new Secure Computing & Information Assurance degree. Our department has access to six computer labs located in Pullen Hall that are shared across the campus. We have three computer labs—two programming labs and one networking lab—that are dedicated for use by our department. More specifically, all the Pullen Hall labs and programming labs are configured with virtual machines, which can support running multiple operation systems and emulating a small scale computer network. Students can explore concepts learned in the classroom and practice using different kinds of information security and forensics software. The networking lab has 20 powerful Intel workstations. Each machine has an eight-core processor and 8GB main memory and is capable of running multiple operation systems simultaneously and emulating a small-scale computer network. More complex security hands-on activities can also be performed on this computer network. All of these labs are equipped with a digital projector for in-lab presentations. In addition an AIX server is also available.

Besides having access to these computer labs, we belong to MSDN-AA (Microsoft Developers Network—Academic Alliance) as well as the Oracle Academic Alliance. These memberships allow the department to supply all necessary software to our students free of charge. In addition, they also equip the labs with state-of-the-art software that can be used in research and project development. All other necessary software materials for this lab are available at no charge through the OSS (Open Source Software) community. The availability of these resources enables us to train and adequately prepare students with industry-relevant information technology skills to meet the demands of the marketplace.

Finally, the Department of Computer Science and Information Technologies will move to a new, state-of-the-art building, the Center for Communications and Information Technology, in 2014 (estimated). In the new building, the department will have more facilities—such as classrooms, computer labs, research facilities, and meeting rooms to support the needs of the new Secure Computing & Information Assurance degree.

Table 1: Resources (Narrative)

1. Reallocated Funds

The program can be offered with current resources, with reallocation of the course load for current faculty in years one, two, and three. Reallocation will be accomplished two ways: courses that are taught on a variable schedule may not be offered as frequently during the reallocation, and course size will be increased temporarily from 20 to 24. There are no foreseeable consequences for the other programs in the department. Should issues arise, they may be addressed with summer offerings or independent studies.

It is anticipated that the Secure Computing & Information Assurance program will require .25 of a faculty position in the first year, with each of the six new students taking two courses in addition to any current students switching to the Secure Computing & Information Assurance program. The reallocation will continue in years two and three to supplement the efforts of two additional faculty members, one new faculty member hired in each of year two (2013) and year three (2014) of the program. During years four (2015) and five (2016) of the program, two additional faculty will be hired, one each year, enabling the department to assign reallocated time to other department needs. The average cost of a current faculty member is \$70,000 salary and fringe benefits of \$23,100 (33% of salary).

2. Tuition and Fee Revenue

Tuition and fee revenue includes only payments by new students who will be attracted to FSU because of this program. As previously noted, we anticipate 10 - 15 new full-time students and two to four part-time students will choose FSU each year, in addition to students who transfer from the other programs. It is further assumed that a part-time student will take two courses per semester for a total of 12 credit hours per year.

3. Grants, Contracts, and Other External Sources

N/A

4. Other Sources

N/A

TABLE 1: RESOURCES					
Resources Categories	2012	2013	2014	2015	2016
1. Reallocated Funds	23,275	23,275	23,275		
2. Tuition/Fee Revenue (c+g below)	50,472	147,564	244,656	366,984	489,312
a. #F.T Students	6	18	30	45	60
b. Annual Tuition/Fee Rate	7,128	7,128	7,128	7,128	7,128
c. Annual Full Time Revenue (a x b)	42,768	128,304	213,840	320,760	427,680
d. # Part Time Students	2	5	8	12	16
e. Credit Hour Rate 219+89+13	321	321	321	321	321
f. Annual Credit Hours	12	12	12	12	12
g. Total Part Time Revenue (d x e x f)	7,704	19,260	30,816	46,224	61,632
3. Grants, Contracts, & Other External Sources	0	0	0	0	0
4. Other Sources	0	0	0	0	0
TOTAL (Add 1 – 4)	73,747	170,839	267,931	366,984	489,312

Table 2: Expenditures (Narrative)

1. New Faculty (# FTE, Salary, and Benefits)

It is anticipated that the Secure Computing & Information Assurance program will require hiring a total of four new faculty members with expertise in cyber security, information assurance, and secure computing, one each in years two, three, four, and five. Estimated costs are based on current average costs of \$70,000 in salary with fringe benefits of \$23,100 (33% of the salary).

2. New Administrative Staff (# FTE, Salary, and Benefits)

The addition of the Secure Computing & Information Assurance program will place a strain on the department chair. To mitigate the strain, a program coordinator will be assigned to each program in the department. Program coordinators will be slowly integrated into the department's leadership structure according to the following schedule: ITEC - year 1, CS – Year 2, CIS- Year 3, SCIA – Year 4. An estimated stipend of \$3,000 per year will be paid to each program coordinator.

3. New Support Staff (# FTE, Salary, and Benefits)

None anticipated at this time.

4. Equipment

As this is a new and cutting edge field, some new equipment, primarily in the form of software, will be necessary. The following is a preliminary list of materials for various classes to be offered in the program:

- T4 Forensic SCSI Bridge (USB Interface): Used for blocking writing to the hard disk. Price: \$399 (Quantity 10)
- Mobile Device Reader: Used for reading SIM card information. Price: \$179.50 (Qty 10)
- EnCase Forensics V7: \$2995

5. Library

No additional costs anticipated at this time beyond regular department allocations.

6. New and/or Renovated Space

No additional space is required beyond what is already planned in the new technology building.

7. Other Expenses

None anticipated at this time.

TABLE 2: EXPENDITURES					
Expenditure Categories	Year 1	Year 2	Year 3	Year 4	Year 5
1. Total Faculty Expenses (b + c below)	0	93,100	186,200	279,300	372,400
a. # FTE	0	1	2	3	4
b. Total Salary	0	70,000	140,000	210,000	280,000
c. Total Benefits	0	23,100	46,200	69,300	92,400
2. Total Administrative Staff Expenses (b + c below)	3,255	6,510	9,765	13,020	13,020
a. # FTE	NA	NA	NA	NA	NA
b. Total Salary	3,000	6,000	9,000	12,000	12,000
c. Total Benefits	255	510	765	1,020	1,020
3. Total Support Staff Expenses (b + c below)					
a. # FTE					
b. Total Salary					
c. Total Benefits					
4. Equipment		8,780			
5. Library	0	0	0	0	0
6. New or Renovated Space	0	0	0	0	0
7. Other Expenses	0	0	0	0	0
TOTAL (Add 1 – 7)	3,255	108,390	195,965	292,320	385,420

New Course Descriptions

SCIA 103 Foundations of Secure Computing and Information Assurance **4 cr.**

Introduction to the foundations of secure computing and information assurance. Computer functions, digital logic circuits, correctness of algorithms, O-notation and efficiency of algorithms. Introductory mathematical material from such fields as probability theory, computational theory, complexity theory, group theory, information theory, graph theory and number theory. Three hrs. lecture, 2 hrs. lab. Every semester. *Prerequisite: Level III or above on mathematics placement test, or a Level II mathematics course.*

SCIA 120 Introduction to Secure Computing & Information Assurance **3 cr.**

Broad overview of computing security. Importance of securing digital information, operating systems security, secure programming, and secure digital communications. Physical security, social engineering, operating systems security, malware, network security, Internet security, cryptography, security models and practices, distributed-applications security, and cloud computing security. Every semester.

SCIA 210 Introduction to Cyber Law **3 cr.**

Overview of federal and state laws that impact computer security, information assurance, and other aspects of security. Examines how laws have adapted and/or been implemented in relationship to the digital age and living in an online society. Computer crimes, identity theft, sexual harassment, intellectual property, plagiarism, cyber stalking, medical issues, and financial concerns. Torts, liability, securities, antitrust laws, bankruptcy, and hiring/termination. Every semester.

SCIA 325 Software Security Engineering **3 cr.** Overview of existing processes, standards, life-cycle models, frameworks, and methodologies that support secure software development. Properties of secure software, requirements engineering, architecture and design, construction and testing, system integration/assembly, and governance and management. Threat modeling, defensive programming, web security and human-computer interaction issues that affect security. Variable. *Prerequisites: Grade of C or better in COSC 241 and SCIA 120.*

SCIA 335 Network Security **3 cr.** Cryptography basics for network security, network- related authentication applications, Email security, IP security, web security, network management security, intruders and malicious software, IDSs and firewalls. Variable. *Prerequisites: Grade of C or better in COSC331 and SCIA 120.*

SCIA 340 Secure Databases **3 cr.** Securing data and information, monitoring communications and auditing database environments. RDBMS, SQL, database communications, database authentication, access control in databases, encryption in databases, database auditing, and databases in the cloud. *Prerequisites: Grade of C or better in COSC 240 and SCIA 120.*

SCIA 360 Operating System Security **3 cr.** Fundamental principles of operating systems and operational security, including process and resource management, security capabilities and limitations, authentication, security policies, sandbox, software vulnerabilities, and virtualization. Case studies of operating systems. *Prerequisites: Grade of C or better in COSC 241 and SCIA 120.*

SCIA 370 Security Policy and Assessment **3 cr.** Information security concepts, security risk management processes, information security lifecycle, security planning and policy, business continuity planning, security assessment and system availability, security review and security audit, security standards. Variable. *Prerequisite: Grade of C or better in SCIA 120.*

SCIA 425 Software Testing and Assurance**3 cr.**

Survey of quality processes and technologies for software development to assure that new software provides sufficient security for the threat environment and functions in the intended manner. Quality and security requirements and specifications; quality in architecture, design, and construction; correctness verification, inspection, and testing techniques; process and product assurance; statistical quality control; and quality management. Variable. *Prerequisite: Grade of C or better in SCIA 325.*

SCIA 435 Access Control**3 cr.** Access

control objectives, formal models and mechanisms, access control of commercial off-the-shelf systems, and security architecture for authorization. Implementation of access control in current systems. Variable. *Prerequisite: Grade of C or better in SCIA 335.*

SCIA 460 Cloud Computing and Security**3 cr.**

Cloud computing basic concepts, architecture, and framework; current popular cloud computing technologies; security challenges and risk facing in cloud computing; concepts, methods, procedures and tools for assuring security in cloud computing. Variable. *Prerequisite: Grade of C or better in SCIA 335.*

SCIA 470 Computer and Network Forensics I**3 cr.**

Forensic tools, methods, and procedures used for investigation of computers; techniques of data recovery and evidence collection, protection of evidence, expert witness skills, and computer crime investigation techniques. Analysis of various file systems and specialized diagnostic software used to retrieve data. Variable. *Prerequisites: Grade of C or better in SCIA 210 and SCIA360.*

SCIA 471 Computer and Network Forensics II**3 cr.**

Forensic methodology, procedures and tools associated with different kinds of cybercrime in a network environment. Importance of network forensic principles, legal considerations, digital evidence controls, and documentation of forensic procedures. *Prerequisite: Grade of C or better in SCIA 470.*

SCIA 472 Hacking Exposed and Incident Response**3 cr.**

Common network attacks, applications of information security concepts, hands-on security assessments of wired and wireless networks, web applications and intrusions, countermeasures to attacks, lifecycle of incident response, real world case studies. Variable. *Prerequisite: Grade of C or better in SCIA 471.*

SCIA 480 Applied Cryptography**3 cr.**

Basics of design of secret codes for secure communication, including encryption and integrity verification: ciphers, cryptographic hashing, and public key cryptosystems, mathematical principles underlying encryption, cryptanalysis concepts, and cryptographic protocols. Variable. *Prerequisite: Grade of C or better in SCIA 335.*

SCIA 485 Emerging Issues and Cyber Warfare**3 cr.**

Current issues, trends and challenges in information warfare; high-level analysis of information warfare threats, such as cyber terrorism, espionage, Internet fraud; intelligence activities, cyber ethics, and law enforcement. Variable. *Prerequisite: Grade of C or better in SCIA 335.*

SCIA 489 Capstone**1 cr.** Creation of

professional vita and a portfolio consisting of student's best examples of programs, projects, and research papers. Integration of curricular concepts into a unified entirety. Administration of degree exit exam. Every semester. *Prerequisites: Senior standing, completion of all core courses and a grade of C or better in at least two required advanced courses.*

SCIA 491 Seminar in Secure Computing & Information Assurance**1-6 cr.**

Group study of advanced topics under faculty supervision; repeatable for maximum of 6 credits if topics are substantially different; up to 3 credits count towards major or minor in Secure Computing & Information Assurance. Variable.

Prerequisites: Grade of C or better in core courses and written permission of faculty supervisor. DEPARTMENT APPROVAL REQUIRED PRIOR TO REGISTERING.

SCIA 494 Field Experience in Secure Computing & Information Assurance **3 cr.**

Work experience in industry, government, or small business providing an opportunity for practical application of academic training in Secure Computing & Information Assurance. The course requirements are: (1) Minimum of 90 hours of field experience; (2) A written report describing in detail the work performed in the field in conjunction with an oral presentation to interested faculty and students; (3) A project paper on a topic related to the work experience. Previous work experience may not be substituted for this course. Repeatable for maximum of 6 credits if placement sites are different; no more than 3 credits count towards major in Secure Computing & Information Assurance. Every semester. *Prerequisites: Junior or senior standing and completion of the core courses in Secure Computing & Information Assurance with a grade of C or better. DEPARTMENT APPROVAL REQUIRED PRIOR TO REGISTERING.*

SCIA 499 Individual Problems in Secure Computing & Information Assurance **1-6 cr.**

Individual advanced topics under faculty supervision. Repeatable for maximum of 6 credits; up to 3 credits can apply to major or minor in Secure Computing & Information Assurance. Students must submit a written proposal to faculty supervisor and department describing topics, time allocation and limitation, objectives, assignment, and projects. Variable. *Prerequisites: Grade of C or better in core courses and written permission of faculty supervisor. DEPARTMENT APPROVAL REQUIRED PRIOR TO REGISTERING.*