UTAH SYSTEM OF HIGHER EDUCATION
Building a Stronger State of Minds

State Board of Regents
Board of Regents Building, The Gateway
60 South 400 West
Salt Lake City, Utah 84101-1284

Phone 801.321.7101
Fax 801.321.7199
TDD 801.321.7130
www.higheredutah.org

July 22, 2015

MEMORANDUM

TO: State Board of Regents

FROM: David L. Buhler

SUBJECT: Southern Utah University – Master of Science in Cyber Security and Information Assurance

Issue

Southern Utah University (SUU) requests approval to offer a new Master of Science in Cyber Security and Information Assurance effective Fall Semester 2015. The proposed program was approved by the SUU Board of Trustees on December 5, 2014.

Background

The proposed Master of Science in Cyber Security and Information Assurance is designed to be offered entirely online. Students will not be place-bound and the institution intends to draw students from broad geographical locations. The program focuses on the design, planning and management of systems and procedures for protecting cyber infrastructure from external threats, including terrorism. The program includes instruction in security and cyber infrastructure, policy, information, vulnerability, threat assessment, contingency, redundancy, emergency, and disaster planning, as well as physical, personnel, and operational security.

Local, regional, and national law enforcement agencies are working to improve response capabilities to cybercrime. Likewise, protection against cyber threats is essential to ensure the security of digital information, including public, private, and personal information. The ability to manage cyber infrastructure enables professionals to address many of these information security challenges. Southern Utah University seeks to provide professionals with the appropriate skills to respond to this pressing industry need. The institution plans to seek accreditation through the Accreditation Board for Engineering and Technology (ABET) for the program.

According to the U.S. Bureau of Labor Statistics (BLS), those who work in information security will see rapid job growth and greater demand for skilled technicians at a 10 year total projected growth rate of 37%. The BLS reported a 2012 median hourly wage of $41.43.

Graduate degrees in fields relating to information security are increasing for executive and management

level positions and can complement information technology certifications like CISSP (Certified Information Systems Security Professional) and CISM (Certified Information Security Manager).
The program was reviewed by legal counsel at the Utah State Attorney General's office to assess whether or not SUU should be required to implement criminal background checks prior to admission into the proposed program. Based on feedback from counsel, it is understood by staff that there is no federal or state statute that requires or prohibits SUU from conducting background checks as part of its admissions policy. This would be a policy decision. If the institution were to implement such a policy, the selectiveness of the process must not be arbitrary or capricious and it must not discriminate against protected classes. That being said, it should be noted that SUU could face lawsuits from students or third parties whether or not it conducts criminal background checks. A student applicant may claim that he/she was improperly denied admission as a result of a background check. On the other hand, an injured third party may claim that SUU was negligent in admitting a dangerous student if a background check is not implemented (or implemented and not followed). Although few courts have addressed the issue of requiring background checks, courts have generally ruled in favor of those colleges and universities that followed policies that are in compliance with federal laws.

Southern Utah University has suggested a solution that would not require background checks but would require screening of applicants to include the following items as well as meeting all other requirements for admission to SUU graduate programs:

- Written letter of intent
- Three letters of recommendation
- Completion of baccalaureate degree in computer science, information systems, computer programming, or related degree
- Depth of related professional experience

International students would be required to submit the following:

- Demonstrated proficiency in English
- Documentation of current residency status
- Proof of identity

A complete statement of admissions criteria was provided by SUU and is included within the body of the proposal.

In addition to legal review regarding background checks, the Commissioner's office contacted the Utah System of Higher Education (USHE) Chief Information Officer (CIO) with a request to review the program and provide guidance relative to IT security issues. This review yielded the following two recommendations that SUU:

1. Conduct an independent penetration test on SUU's student IT system.
2. Conduct an annual risk analysis on the student IT system.

Southern Utah University has committed to adhere to these two recommendations.

Policy Issues

The proposed program has been developed through established institutional procedures and Board of Regents policy. Chief academic officers as well as faculty in related departments from the Utah System of Higher Education institutions have reviewed the proposal and have provided input. There are no additional policy issues that need to be addressed relative to approval of the program.

Commissioner's Recommendation

The Commissioner recommends the Board of Regents approve the Master of Science in Cyber Security and Information Assurance to move to the full Board for approval with recommendation that Southern Utah University: 1) coordinate with USHE's Chief Information Officer, or his designee, to develop and implement the graduate student IT system; 2) conduct an independent penetration test on the student IT system prior to enrolling students in the program; 3) conduct annual risk analyses on the student IT system; and 4) provide a status report of the program to the Board of Regents' Academic and Student Affairs Committee during the November, 2017 meeting (following the first year of program implementation) that provides an accounting of enrollments, risk analysis, results of the IT penetration test, assessment of the student admissions process, future direction for the program, and overall strengths and opportunities for improvement of the program.

_____
David L. Buhler
Commissioner of Higher Education

DLB/BKC
Attachment

Program Description – Full Template
Southern Utah University
Master of Science in Cyber Security and Information Assurance (online)

Section I: The Request

Southern Utah University (SUU) requests approval to offer an online Master of Science in Cyber Security and Information Assurance (CSIA) effective Fall Semester, 2016. This proposed program would be administered by SUU's Department of Computer Science and Information Systems (CSIS). The proposal for the program received approved by the SUU Board of Trustees on December 4, 2013. That proposal was revised and the revised proposal (included herein) received approval from the SUU Board of Trustees on December 5, 2014.

Section II: Program Description

Complete Program Description

The proposed Master of Science in Cyber Security and Information Assurance program focuses on the design, planning and management of systems and procedures for protecting cyber systems and infrastructure from external threats, including terrorism. The program will be delivered online and includes instruction in: 1) cyber security and IT policy; 2) information, vulnerability, and threat assessment; 3) physical, personnel, and operational security; and 4) contingency, redundancy, emergency, and disaster planning.

Purpose of Degree

Cyber Security and Information Assurance are areas of growing concern in the nation and in the world. Local, regional, and national law enforcement agencies are currently trying to improve their response capabilities to cybercrime. Likewise, protection of cyber infrastructure against such threats is essential to ensure the security of digital information, including public, private, and personal information. The ability to manage cyber infrastructure enables professionals to address many of these information security challenges, and by offering a Master's of Science degree in Cyber Security and Information Assurance, SUU will be able to provide professionals with the appropriate skills to respond to a growing industry need. In addition to addressing industry need for these types of professionals, there currently is no master's level offering of a degree like this in the Utah System of Higher Education. Due to the market demand for these professionals, graduates of the proposed program will have many doors opened to them in both private industry and government sectors.

Institutional Readiness

Six CSIS faculty members are already qualified to teach graduate courses for the proposed program. As the program grows, additional full-time faculty will be added as demand warrants. The Department Chair and faculty members will work with SUU student support systems and the Dean of Graduate Studies to provide orientation of the program, its admissions criterion, and markets for recruitment.

Departmental Faculty

Department Faculty Category	Department Faculty Headcount – Prior to Program Implementation	Faculty Additions to Support Program	Department Faculty Headcount at Full Program Implementation
With Doctoral Degrees (Including MFA and other terminal degrees, as specified by the institution)			
Full-time Tenured	6		6
Full-time Non-Tenured	2	2	4
Part-time Tenured			
Part-time Non-Tenured			
With Master's Degrees			
Full-time Tenured	1		1
Full-time Non-Tenured	2		2
Part-time Tenured			
Part-time Non-Tenured			
With Bachelor's Degrees			
Full-time Tenured			
Full-time Non-Tenured			
Part-time Tenured			
Part-time Non-Tenured			
Other			
Full-time Tenured			
Full-time Non-Tenured			
Part-time Tenured			
Part-time Non-Tenured			
Total Headcount Faculty in the Department			
Full-time Tenured	7		7
Full-time Non-Tenured	4		6
Part-time Tenured			
Part-time Non-Tenured			
Total Department Faculty FTE (As reported in the most recent A-1/S-11 Institutional Cost Study for "prior to program implementation" and using the A-1/S-11 Cost Study Definition for the projected "at full program implementation.")	11	2	13

Staff

The proposed program requires one part-time administrative assistant who will work on managing the secretarial, clerical, and administrative needs of the program. This could develop into a full-time position as the program grows. Academically qualified instructors from the information technology industry will be utilized as needed.

Library and Information Resources

Current library and online resources (including both online databases and current holdings) are sufficient to support success of the program. There are currently 62 items listed in the SUU holdings related specifically to Cyber Security and SUU is able to access additional electronic resources including the *International Journal on Cyber Security and Digital Forensics*.

Admission Requirements

All students applying to the proposed Cyber Security program must meet all of the requirements for graduate admissions at SUU, including:

1. An earned bachelor's degree from an accredited institution
2. Copies of official transcripts from all previous institutions attended
3. Minimum 3.0 GPA for the last 60 credits of undergraduate coursework
4. Official copy of a recent GRE score
5. Application fee
6. Letter of intent
7. Three letters of recommendation

The letter of intent must include a detailed description of the applicant's academic background, relevant work experience, career goals, and desired emphasis area (cyber and web security *or* government regulation and compliance).

The three letters of recommendation must be from current or recent employers, faculty mentors, or other professionals in the field who can attest to the student's academic preparation and promise, as well as the student's character.

Southern Utah University will screen applicants (using the admissions requirements noted above) to ensure students will be successful in the proposed program (i.e., to ensure that they are reasonably well prepared to achieve success in the program, to contribute meaningfully to the learning environment, and to participate in group work and related activities). The institution will accomplish this by looking for one or both of the following:

> Academic Preparation -- prior baccalaureate degree in computer science, information systems, computer programming, or related degree. This academic preparation provides some assurance that students entering the program will be successful, and that they will be capable of developing the knowledge, skills, and dispositions to complete the requirements and compete for professional employment.

Professional Experience -- some applicants may have significant professional experience that will lead to success in the program. Even if they might not have the typical academic preparation in computer science, the institution recognizes that applicants with professional experience and on-the-job training would also be successful in the program. In this way, professional experience can provide assurance that students entering the program will be successful, and that they are capable of working hard, that they are mature, and motivated by real-world desires to advance their careers.

Faculty members from the CSIS Department will screen all complete applications received by the deadlines established by the institution. Admission to the program is selective and cohort-based, and therefore not all students who apply will be admitted. Employment history (including current employment) will be confirmed directly with employers and supervisors. Likewise, those writing letters of recommendation will be contacted directly to verify the academic aptitude of the applicant.

International students will have a separate application process. In addition to all of the above admissions requirements (including directly confirming details of their employment history and personally contacting the people who have written letters of recommendation), international applicants must also provide documentation regarding minimum English proficiency (TOEFL score of 550 for paper-based test, a score of 213 on the computer-based test, or a score of 79 on the internet-based test), documentation related to current residency status, and proof of identity (current passport with photo). International students who do not hold the required degree from an accredited institution in the United States must submit translated transcripts along with a letter from a qualified foreign transcript evaluation service certifying equivalency to a degree meeting standards of higher education institutions in the United States.

It is anticipated the program will attract undergraduate students seeking to further their education in Cyber Security and Information Assurance at the graduate level and professionals in the information security field seeking to obtain an advanced degree to further their career and advance to higher-level positions.

Students who do not have an IT background or related degree will be handled on a case-by-case basis. Additional coursework may be required before formal admission to the program is granted.

Given the nature of this program and the prevalence of cybercrimes, SUU will require students admitted to this program to sign and adhere to “White Hat” agreements where appropriate in the curriculum. The term “White Hat” is an industry-specific term that refers to a strict professional code of conduct (overarching ethical framework) and is used in contexts when the work involves identifying security vulnerabilities. Adherence to these White Hat agreements will be essential especially in courses that provide the tools that could be used to gain access to sensitive information, such as those in the field of penetration (or “pen”) testing. In these cases, students will be provided with clear expectations regarding ethical and responsible conduct and will be required to adhere to White Hat professional standards. Violation of such White Hat agreements will be grounds for dismissal from the program. (A sample White Hat agreement is provided as an attachment to the end of this proposal.) Finally, SUU will develop ways to regulate the sharing of intellectual property with individuals residing outside of the United States in accordance with United States export control laws. Similar to White Hat agreements, students in the program will sign and adhere to these rules.

Student Advisement

Students will be advised by the CSIS Department faculty members and the Department Chair.

Justification for Graduation Standards and Number of Credits

This program will require 33 credit hours. This falls within the expected number of credits required for master degree programs.

External Review and Accreditation

Future plans for accreditation include the designation from the National Security Agency (NSA) for a Center of Academic Excellence in Information Assurance and Cyber-Defense (CAE-IA/CD). That designation includes standards regarding knowledge units the program must deliver and a site visit by an evaluation team. It is projected that SUU would have a site visit no earlier than 18 months from the time of application, as that is the timeframe given by NSA. Application for this designation is projected to be submitted during the second year of the program (Fall 2017 or Spring 2018).

The Accreditation Board for Engineering and Technology (ABET) currently accredits SUU's undergraduate programs in CSIS and would be petitioned to accredit the proposed online Master's degree. The ABET accreditation process requires that the program have at least one graduating class. Therefore, accreditation will be sought after the third year of the program. Within ABET, several accrediting Commissions exist to serve different educational programs. A determination will be made as to which ABET Commission will be used to accredit the proposed graduate program. The Commission that accredits the CSIS undergraduate programs (the Computing Accreditation Commission) does not list Master level programs; however, the Applied Science Accreditation Commission (ASAC) does list Master level programs. Further discussions have been initiated with ABET to clarify which Commission will be used to seek accreditation for the proposed graduate program.

The program will host a Program Advisory Committee (PAC) that will include CSIS faculty as well as experts from the security industry, and members from CSIS's Industrial Advisory Board (which includes many local employers in Southern Utah). The PAC will ensure that course content and curriculum design is in accordance with Utah, CAE-IA/CD, and ABET Educational Standards and will work with program faculty to maintain currency of program content.

Program courses will adhere to the quality standards consistent with SUU's other graduate programs. The same requirements associated with current SUU graduate degrees, as well as the tools and support used to create and ensure quality for their delivery, will be applied to support this program. The tools and support for these programs include an instructional technology team that provides best practices for online delivery of courses.

Faculty developing the courses will have the opportunity to participate in structured curriculum development workshops offered by SUU Online (http://suu.edu/scps/distance). Likewise, when using the online course management system (Canvas), SUU faculty and students will be supported through the SUU Help Center (https://help.suu.edu/suuonline) as well as the faculty and student resources page (http://suu.edu/scps/distance/resources.html).

When the individual courses were identified for the program, research and evaluation of other similar graduate level programs was conducted. It was determined that the courses that will be offered are in line with other programs across the state and the nation. Additionally, discussions with graduate faculty at other

USHE institutions indicate that these courses are appropriate to the subject matter of such a degree, and complementary to (and build upon) other existing programs. All faculty teaching in this program have terminal degrees (Ph.D.) and have experience teaching at the graduate level.

Ongoing quality and rigor will be maintained in accordance with existing department processes and reviews. For example, the CSIS Department currently maintains ABET accredited undergraduate programs and is therefore required to have formal review structures in place. These same review structures will be employed to ensure quality and rigor of the proposed graduate program.

Projected Program Enrollment and Graduates; Projected Departmental Faculty/Students

Data Category	Current – Prior to New Program Implementation	Projected Year 1	Projected Year 2	Projected Year 3	Projected Year 4	Projected Year 5
Data for Proposed Program						
Number of Graduates in Proposed Program	X	0	0	15	15	25
Total # of Declared Majors in Proposed Program	X	15	30	40	55	80
Departmental Data – For All Programs Within the Department						
Total Department Faculty FTE (as reported in Faculty table above)	11	11	12	12	13	13
Total Department Student FTE (Based on Fall Third Week)	310	325	350	375	400	400
Student FTE per Faculty FTE (ratio of Total Department Faculty FTE and Total Department Student FTE above)	28.18	29.54	29.16	31.25	30.76	30.76
Program accreditation-required ratio of Student FTE/Faculty FTE, if applicable: N/A	N/A	N/A	N/A	N/A	N/A	N/A

Expansion of Existing Program - N/A

Section III: Need

Program Need

Today's information society is driven by "big data," personal information, and the transfer, storage, and security of that information. The Bureau of Labor Statistics has estimated the creation of almost 629,000 jobs in the information technology industry from 2010 to 2020. Individuals looking to advance in the industry will have a competitive advantage through the skills obtained in the proposed graduate degree in Cyber Security and Information Assurance.

Labor Market Demand

According to the International Information Systems Security Certification Consortium otherwise known as (ISC)[2] (note: the number 2 is part of the trade name of the organization and does not reference a footnote), careers associated with information security skill sets is on a rapid increase. (ISC)[2] is the world's largest body of information security professionals with a membership of nearly 90,000 certified security professionals in 135 countries. The (ISC)[2]'s 2015 *Global Information Security Workforce Study* reported that the shortfall of IT security professionals worldwide will reach 1.5 million in five years.[1]

According to the U.S. Bureau of Labor Statistics (BLS), those who work in information security will see rapid job growth and greater demand for skilled technicians at a 10 year total projected growth rate of 37%. This projected growth will generate a greater demand for information security experts which will lead to increases in the expected earnings of those working within the field. The BLS indicated that as of May 2012 the median salary for an Information Security Analyst was $86,170.[2]

According to Burning Glass Technologies, in 2013 there were more than 209,000 postings for Cyber Security-related jobs in the United States alone, ranging across multiple business sectors including defense, financial services, retail, healthcare and professional services. The 2013 total is 74% higher than the number of security jobs posted in 2007.[3]

There are a number of online job boards that currently list information security (cyber security) type positions. Depending on where jobs are searched for (online job boards) will determine the range of jobs available or advertised currently in this field in Utah. For example, the institution reported a recent search at Usajobs.gov listed 182 information security jobs in Utah (4900+ nationwide), 54 openings in Utah through Indeed.com, 68 Utah job openings through Monster.com, and 108 Utah job openings through Linkedin. ClearanceJobs.com identified Salt Lake City (and the surrounding area) as one of the top five cities in the country for employment in cyber security[4].

Graduate degrees in the fields relating to information security, while relatively a new trend, are increasing for executive and management-level positions, often complementing current advanced information technology certifications like CISSP (Certified Information Systems Security Professional) and CISM (Certified Information Security Manager).

---

[1] https://www.isc2cares.org/uploadedFiles/wwwisc2caresorg/Content/GISWS/FrostSullivan-%28ISC%29%C2%B2-Global-Information-Security-Workforce-Study-2015.pdf

[2] http://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm

[3] http://www.burning-glass.com/research/cybersecurity/

[4] http://news.clearancejobs.com/2013/05/23/top-5-cities-for-cyber-security-jobs/

The Federal Emergency Management Association (FEMA) has developed a dedicated Emergency Management Institute to provide information about a variety of educational opportunities. Specifically, the Emergency Management Institute publishes "The College List" which provides information on emergency management programs offered by accredited institutions of higher education within the United States.[5] Emergency management programs listed on The College List include:

- 67 certificates, minors, diplomas, tracks, or focus areas
- 50 associate degrees
- 47 bachelor degrees
- 87 master's-level programs
- 9 doctoral-level programs

Given the rapid increase in employment and career opportunities in the field of Cyber Security, the rate by which higher education is developing graduate-level programs in this field is well below the current and projected employment demands. It is anticipated that prospective students be drawn to the educational opportunity provided by the program and that the fully online delivery mode will accommodate students throughout the country who are currently employed in the information technology sector.

Student Demand

A preliminary survey was administered by SUU during the opening weeks of Fall Semester 2013. The survey was distributed to current SUU students, members of the CSIS Industrial Advisory Board, local industry professionals, and international participants (total surveyed, N = 376). Results indicated that 84% of respondents were "Definitely interested" (45%) or "Somewhat interested" (39%), in the proposed online graduate degree in Cyber Security and Information Assurance.

Similar Programs

There are currently no online master degrees offered in the Utah System of Higher Education that specifically address Cyber Security and Information Assurance, although there are some related offerings. These are mentioned below.

Through its School of Computing, the University of Utah currently provides undergraduate and graduate programs in Information Systems that focus on a traditional Information Systems curriculum (i.e., creating and managing information systems within a business setting/environment). The Master's program in Information Systems is "designed to provide advanced IT training for individuals seeking the skills necessary to manage the technology of business." [6] The School of Computing also offers a graduate program in Computer Science that includes ancillary topics in security that would provide an avenue to articulate students between the programs depending on the focus the student wishes to pursue in their Master's education.

Utah Valley University (UVU) offers undergraduate degrees in Information Systems and Technology, including a program in Emergency Service Administration that prepares graduates for careers in many state, federal, and private industries. Graduates from this degree program could easily articulate into the proposed graduate degree in Cyber Security and Information Assurance. Recently, UVU developed a graduate certificate program in Cyber Security that is funded through a national grant. Conversations have taken place with UVU to create pathways between UVU and SUU.

[5] http://www.training.fema.gov/EMIWeb/edu/collegelist/

[6] http://msis.business.utah.edu/page/msis-program-overview

Utah State University (USU) currently offers a traditional Management Information Systems degree, both at the undergraduate and graduate levels. However, these programs do not include a security component. The proposed graduate program in Cyber Security and Information Assurance at SUU includes a digital forensics component, which was very appealing to those at USU.

Finally, Dixie State University (DSU) offers an undergraduate degree in Information Technology with an emphasis in Computer and Information Technology. Much like the other undergraduate programs within USHE, graduates from DSU's program would be prepared to pursue graduate work in the proposed degree program.

Nationally, there are a number of graduate programs in Cyber Security, which are being created in response to the growing demand of these types of professionals. Carnegie Mellon, George Washington University, and University of South Florida (online program) are a few institutions that have created these types of advanced degrees. The tuition and fee structure of SUU is very competitive with respect to these other institutions.

Collaboration with and Impact on Other USHE Institutions

Utah institutions of higher education recognize the importance of providing continued education and training for professionals in cyber security. This emerging field provides new opportunities for USHE institutions to collaborate in a number of different ways. As mentioned above, Utah Valley University recently created a graduate certificate in Cyber Security. SUU is willing to work closely with UVU to articulate those students into the proposed graduate degree program. SUU will also work with the other USHE institutions to advise students into the appropriate graduate program in USHE to best fit their career goals.

Benefits

According to a global survey of senior risk decision-makers assembled by KPMG, 50 percent of U.S. boards and 41 percent of boards globally are increasing their focus on solutions relating to Government, Risk, and Compliance (GRC), compared with just 13 percent in the United States and 10 percent globally (among those polled prior to the recent financial crisis). The survey findings also suggested that respondents identified executive management (42 percent in the United States and 48 percent globally) and regulators (27 percent in the United States and 43 percent globally) as the stakeholders exerting the most pressure on organizations to improve convergence of their GRC activities.[7] Support for these executives stem in large part by added expertise offered by formally trained mid-level managers who possess a combination of experience and postgraduate and certification-based training in Cyber Security and Information Assurance. It is anticipated that this program will play a role to close the security gaps found in IT systems.

Consistency with Institutional Mission

Southern Utah University's mission states, "…SUU engages students in a personalized and rigorous experiential education, empowering them to be productive citizens, socially responsible leaders, high achievers and lifelong learners." This program embodies the "rigorous experiential education" that will

[7] http://www.kpmg.com/US/en/IssuesAndInsights/ArticlesPublications/Press-Releases/Pages/Boards-Raise-Focus-On-Risk-Senior-Execs-Demand-Convergence-With-Governance-Compliance-KPMG-Survey.aspx

produce graduates with the skills to be "high achievers and lifelong learners" and to enter the Cyber Security and Information Assurance workforce as responsible and ethical leaders in their field.

Section IV: Program and Student Assessment

Program Assessment - The goals of the program will include:

Program Goal	Measurement
Provide a high-quality, applied-learning experience in Information Security Risk Management and IT Infrastructure Policy Development.	- SUU will track internships and applied-learning activities. - Apply ABET standards to the program, currently used in the Undergraduate programs.
Produce professionals with in-depth understanding of current as well as emerging cyber security and information assurance issues, who can fill the growing need in this field.	- Produce 20 or more graduates on an annual basis. - Employers/Advisory board members will be surveyed to evaluate graduate performance/understanding/skills.
Produce industry-ready CSIA-graduate/ professionals to meet the long-term, growing demand for placement in cyber security positions in a variety of industries and government agencies.	- Student out-placement is expected to exceed 80 percent within 90 days of graduation. - Employers/Advisory board members will be surveyed to evaluate graduate readiness for the industry.

Expected Standards of Performance
The expected learning outcomes include the following:

LO1:	Students will be able to identify, apply, and analyze concepts and practices governing the creation and maintenance of cyber technology infrastructures, including policy development, integrated controls, and web architecture risk mitigation.
Rationale:	Skills in policy development, integrated controls, and web architecture risk mitigation are a growing need in organizations. Industry analysts support this growing need and according to industry trends as reported by several leading organizations including the SANS Institute.
Formative Assessment:	Student performance on quizzes/exams will be analyzed for the purpose of making changes in instruction/curriculum as needed. Instructors will review student work along the process of project completions for the purposes of providing students with ongoing feedback and for making changes in instruction/curriculum as needed.
Summative Assessment:	Eighty percent of students will pass each project, exam or quiz associated with this outcome with a grade of "B" or higher.
LO2:	Students will design, plan, and establish Government, Regulatory, and Compliance (GRC), security, and cyber infrastructure frameworks.

Rationale:	Cyber systems have become the target of many cyber criminals to disrupt national economic progress and financial institutions, it is necessary to have individuals who can design, plan and secure those systems.
Formative Assessment:	Instructors will review student work along the process of project completions for the purposes of providing students with ongoing feedback and for making changes in instruction/curriculum as needed.
Summative Assessment:	Eighty percent of students will pass each project associated with this outcome with a grade of "B" or higher.
LO3:	Students will be able to critically gather, analyze, evaluate, communicate and translate technology-driven data for a variety of audiences, with an emphasis on how to articulate risk mitigation issues to executive and board leadership.
Rationale:	Due to the rapid change in the information technology field, and the rapid change in the nature, scope, and source of the threats to information security, graduates of the program must possess transferable skills to respond to new threats, challenges, and opportunities. Beyond merely knowing such things, graduates will be expected to work in teams and to communicate key findings succinctly to stakeholders at a variety of levels of management.
Formative Assessment:	Instructors will review student work along the process of project completions for the purposes of providing students with ongoing feedback and for making changes in instruction/curriculum as needed.
Summative Assessment:	Eighty percent of students will pass each project associated with this outcome with a grade of "B" or higher.
LO4:	Students will be able to identify, analyze, and apply ethical reasoning relating to cyber security and information assurance issues.
Rationale:	Personal, private, and confidential information is central to cyber security issues. Professionals in this industry need to exercise and maintain ethical behavior and reasoning relating to this sensitive information.
Formative Assessment:	Instructors will review student work along the process of project completions for the purposes of providing students with ongoing feedback and for making changes in instruction/curriculum as needed.
Summative Assessment:	Eighty percent of students will pass each project associated with this outcome with a grade of "B" or higher.

In addition to the above listed learning outcomes, assessment will be accomplished in classes by instructors through the use of projects to assess student learning of the course objectives and to improve both teaching and learning in the online or virtual classroom. Additional assessment will be used in the form of exams, include both in-class and external industry certification exams, to evaluate student competency of the given coursework completed in the program. The external exams were chosen because they measure minimum industry competency standards for the security field in which this proposed program educates.

Section V: Finance

Department Budget

5-Year Budget Projection							
Departmental Data	Current Departmental Budget – Prior to New Program Implementation	Departmental Budget					
		Year 1		Year 2		Year 3	
		Addition to Budget	Total Budget	Addition to Budget	Total Budget	Addition to Budget	Total Budget
Personnel Expense							
Salaries and Wages	631,836	59,760	691,596	95,155	786,752	24,683	811,435
Benefits	231,925	35,399	267,325	34,501	301,826	13,026	314,853
Total Personnel Expense	$863,762	$95,160	$958,922	$129,656	$1,088,578	$37,709	$1,126,288
Non-Personnel Expense							
Travel	9,080	3,000	12,080	0	12,080	0	12,080
Capital	0	0	0	0		0	
Library	0	0	0	0		0	
Current Expense	52,987	2,000	54,987	0	54,987	0	54,987
Total Non-personnel Expense	62,067	5,000	67.067	0	67.067	0	67.067
Total Expense (Personnel + Current)	$925,828	$100,160	$1,025,988	$129,656	$1,155,645	$37,709	$1,193,355
Departmental Funding							
Appropriated Fund	884,596	100,159	984,756	129,657	1,114,413	37,710	1,152,123
Other:							
Special Legislative Appropriation	25,000		25,000		25,000		25,000
Grants and Contracts	3,879		3,879		3,879		3,879
Special Fees / Differential Tuition	12,354		12,354		12,354		12,354
Total Revenue	$925,828	$100,159	$1,025,988	$129,656	$ 1,155,645	37,709	$1,193,355
Difference							
Revenue -	$0	$0	$0	$0	$0	$0	$0

Expense							
Departmental Instructional Cost/Student Credit Hour*	$184.48		$211.69		$227.55		$248.69
* Projected Instructional Cost/Student Credit Hour data contained in this chart are to be used in the Third-Year Follow-Up Report and Cyclical Reviews required by R411.							

Funding Sources

Initial funding of the program will come through the reallocation of existing resources and tuition generated through increased graduate student enrollment. Current faculty schedules will be restructured to accommodate the teaching of courses in the program. As the program grows, additional external funding will be sought (e.g., grants, etc.), to enable students the opportunity for research in the program's areas of study. It is important to note that the seeking of external funding is not meant to help sustain the program, but rather to provide research opportunities to students and faculty. The special legislative appropriation is the continuing support to the College of Science and Engineering from the state's Engineering and Computer Technology Initiative. Contracts and grants are also funds currently allocated to CSIS. The Special Fees/Differential Tuition shows the current amount of program fees going to CSIS and the new amount is based on fees generated by the estimated enrollment in the program.

Reallocation

Current faculty will service courses up to a full course load, according to approved SUU policy. Faculty loads will be adjusted in the undergraduate program to accommodate this shift. CSIS 1000 is being dropped as a University GE requirement and will become an elective GE class. The adjustment would come through offering fewer sections of this course thereby freeing faculty to participate in servicing the graduate level courses.

Impact on Existing Budgets

Based on the ability to adjust current faculty workloads, the only impact would be the hiring of qualified contingent instructors, as needed. Tuition dollars generated by the program will be sufficient to accommodate the hiring of these instructors.

Section VI: Program Curriculum

All courses were reviewed and approved by the College of Science and Engineering Curriculum Committee and the University Graduate Curriculum Committee according to SUU academic policy.

All Program Courses (with New Courses in Bold)

Course Prefix and Number	Title	Credit Hours
Required Courses		
CSIA 6000	Network Security	2
CSIA 6010	Communication, Critical Thinking, Problem Solving and Decision Making	3
CSIA 6020	IT Policy Compliance and Disaster recovery	3
CSIA 6030	Advance Persistent Threats	2
CSIA 6040	Project Management (Cyber Infrastructure)	3

Course Prefix and Number	Title	Credit Hours
CSIA 6060	Cyber Infrastructure Risk Management	2
	Sub-Total	15
Emphasis #1	*Cyber and Web Security Emphasis*	
	(Select 12 Credits from the following courses)	
CSIA 6200	Hacking and Security Vulnerability Management	3
CSIA 6210	Penetration Testing	3
CSIA 6220	Mobile Hacking and Web Application Security	3
CSIA 6230	Cryptography Fundamentals	3
CSIA 6240	Digital Forensics	3
CSIA 6250	Network and Internet Forensics	3
CSIA 6260	BYOD & Mobile Computing Infrastructure	3
	Sub-Total	12
Emphasis #2	*Government, Regulation, and Compliance (GRC) and IS Controls Emphasis*	
	(Select 12 Credits from the following courses)	
CSIA 6300	e-Business Security and Cyber Investigations	3
CSIA 6310	HIPAA-based Business Modeling and Policy Development	2
CSIA 6320	ISO/IEC 27001 ISMS Security Frameworks	2
CSIA 6330	Technology Frameworks and Corporate Governance	2
CSIA 6340	FISMA & Government Infrastructure Mandates	3
CSIA 6350	PCI / DSS / GLBA (Harvard Business Review)	3
CSIA 6360	Basel III – Impact on Bank Risk Management	3
	Sub-Total	12
CSIA 6500	Capstone Experience (Thesis and/or approved Internship)	6
	Total Number of Credits	33

Program Schedule of Courses

Sample Course Sequence: Emphasis #1 - *Cyber and Web Security*

First Semester

CSIA 6000 - Network Security	2
CSIA 6010 - Communication, Critical Thinking, Problem Solving and Decision Making	3
CSIA 6020 - IT Policy Compliance and Disaster Recovery	3
CSIA 6030- Advance Persistent Threats	2
Maximum Semester Credits:	10

Second Semester

CSIA 6040 - Project Management (Cyber Infrastructure)	3
CSIA 6060 - Cyber Infrastructure Risk Management	2
CSIA 6200 - Hacking and Security Vulnerability Management *or*	3

CSIA 6210 - Penetration Testing	
Maximum Semester Credits:	8

Third Semester

CSIA 6220 - Mobile Hacking and Web Application Security	3
CSIA 6230 - Cryptography Fundamentals	3
CSIA 6240 - Digital Forensics *or*	3
CSIA 6250 – Network & Internet Forensics *or*	
CSIA 6260 - BYOD & Mobile Computing Infrastructure	
Maximum Semester Credits:	9

Fourth Semester

CSIA 6500 -Capstone Experience (Thesis and/or approved internship)	6
Maximum Semester Credits:	6

Sample Course Sequence: Emphasis #2 - *GRC and IS Controls Emphasis*

First Semester

CSIA 6000 - Network Security	2
CSIA 6010 - Communication, Critical Thinking, Problem Solving and Decision Making	3
CSIA 6020 - IT Policy Compliance and Disaster Recovery	3
CSIA 6030 - Advance Persistent Threats	2
Maximum Semester Credits:	10

Second Semester

CSIA 6040 - Project Management (Cyber Infrastructure)	3
CSIA 6060- Cyber Infrastructure Risk Management	2
CSIA 6300 - e-Business Security and Cyber Investigations *or*	3
CSIA 6310 - HIPAA-based Business Modeling and Policy Development	2
Maximum Semester Credits:	7-8

Third Semester

CSIA 6320 - ISO/IEC 27001 ISMS Security Frameworks	2
CSIA 6330 - Technology Frameworks and Corporate Governance	2
CSIA 6340 - FISMA & Government Infrastructure Mandates	3
CSIA 6350 – PCI / DSS / GLBA (Harvard Business Review Case Study) *or*	3
CSIA 6360 - Basel III – Impact on Bank Risk Management / Sarbanes Oxley	
Maximum Semester Credits:	10

Fourth Semester

CSIA 6500 - Capstone Experience (Thesis and/or approved Internship)	6
Maximum Semester Credits:	6

Section VII: Faculty

The following faculty are in the Department of Computer Science and Information Systems:

Dr. Robert A. Robertson (Department Chair)

- Ph.D. in Information Systems, Security Emphasis (Nova Southeastern University)
- Master's in Business Administration
- Certified Ethical Hacker Certification
- GIAC Certified Forensic Examiner
- GIAC Certified Forensic Analyst

Dr. Shalini Kesar

- Ph.D. in Information Systems (University of Salford, UK)
- Master and Doctoral degrees have been in the area of information security: focused on computer crime.
- Research has also included the following:
    - Ethical, legal, and policy issues associated with computer crime.
    - Cybercrime and electronic government
    - Electronic Government: The Weakest Link in Cybercrime

Dr. Nathan Barker

- Ph.D. in Computer Science (University of Utah)
- Computer Hacking Forensic Investigator (CHFI)
- Certified Computer Forensics Examiner (CCFE)

Dr. Michael Grady

- Ph.D. in Mathematics (University of California, Santa Barbara)
- Will be teaching the Cryptography course
- Expertise areas - computational number theory, computational combinatorics and abstract algebra.

Dr. Nasser Tadayon

- Ph.D. in Computer Science (University of Louisiana in Lafayette)
- Research areas include:
    - Software Engineering, Data Mining and Neural Networks
    - Computing Education, Design and Analysis of Combinatorial and Geometric Algorithms
    - Graph Theory, Numerical Analysis, Discrete Structures

Dr. Dezhi Wu

- Ph.D. in Information Systems (New Jersey Institute of Technology)
- Research areas include:
    - Human Computer Interaction
    - Information Systems Security
    - Mobile Computing
    - Project Management (Currently PMP Certified)

SAMPLE WHITE HAT AGREEMENT

White Hat Agreement

As part of this course, you will be exposed to systems, tools and techniques related to Information Security. With proper use, these components allow a security or network administrator to better understand the vulnerabilities on the network and the security precautions in effect. Misused, intentionally or accidentally, these components can result in breaches of security, damage to data or other undesirable results.

Since these lab experiments will be carried out in part on a public network that is used by people for real work, you must agree to the following before you can participate. If you are unwilling to sign this form, then you cannot participate in the lab exercises.

Student Agreement Form

I agree to:

- Examine only the special course accounts for privacy vulnerabilities.
- Report any security vulnerabilities discovered to the course instructor immediately, and not disclose them to anyone else.
- Maintain the confidentiality of any private information I learn of through the course exercises.
- Actively use my course account with the understanding that its contents and actions may be discovered by others.
- Hold harmless the course instructor and Southern Utah University for any consequences associated with my own misuse of course software or hardware.
- Abide by the computing policies of Southern Utah University and by all laws governing use of computer resources on campus.

I agree NOT to:

- Attempt to gain root access or any other increase in privilege on any University workstation other than those authorized in this classroom (ELC306).
- Disclose or use for my own purposes, any private information that I discover as a direct or indirect result of the course exercises.
- Take actions that will modify or deny access to any data or service not owned by me.
- Attempt to perform any actions or use utilities presented in the class outside the confines and structure of the classroom (ELC306).
- Utilize any security vulnerabilities or exploits beyond the target accounts in the course or beyond the duration of the course exercises.
- Pursue any legal action against the course instructor or Southern Utah University for consequences related to misuse of materials used in this course.

Moreover, I consent for my course accounts and systems to be examined for security and privacy vulnerabilities by other students in the course, with the understanding that this may result in information about me being disclosed.

This agreement has been explained to me to my satisfaction. I agree to abide by the conditions of the White Hat Oath and Code of Ethics found in the preface to the Lab Manual text.

Student Signature: _____ Date:_____

Student Printed Name: _____

E-mail Address:_____