Request to Offer a New Degree Program

University of South Florida	**Fall 2014**
University Submitting Proposal	Proposed Implementation Term
Business, Engineering, Arts & Sciences, and Behavioral and Community Sciences	**Institute for Secure and Innovative Computing**
Name of College(s) or School(s)	Name of Department(s)/ Division(s)
Cybersecurity	**Master of Science in Cybersecurity**
Academic Specialty or Field	Complete Name of Degree
43.0303	
Proposed CIP Code	

The submission of this proposal constitutes a commitment by the university that, if the proposal is approved, the necessary financial resources and the criteria for establishing new programs have been met prior to the initiation of the program.

Date Approved by the University Board of Trustees	President Date
Signature of Chair, Board of Date Trustees	Vice President for Academic Date Affairs

Provide headcount (HC) and full-time equivalent (FTE) student estimates of majors for Years 1 through 5. HC and FTE estimates should be identical to those in Table 1 in Appendix A. Indicate the program costs for the first and the fifth years of implementation as shown in the appropriate columns in Table 2 in Appendix A. Calculate an Educational and General (E&G) cost per FTE for Years 1 and 5 (Total E&G divided by FTE).

Implementation Timeframe	Projected Enrollment (From Table 1)		Projected Program Costs (From Table 2)				
	HC	FTE	E&G Cost per FTE	E&G Funds	Contract & Grants Funds	Auxiliary Funds	Total Cost
Year 1	120	112.50	0	0	0	$1,286,210	$1,286,210
Year 2	300	281.26					
Year 3	300	281.26					
Year 4	300	281.26					
Year 5	300	281.25	$0	0	0	$4,781,173	$4,781,173

Note: This outline and the questions pertaining to each section <u>must be reproduced</u> within the body of the proposal to ensure that all sections have been satisfactorily addressed. Tables 1 through 4 are to be included as Appendix A and not reproduced within the body of the proposals because this often causes errors in the automatic calculations.
Introduction

I. *Program Description and Relationship to System-Level Goals*

    A. *Briefly describe within a few paragraphs the degree program under consideration, including (a) level; (b) emphases, including concentrations, tracks, or specializations; (c) total number of credit hours; and (d) overall purpose, including examples of employment or education opportunities that may be available to program graduates.*

In February 2010, Admiral Mike McConnell, Former Director of National Intelligence was quoted in the *Washington Post* as follows: *The United States is fighting a cyber-war today, and we are losing. It's that simple. As the most wired nation on Earth, we offer the most targets of significance, yet our cyber-defenses are woefully lacking…for all our war games and strategy documents focused on traditional warfare, we have yet to address the most basic questions about cyber-conflicts.*

USF proposes to implement a Master of Science in Cybersecurity that will be interdisciplinary and will utilize talent across Business, Engineering, Arts & Sciences and Behavioral and Community Sciences. The program will offer four concentrations totaling 18 credit hours, as follows: Information Assurance, Cyber Fundamentals, Cyber Intelligence, and Cyber Crime.

The program will require 30 credit hours of coursework, **all of which can be completed online** in this proposed cost-recovery program. Common core courses (4 in total, 3 credit hours each) proposed for the Master's program are:

- Data Communications/Networks,
- Cryptography,
- Basics of Information Security, and
- Decision Processes for Business Continuity and Disaster Recovery.

Following the core courses students will elect a concentration in one of the following:
- assurance
- intelligence
- operations
- forensics.

The concentrations will be available to students as they complete the core courses.

The general purpose of this program is to prepare students for leadership, managerial and domain-specific roles in Cybersecurity. In March 2013, Steve Rosenbush wrote in The Wall Street Journal's CIO Journal that "Demand for Cybersecurity Jobs is Soaring". The article extensively quotes Burning Glass International Inc., a company specializing in real-time matching of job postings and job seekers. One such quote was that the demand for cybersecurity jobs was growing 12 times faster than the overall job market. Salaries for cybersecurity experts averaged $101,000 in the recent past based on advertised salaries studied by this firm. Job opportunities for graduates exist in both public and private sectors. Some notable sectors include defense, finance and banking, healthcare, retail, and utilities.

Broadly, the program prepares students for employment in managerial and operational positions that require quick analytical thinking, decision-making under uncertainty regarding critical resources, and domain-specific technical skills for managing secure operations. Specifically, based on the design of the concentrations and the core of this program, the program is also designed to prepare students for 1) intelligence positions that require innovative, analytical, decision-making, and technical skills for providing cybersecurity intelligence, 2) information assurance positions that require secure management of information and data transferred, used, stored, and processed in information systems, 3) law enforcement positions that are required to deal more and more with cyber-crimes, and 4) cybersecurity positions that require deep technical skills in the security domain.

> B. *Describe how the proposed program is consistent with the current State University System (SUS) Strategic Planning Goals. Identify which specific goals the program will directly support and which goals the program will indirectly support. (See the SUS Strategic Plan at http://www.flbog.org/about/strategicplan/)*

The Master of Science in Cybersecurity **directly** supports the following goals in the State University's System's Strategic Plan:

- Teaching & Learning
- Scholarship, Research, and Innovation
- Community and Business Engagement

With a goal of graduating 120 students with a Master of Science in Cybersecurity by 2015, 300 by 2016, and 480 by 2017, this program will directly support the SUS Strategic Planning Goal of **Teaching & Learning** by increasing the number of degrees awarded in areas of strategic emphasis. The program will particularly strengthen the quality and reputation of academic programs by offering coursework in subjects relevant to current workforce needs. There is a growing workforce shortage in all areas of cybersecurity.

The program will include collaborative efforts between the university and external partners such as U.S. Central Command at MacDill Air Force Base to obtain data for research, sponsorships for interdisciplinary research projects that could support postdoctoral scholars to enhance research productivity. All of these directly support the SUS Strategic Planning Goal of **Scholarship, Research, & Innovation** for increased collaboration and external support for research activity in a knowledge economy. The degree by its very nature will require technological innovation. The very purpose of the degree is to train students in the methods required to stay ahead of security breaches through technological innovations and creative methodology.

Consistent with the SUS Strategic Planning Goal of **Community and Business Engagement**, the program will strengthen USF's relationships with the business community and government agencies in Florida through collaborative efforts in cybersecurity research, vulnerability determination, cyber intelligence, cyber-crime, securing systems, and ensuring business continuity. Various research and studies combined with direct conversations with public and private companies including the U.S. Air Force, Raymond James Security, Tampa Electric Company, and TechData have identified Cybersecurity as an area where there is high demand for skilled and qualified professionals while supply lags behind. The graduates of the proposed program could fulfill the work force needs of Florida and nationwide, as it relates to cybersecurity and related fields.

C. *If the program is to be included in an Area of Programmatic Strategic Emphasis as described in the SUS Strategic Plan, please indicate the category and the justification for inclusion.*

The program is to be included in the Science, Technology, Engineering, and Math (STEM) related area of Programmatic Strategic Emphasis as described in the SUS Strategic Plan since the program will provide education and support research in STEM related topics. Given the highly technical nature of the program including a deep understanding of computer architecture and programming, this program is technologically and mathematically oriented.

> D. *Identify any established or planned educational sites at which the program is expected to be offered and indicate whether it will be offered only at sites other than the main campus.*

The Master of Science in Cybersecurity is planned to be hosted at the main USF campus in Tampa, Florida. All courses in this program are anticipated to be delivered online, thus posing minimum demand for USF campus facilities.

Institutional and State Level Accountability

II.   *Need and Demand*

> A. *Need: Describe national, state, and/or local data that support the need for more people to be prepared in this program at this level. Reference national, state, and/or local plans or reports that support the need for this program and requests for the proposed program which have emanated from a perceived need by agencies or industries in your service area. Cite any specific need for research and service that the program would fulfill.*

In 2010, President Obama expanded federal cybersecurity initiatives begun under President George W. Bush, and the resulting Comprehensive National Cybersecurity Initiative (CNCI) called cybersecurity "one of the most serious economic and security challenges we face as a nation." [1]

Many of the 2010 CNCI's initiatives focus on protecting federal data, information, and systems, but two initiatives specifically address support for the need for more people to be prepared in this program at this level. These are: **Initiative #8- Expand cyber education, and Initiative #9- Define and develop enduring "leap-ahead" technology, strategies, and programs.**

> **Initiative #8: Expand cyber education --** While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the well-trained workforce with the right knowledge, skills, and abilities to implement those technologies that primarily determines success of security investments. However there are not enough cybersecurity experts within the Federal Government or private sector to implement CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in their focus, or lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a

---

1 "The Comprehensive National Cybersecurity Initiative," National Security Council, The White House (n.d.), p. 1.
http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative

national strategy, similar to the efforts in the 1950's to upgrade science and mathematics education, to meet this challenge.

Initiative #9: Define and develop enduring "leap-ahead" technology, strategies, and programs -- One of the goals of CNCI is to develop technologies that provide increases in cybersecurity by orders of magnitude above current systems within the next 5 to 10 years. This initiative seeks to develop strategies and programs to enhance the component of the government R&D portfolio that pursues high-risk/high-payoff solutions to critical cybersecurity problems. The Federal Government has begun to outline Grand Challenges for the research community to help solve these difficult problems that require 'out of the box' thinking. In dealing with the private sector, the government is identifying and communicating common needs that should drive mutual investment in key research areas. [2]

Additionally, looking at the perceived need for the program, Symantec's *CIO Digest* notes unusually strong bipartisan support in the U.S. House for the Cybersecurity Enhancement Act (HR 4061). The bill authorized "hundreds of millions of dollars for cybersecurity research and education," including funding enabling the National Science Foundation's basic cyber-research scholarships "to increase the size and skills of the cybersecurity workforce" and increased "research and development, standards development and coordination, and public outreach" in cybersecurity. [3] While two-thirds of the appropriation covered 2010-2014, another $320 million was designated for continued action after 2014. The support for cyber-research, cyber-development, and coordination by the NSF suggests that there is an eminent need for Master's level people who excel in cybersecurity.

Workforce development and economic development

Computerworld noted in a 2013 report that "demand for cybersecurity professionals over the past five years grew 3.5 times faster than demand for other IT jobs and about 12 times faster than for all other jobs." [4]

The Master of Science in Cybersecurity program at USF will utilize an existing robust group of well-credentialed research and teaching faculty (see Appendix B) in a wide range of disciplines with expertise in a variety of fields, such as business, education, technology, social sciences, and health care, as well as local subject-matter experts, particularly in conjunction with retired high-ranking military officers who have

---

2 "The Comprehensive National Cybersecurity Initiative," p. 4.
3 Heckert, Brian, "Defining the Cybersecurity Enhancement Act: Vulnerabilities of IT and Communications Infrastructure," *CIO Digest*, July 2010,   p. 7.
4 Vijayan, Jaikumar, "Demand for IT Security Experts Outstrips Supply," *Computerworld*, March 7, 2013. *http://www.computerworld.com/s/article/print/9237394/Demand_for_IT_security_experts*

remained in the Tampa Bay area. Students enrolled in the program will have an opportunity to excel in the field as a result of working with world-renowned researchers and educators who support the program.

The metropolitan area of Tampa offers abundant opportunities for workforce development and USF is in proximity of MacDill Air Force Base, home to both the U.S. Central Command (CENTCOM) and US Special Operations Command (SOCOM), with 10,500 military and 4,000 civilian personnel on base. [5] Students enrolled in the program may be supported by government agencies through collaborative efforts, such as research and development projects. Additionally, the Tampa Bay area is an important center for global financial operations including anti-money laundering efforts. This provides opportunities for program support from the private sector.

> B. *Demand: Describe data that support the assumption that students will enroll in the proposed program. Include descriptions of surveys or other communications with prospective students.*

Based on a recent phone survey of 6 universities around the United States conducted in September 2013, a range of 25 – 40 students are consistently enrolled in graduate-level programs that offer coursework specific to or related to Cybersecurity. If similar coursework and course content is offered in a Master of Science in Cybersecurity program at USF, then student enrollment can be expected to grow as indicated in Appendix A, as this degree will be fully online, a differentiating factor that allows access to students who would not otherwise be able to attend on-campus only classes. Working professionals will be attracted to the ability to earn this valuable credential while fully employed. Also of note is that University of Maryland University College reported enrolling **4200** students in Fall 2012 in undergraduate and graduate programs in cybersecurity, which are fully online, helping to underscore the demand for online access to this subject area. (http://www.umuc.edu/visitors/about/ipra/glance.cfm)

In addition, this program is truly inter-disciplinary covering areas of technology, forensics, law, policy, compliance, psychology, behavioral science and the like. This is one of the differentiating aspects when compared to other such degree programs offered by other academic institutions in Florida and the nation.

> C. *If substantially similar programs (generally at the four-digit CIP Code 43.0303 or 60 percent similar in core courses), either private or public exist in the state, identify the institution(s) and geographic location(s). Summarize the outcome(s) of communication with such programs with regard to the potential impact on their enrollment and opportunities for possible collaboration (instruction and research). In Appendix B, provide data that support the need for an additional program as well as letters of support, or letters of concern, from the provosts of other state*

---

5 "MacDill By the Numbers," MacDill Air Force Base. *http://www.macdill.af.mil/questions/topic.asp?id=570*

universities with substantially similar programs.

According to the academic program inventory of the State University System of Florida[6], there are no other programs in the 43.0303 CIP code. There is one bachelors program offered by FSU in the CIP code 43.0116, "Cyber/computer forensics and counter-terrorism." Therefore, similar programs do not appear to exist elsewhere in the state. Furthermore, the Cybersecurity program is designed to prepare students for

leadership, managerial and domain-specific roles in Cybersecurity, positions calling for graduate preparation beyond the baccalaureate level.

> D. *Use Table 1 in Appendix A (A for undergraduate and B for graduate) to categorize projected student headcount (HC) and Full Time Equivalents (FTE) according to primary sources. Generally undergraduate FTE will be calculated as 40 credit hours per year and graduate FTE will be calculated as 32 credit hours per year. Describe the rationale underlying enrollment projections. If, initially, students within the institution are expected to change majors to enroll in the proposed program, describe the shifts from disciplines that will likely occur.*

As seen from Table 1-B in the appendix, a total enrollment of 120 (FTE: 112.50) students is projected in the first year, followed by steady growth in subsequent years, leading to a projected enrollment of 300 students (FTE: 281.25) in the 5th year.

The enrollment projections are realistic, given the shortage of cybersecurity trained professionals in the work force, as well the fact that the USF program offers 4 distinctive concentrations covering a variety of informational areas – Cyber Fundamentals, Information Assurance, Cyber Intelligence, and Cyber Crime. Further, certificates will also be offered in the various concentrations, thereby making the program more attractive to students as well as generating additional revenues via students who might be interested in starting the program due to the certificate options.

There are additional factors that suggest that the program should attract strong enrollment. The Wall Street Journal's March 2013 article "Demand for Cybersecurity Jobs in Soaring" notes that salaries for engineers and experts in the field range from $80,000 to over $100,000. However we do note that starting salaries for graduates may be lower, but the ability to grow to these salaries in reasonable time will make this program attractive to potential students. *Computerworld* noted in a 2013 report that "Demand for cybersecurity professionals over the past five years grew 3.5 times faster than demand for other IT jobs and about 12 times faster than for all jobs." [7] Students from similar disciplines are expected to enroll in the Master of Science in

---

6 https://prod.flbog.net:4445/pls/apex/f?p=136:45:2367149463925016::NO:::, (Accessed 9/1/2013)
7 Vijayan, Jaikumar, "Demand for IT Security Experts Outstrips Supply," *Computerworld*, March 7, 2013.
http://www.computerworld.com/s/article/print/9237394/Demand_for_IT_security_experts

Cybersecurity program. However, the addition of this program would increase the overall graduate enrollment at USF, instead of cannibalizing existing graduate programs.

> E. *Indicate what steps will be taken to achieve a diverse student body in this program. If the proposed program substantially duplicates a program at FAMU or FIU, provide, (in consultation with the affected university), an analysis of how the program might have an impact upon that university's ability to attract students of races different from that which is predominant on their campus in the subject program. The university's Equal Opportunity Officer shall review this section of the proposal and then sign and date in the area below to indicate that the analysis required by this subsection has been reviewed and approved.*

Diversity among the program's student body is as important to the Institute of Secure and Innovative Computing as it is to the US Intelligence Community, which regards it as a "mission critical" need. We will use strategies such as targeted recruitment and advertising that the IC has used successfully over the past 10 years to increase the representation of under-represented groups to diversify its workforce.

Strategies currently utilized by the Office of the Equal Opportunity Officer at USF will be leveraged to the fullest extend to ensure a diverse student population. Efforts will be made to reach out to "instate" and "out-of-state" under-represented population though program announcements in publications that target this population, and through best practices suggested by the Equal Opportunity Officer.

Signature of Equal Opportunity Officer	**Date**

III. *Budget*

> A. *Use Table 2 in Appendix A to display projected costs and associated funding sources for Year 1 and Year 5 of program operation. Use Table 3 in Appendix A to show how existing Education & General funds will be shifted to support the new program in Year 1. In narrative form, summarize the contents of both tables, identifying the source of both current and new resources to be devoted to the proposed program. (Data for Year 1 and Year 5 reflect snapshots in time rather than cumulative costs.) If the university intends to operate the program through continuing education on a cost-recovery basis or market rate, provide a rationale for doing so and a timeline for seeking Board of Governors' approval, if appropriate.*

The proposed program will be offered as a cost recovery program. This means, no E&G funds will be utilized for this program. Revenues generated from tuition and distance

learning fees will be used to pay for all the expenses of the program as shown below.

	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Number of Courses	8	20	20	24	25	25
Number of Sections Taught	20	60	72	78	87	317
Number of Students in Program	120	300	300	300	300	300
Number of Registrations	360	1,440	1,800	1,800	1,800	7,200
SCH	1,080	4,320	5,400	5,400	5,400	21,600
Average students/class	18	24	25	23	21	25
Tuition and DL Fees	$ 900,709	$ 3,602,837	$ 4,785,786	$ 4,926,906	$ 4,926,906	$19,143,144
Expenses						
Instruction	$ 322,950	$ 986,612	$ 1,211,547	$ 1,346,170	$ 1,538,065	$ 5,405,344
3rd Party Marketing and Student Support	$ 321,749	$ 1,286,998	$ 1,715,999	$ 1,769,624	$ 1,769,624	$ 6,863,995
Course Conversion and Maintenance	$ 300,000	$ 280,000	$ 120,000	$ 385,000	$ 230,000	$ 1,315,000
Proctoring	$ 12,600	$ 50,400	$ 63,000	$ 63,000	$ 63,000	$ 252,000
Faculty Stipends for Course Conversion	$ 48,000	$ 32,000	$ -	$ 20,000	$ -	$ 100,000
College / Department Services	$ 84,338	$ 248,553	$ 292,714	$ 437,891	$ 438,905	$ 1,502,399
Innovative Education Services	$ 99,834	$ 304,538	$ 372,772	$ 372,772	$ 372,772	$ 1,522,687
Other University Services	$ 22,248	$ 88,992	$ 111,240	$ 111,240	$ 111,240	$ 444,960
Other University Fees	$ 74,490	$ 193,984	$ 222,604	$ 256,493	$ 257,567	$ 1,005,140
Total Expenses	$1,286,210	$ 3,472,077	$ 4,109,875	$ 4,762,190	$ 4,781,173	$18,411,525
Surplus / (Deficit)	$ (385,500)	$ 130,760	$ 675,911	$ 164,716	$ 145,733	$ 731,619
Cumulative Surplus / (Deficit)	$ (385,500)	$ (254,740)	$ 421,170	$ 585,886	$ 731,619	
Gross Margin			5%		4%	

The total projected cost for Year 1 is $1,286,210. It is expected that eight 8-week courses will be offered in the first year, with twenty sections taught. The cost of instruction is $322,950, at an average faculty salary of $15,000 per course. Faculty salaries and benefits of $370,950 also include stipends to faculty of $48,000 for their involvement in course development and conversion activities. Instructional design costs for course conversions are projected to be $300,000 in Year 1 for the digitization of 12 courses, including four to be delivered in Year 2, at an average cost of $25,000. In order to grow enrollments of qualified students in an expedient manner, marketing and student enrollment services will be outsourced to a third party provider at an expected rate of 38% of gross tuition, as per existing negotiated contracts with third party providers. With 360 registrations anticipated for 120 students in the first year, tuition is projected at $846,709, distance learning fee revenue at $54,000, and third party marketing and student support services at $321,749. The cost of online proctoring to meet authentication standards and maintain academic integrity of the program is projected at $12,600, averaging $35 per student per course. Program development and support is provided by various university departments. The College of Business Administration provides administration and advising services, the cost of which is projected to be $84,338 in Year 1. Innovative Education provides program development, program management, marketing oversight, financial management, human resources,

compliance, student support, registration, and proctoring support. The total cost of these services in the first year is projected to be $99,834. Other university services and fees, with a cost of $96,738, provide support for admissions, financial aid, registration, technology, student success, and library services.

The total projected cost for Year 5 is $4,781,173. The cost of instruction is forecasted at $1,538,065 with 25 courses offered and 87 sections taught. The cost of third party student enrollment support and marketing services is projected to be $1,769,624, equal to 38% of gross tuition of $4,656,906. (Total revenue of $4,926,906 also includes $270,000 in distance learning fees.) One new course is built in Year 5, and instructional design updates are projected for all courses in order to stay current with evolving knowledge and research in cybersecurity, with an expected cost of $230,000. The cost of proctoring is projected at $63,000, averaging $35 per student per course. With 1,800 registrations, 300 students, and 87 course sections taught, College support costs are projected at $438,905. Innovative Education services described above are projected at $372,772, and other university services and fees are projected at $368,807.

Costs are managed to an appropriate level of reinvestment in the program, providing for academic quality and student service while tuition recovers the costs of the program. Projected revenues cover costs by a conservative margin to allow for forecasting errors and provide necessary working capital. After 3 years, the excess of projected revenues over expenses represents a margin of 5%, and after 5 years, 4%. By year 5, annual revenues and expenses have stabilized, with projected revenues covering expenses by $145,733, or 3%.

> B. *If other programs will be impacted by a reallocation of resources for the proposed program, identify the program and provide a justification for reallocating resources. Specifically address the potential negative impacts that implementation of the proposed program will have on related undergraduate programs (i.e., shift in faculty effort, reallocation of instructional resources, reduced enrollment rates, greater use of adjunct faculty and teaching assistants). Explain what steps will be taken to mitigate any such impacts. Also, discuss the potential positive impacts that the proposed program might have on related undergraduate programs (i.e., increased undergraduate research opportunities, improved quality of instruction associated with cutting-edge research, improved labs and library resources).*

This scenario would not occur as no reallocation of resources is planned. As a cost-recovery program, the full costs of using any E&G faculty or other resources will be recovered and paid through the auxiliary fund set up for this program.

       C. Describe other potential impacts on related programs or departments (e.g., increased need for general education or common prerequisite courses, or increased need for required or elective courses outside of the proposed major).

There are no anticipated negative impacts. See above.

       D. Describe what steps have been taken to obtain information regarding resources (financial and in-kind) available outside the institution (businesses, industrial organizations, governmental entities, etc.). Describe the external resources that appear to be available to support the proposed program.

This program would be primarily supported by tuition revenue. Efforts are being made to line up corporate sponsors who could send their employees to enroll in this program.

IV. *Projected Benefit of the Program to the University, Local Community, and State*

Use information from Tables 1 and 2 in Appendix A, and the supporting narrative for "Need and Demand" to prepare a concise statement that describes the projected benefit to the university, local community, and the state if the program is implemented. The projected benefits can be both quantitative and qualitative in nature, but there needs to be a clear distinction made between the two in the narrative.

The development of the proposed program will enormously benefit USF, the Tampa region, and the state of Florida. Secure critical systems, secure critical processes, information assurance, national security, protection from criminals, and secure critical infrastructure – which are at the core of cybersecurity – are recognized as a priority from local, state, and global perspectives because the often complex nature of systems, processes, data, population centers, and technologies that need to be protected, as gaps in protection could have catastrophic consequences.   According to the Comprehensive National Cybersecurity Initiative (CNCI), cybersecurity is recognized as "one of the most serious economic and security challenges we face as a nation." The proposed program will provide education and training for students to secure computer and information systems, business systems and processes, and securing infrastructure from threats at all levels – from the university to the local, state, and, prospectively and naturally, global and national levels.

USF has a highly successful track record in drawing research funding ($411 million in FY 2012) and is ranked 10th in among world universities for the number of US patents granted. USF is centrally located in a thriving eight-county "Tampa Bay" regional economic development area. Both USF and the region are rich in global ties in the community as well as in the business world. Added to these abundant resources is the

proximity of MacDill Air Force Base, home of both the U.S. Central Command (CENTCOM) and US Special Operations Command (SOCOM), with 10,500 military and 4,000 civilian personnel on base. These combined with companies and small businesses in the Tampa Bay area and in Florida, provide a supportive ecosystem for the proposed program, thus ensuring demand.

Cybersecurity is a field all of its own in that it is multi-disciplinary by nature, and the program will benefit USF by advancing multidisciplinary training and research across the College of Business, the College of Engineering, the College of the Arts and Sciences, and the College of Behavioral and Community Sciences The program will tap into an existing robust group of well-credentialed research and teaching faculty in an interdisciplinary way, bringing together research in fields in business, education, technology, social sciences, and health care. Local subject-matter experts and military experts in the Tampa Bay area will also benefit the university through collaborative efforts and outreach programs. Further, graduate students enrolled in the program who conduct research, will also benefit the university by the securing of grants from sources such as the National Science Foundation (NSF).
.

V.   *Access and Articulation – Bachelor's Degrees Only*

A. *If the total number of credit hours to earn a degree exceeds 120, provide a justification for an exception to the policy of a 120 maximum and submit a separate request to the Board of Governors for an exception along with notification of the program's approval. (See criteria in Board of Governors Regulation 6C-8.014)*

Not applicable.

B. *List program prerequisites and provide assurance that they are the same as the approved common prerequisites for other such degree programs within the SUS (see the Common Prerequisite Manual at FACTS.org). The courses in the Common Prerequisite Counseling Manual are intended to be those that are required of both native and transfer students prior to entrance to the major program, not simply lower-level courses that are required prior to graduation. The common prerequisites and substitute courses are mandatory for all institution programs listed, and must be approved by the Articulation Coordinating Committee (ACC). This requirement includes those programs designated as "limited access."*

If the proposed prerequisites are not listed in the Manual, provide a rationale for a request for exception to the policy of common prerequisites. NOTE: Typically, all lower-division courses required for admission into the major will be considered prerequisites. The curriculum can require lower-division courses that are not prerequisites for admission into the major, as long as those courses are built into the curriculum for the upper-level 60 credit hours. If there are already common prerequisites for other degree programs with the same proposed CIP, every effort must

be made to utilize the previously approved prerequisites instead of recommending an additional "track" of prerequisites for that CIP. Additional concentrations may not be approved by the ACC, thereby holding up the full approval of the degree program. Programs will not be entered into the State University System Inventory until any exceptions to the approved common prerequisites are approved by the ACC.

Not applicable.

C. *If the university intends to seek formal Limited Access status for the proposed program, provide a rationale that includes an analysis of diversity issues with respect to such a designation. Explain how the university will ensure that community college transfer students are not disadvantaged by the Limited Access status. NOTE: The policy and criteria for Limited Access are identified in Board of Governors Regulation 6C-8.013. Submit the Limited Access Program Request form along with this document.*

Not applicable.

D. *If the proposed program is an AS-to-BS capstone, ensure that it adheres to the guidelines approved by the Articulation Coordinating Committee for such programs, as set forth in Rule 6A-10.024 (see [Statewide Articulation Manual](#) at FACTS.org). List the prerequisites, if any, including the specific AS degrees which may transfer into the program.*

Not applicable.

Institutional Readiness

VI.   *Related Institutional Mission and Strength*

A. *Describe how the goals of the proposed program relate to the institutional mission statement as contained in the SUS Strategic Plan and the University Strategic Plan.*

The goals of the proposed program relate to the SUS Strategic plan by providing graduate and professional education, research, and public service of the highest quality through a well-known higher learning research-oriented university. The program is dedicated to serving the needs of a diverse state and a global society inherently because cybersecurity reaches across local, state, national, and global boundaries. Further, the program will support students' development of the knowledge, skills, and aptitudes needed for success in a global society and marketplace within the cybersecurity domain; transform and revitalize Florida's economy and society through research, creativity, discovery, and innovation in cybersecurity; mobilize resources to address the significant

challenges
and opportunities facing Florida's citizens, communities, regions, the state, and beyond by engaging with local businesses and the community in outreach programs; and deliver knowledge to advance the welfare and economy through community and business engagement and service through relationships built and maintained between the university, the program, and the business community.

The proposed program goals of conducting basic and applied research, educational goals, and collaborative efforts with local business community, CENTCOM, and SOCOM directly relates to the USF 2013-2018 Strategic Plan in that it will deliver a competitive graduate and professional program, generate knowledge, foster intellectual development, and ensure student success in a global environment.

> B. *Describe how the proposed program specifically relates to existing institutional strengths, such as programs of emphasis, other academic programs, and/or institutes and centers.*

The Information Systems & Decision Sciences department hosting the Information Assurance track has been ranked among the top 10 nationally for publication in premier MIS journals in the past. More recently, the undergraduate MIS program was ranked #25 by Business Week. The Computer Science and Engineering department, hosting the Cyber Fundamentals track, is in the top third departments nationally based on NRC rankings. Significant investments have been made in the Computer Science and Engineering department to recruit high research active scholars in the cybersecurity field (there are 3 tenured/tenure track faculty members who teach and research in cybersecurity). The College of Behavioral and Community Sciences, and the College of Arts and Sciences also have expertise relevant to the proposed program. Moreover, CENTCOM and SOCOM are in need of cybersecurity professionals, and their close proximity to USF and the proposed program would be beneficial to both USF and U.S. Government agencies. All these strengths would be leveraged to deliver the proposed program.

> C. *Provide a narrative of the planning process leading up to submission of this proposal. Include a chronology (table) of activities, listing both university personnel directly involved and external individuals who participated in planning. Provide a timetable of events necessary for the implementation of the proposed program.*

In August 2013, the USF Institute for Secure and Innovative Computing was established. Simultaneously, the Board of Governor's report was drafted, the proposal for the Master in Science in Cybersecurity, and the Steering Committee and Focus Group Summits were held. Planning activities involved Sri Sridharan, the Managing Director of Cybersecurity, the provost, Ralph Wilcox, and the four Deans (Moez Limayem, Julie Serovich, Eric Eisenberg and Rafael Perez.

Planning Process

Date	Planning Activity
Summer 2013 – August 2013	USF Institute for Secure & Innovative Computing – application submitted
August 2013	Cybersecurity Survey – Tampa Bay Region
June 2013 – October 2013	Board of Governor's Report Planning
August 2013	Steering Committee Summit Planning
August 2013	Focus Group Summit Planning

Events Leading to Implementation

Date	Implementation Activity
August 2013	USF Institute for Secure & Innovative Computing – approved
August 2013	Steering Committee Summit
August 2013	Focus Group Summit
September 2013	Board of Governor's report – 1st draft
September 2013	Board of Governor's report – 2nd draft
October 2013	Board of Governor's report – final draft

VII.   *Program Quality Indicators - Reviews and Accreditation*

Identify program reviews, accreditation visits, or internal reviews for any university degree programs related to the proposed program, especially any within the same academic unit. List all recommendations and summarize the institution's progress in implementing the recommendations.

The Information Systems and Decision Sciences department is housed in the College of Business. The college is accredited by the AACSB (Association to Advance Collegiate Schools of Business). The Department of Computer Science is part of the College of Engineering, which is accredited by ABET, the Accreditation Board for Engineering and Technology. USF is accredited by SACS, the Commission on Colleges of the Southern Association of Colleges and Schools and all requirements related to comparability of online programs will be heeded and appropriate data provided.

VIII.   *Curriculum*

A. Describe the specific expected student learning outcomes associated with the

proposed program. If a bachelor's degree program, include a web link to the Academic Learning Compact or include the document itself as an appendix.

Student learning outcomes will be related to multiple domains of critical infrastructure protection and cybersecurity. These include secure systems analysis, planning and design, threat modeling, policy development, secure operations, decision-making for infrastructure protection, cyber-forensics and cyber-intelligence. Pedagogical methods used will include lectures, case development and discussion, and hands-on projects. Student learning will be measured in terms of the ability of graduates to enter the workforce with the knowledge and skills that will enable them to succeed in the program areas that each track sets forth to prepare them as professionals.

Student learning outcomes include the following:
1. Graduating students will demonstrate the ability to elicit functional and information requirements as well as assist in the planning, definition and implementation of cybersecurity related tasks. In this process, the student will be familiar with advanced techniques for conducting and managing all security related breaches as well as implementation of protection. This outcome aligns with AACSB Assurance of Learning Standards 19 and 20 for Master's level programs in Business.
2. Students will demonstrate the ability analyze situations and make decisions under uncertain circumstances regarding critical resources.
3. Students will demonstrate the ability to perform technical tasks for providing cybersecurity intelligence.
4. Students will demonstrate specific skills of leadership and management such as critical analysis, exegetic thinking and decision making in uncertainty.

B. Describe the admission standards and graduation requirements for the program.

Admissions will be based on an assessment of the application package, consisting of college transcripts, professional experience and standardized scores (GRE or GMAT). Current standards of admission into the College of Business and College of Engineering will be used as parameters for admission into this program. Students entering the program will be required to have one semester equivalent of programming and operating system coursework, among other technical skills that will be determined by faculty, deans, and others who determine the curriculum. Upon graduation, students must have completed 30 credit hours and will have the option to finish either a master's thesis or participated in an approved practicum program.

C. Describe the curricular framework for the proposed program, including number of credit hours and composition of required core courses, restricted electives, unrestricted electives, thesis requirements, and dissertation requirements. Identify the total numbers of semester credit hours for the degree.

In the proposed program, there will be four required core courses and four concentrations that will require electives determined by the departments leading the concentrations: Information Assurance, Cyber Fundamentals, Cyber Intelligence, and Cyber Crime. Each course will be for three credit hours. Each track will define four electives required to complete the concentration. Students completing the degree in a specific concentration will complete the four required core courses, the four required electives in the concentration and any two electives offered by the other concentrations within the degree program, or other courses approved by faculty as meeting the requirements for the degree. Thesis and practicum options could be exercised in lieu of the six additional hours of elective credits. The total number of semester hours for the program is 30.

> D. *Provide a sequenced course of study for all majors, concentrations, or areas of emphasis within the proposed program.*

Each concentration will require four core courses (Data Communications /Networks, Cryptography, Basics of Information Security, and Decision Processes for Business Continuity and Disaster Recovery). These have been agreed upon by a Cybersecurity Academic Committee at USF comprising representatives from the colleges of Business, Engineering, Behavioral and Community Sciences, and Arts and Sciences. Following the core, each concentration will have its own sequence. Information Assurance with an area of emphasis in designing and managing secure critical infrastructure systems , Cyber Fundamentals with an area of emphasis in operating secure critical infrastructure systems; Cyber Intelligence with an area of emphasis in methodologies for complex information processing for critical systems, and Cyber Crime with an emphasis on forensics following attacks on critical infrastructure systems.

> E. *Provide a one- or two-sentence description of each required or elective course.*

The four core courses are the following:

Required: Data Communications /Network -- This course describes the components of IT infrastructures and their interactions. Specific topics include Physical layer & data link layer/ Ethernet, Network layer/ IP & Transport layer/ TCP, Application layer & support services, Routing & subnetting, WAN technologies, Wireless & phone networks, and Network security and managerial issues.

Required: Cryptography -- This course covers Cryptography context (design criteria, generic attacks), Block ciphers, Hash functions, Message authentication codes, Secure channel, Key negotiation, Prime numbers, Diffie-Hellman, RSA, Key negotiation, Key management (Kerberos), PKI, and Storing secrets.

Required: Basics of Information Security and Risk Management -- The course will include class presentations and extensive hands-on projects on implementing the common IT controls such as access control lists (ACLs), firewalls, network scanning, STIG (Security Technical Implementation Guidelines), identifying software errors and documenting some key IT General Controls. Required reports will help students improve their writing and documentation skills.

Required: Decision Processes for Business Continuity and Disaster Recovery -- This course covers topics such as disaster recovery and business continuity following extreme events. The course will also present methods for decision making in such scenarios, with an emphasis on risk assessment and management. The course will also discuss the guidelines of the U.S. Department of Commerce, National Institute of Standards and Technology (NIST)'s *Computer Security Incident Handling Guide*.

The Courses Required for the Cybercrime Concentration are the following:

CJE 6688 Cybercrime and Criminal Justice
This course will be an introduction to the topic of criminality in online environments. Topics include hacking, online identity theft, fraud, trade in illicit substances/items, sexual crimes online, and responses to cyber criminality (security, law enforcement, surveillance, etc.)

CJE 6623 Digital Evidence Recognition
This course is designed to instruct participants in the basics of recognizing potential sources of electronic evidence, preparing them to respond to an electronic crime scene, and to safely and methodically preserve and collect items of evidentiary value to be used in court proceedings.

CJE 6624 Introduction to Digital Evidence
This course is designed to facilitate development of the basic knowledge and skills necessary to recognize, identify, collect, and preserve digital evidence in any kind of criminal investigation. Topics will include legal and evidentiary considerations in the field and the courtroom, foundations of digital forensics, applying forensic science to digital technologies, digital crime scenes and digital investigations, digital evidence on networks, and digital evidence on the Internet.

CJE 6625 Network Forensic Criminal
As applied to criminal investigations, this course focuses on forensic security issues involving access to data stored on networked computer systems and the transmission of data between systems. Topics include detecting and monitoring intrusions of networks and systems, authentication protocols, malware, and intrusion response strategies.

CJE 6626 Digital Forensic Criminal Investigations

This course will introduce students to digital forensics as practiced by local, state, and federal law enforcement. Students will gain hands-on experience with several digital forensic tools in this laboratory-based course. Students taking this course will become familiar with the emerging responsibilities of cyber crime investigators as well as developing a hands-on working knowledge of software commonly used at many law

The Courses Required for the Cyberintelligence Concentration are the following:

LIS 593 Visual Information Analytics
This course is a hands-on class where the students will analyze data by employing statistics and converting the results into visual representations. The students in the class will also develop the skills necessary to solve different quantitative problems that will allow them to evaluate diverse visualization platforms and applications.

ENG 42335 Analytic Communication
This course focuses on the writing requirements of analytic professionals, with emphasis on the content, organization, format and style of specific types of information technology documents. This course also provides students with the opportunity to develop presentation skills while improving communication and critical thinking skills.

CCJ 6074 Advanced Intelligence Analytic Methods
The objective of this course is to teach students to:
- Understand the applications and limitations of contemporary data analysis software
- Understand the relationship between demographics, technology and the impacts on critical infrastructures within the assigned areas of research.
- Compare the merits of existing technologies and their relationship to future needs.
- Develop a rational and philosophy for data-driven intelligence.
- Explain the scope and applications of open source intelligence gathering by
- business and government entities and its impact on information security

INR 5365 Core Concepts in Intelligence
This course will explore the organization and functions of the U.S. Intelligence Community, its interaction with national security policymakers, key issues about its working, and the challenges it faces in defining its future role. It will also look at some of the key intelligence missions, such as strategic warning, counterterrorism, counter proliferation, and counterinsurgency.

DSC 6600 Cyber intelligence
This course will review the main actors, targets, threats, and other troublesome activities in cyberspace. It builds a foundation for understanding how cyber intelligence

and counterintelligence can support cybersecurity and contribute more broadly to an enterprise or national security mission.

LIS 6758 Information Strategy & Decision Making
This new online course suggests that understanding strategy is a foundation for making information meaningful. Students will understand what strategy means and how it is a fundamentally human endeavor. They will acquire tools and tactics to expand their thinking and problem solving. The course examines the human dimensions of analytic and strategic thought.

The Courses Required for the Assurance Concentraion are the following:

ISM 6145 Seminar on Software Testing
This course will survey and analyze the best practices in industrial testing groups. Students will gain practical experience with both functional and structural testing methods via assignments. Automated testing tools will be an important part of the educational experience. The goal is for all students to come away with an in-depth understanding of software testing practice and research.

ISM 6125 Software Architecture
Software Architecture has emerged as a major area of study for software professionals and researchers. In this course, the students will learn the basic concepts and various Architectural styles with case studies and stress the importance of Software Architecture in building the information systems.

ISM 6124 Advanced Systems Analysis and Design
The goal of this course is to instruct in students in the technical and managerial foundations of software engineering and information systems development. Based on a prerequisite understanding of basic systems concepts, students will learn to manage and perform activities throughout the software-intensive systems development life cycle, from the analysis of system requirements through system design to system implementation, testing, and maintenance.

ISM 6316 Project Management
The general objective of this course is to become familiar with the fundamental issues for managing projects and to develop an understanding of the overall process of dealing with competing demands in various environments.

ISM 6218 Advanced Database Administration
ACG 6457 Accounting Systems Audit, Control, and Security
The purpose of this course is to equip students with the knowledge and skills necessary to add value to organizations as an auditor of IT-intensive accounting systems. Key concerns relating to advanced computer-based accounting systems are the risks

associated with such systems, the controls and security measures that should be incorporated into such systems. This course will enhance the student's ability to design and evaluate information technology controls surrounding accounting information systems.

The Courses Required for the Cyberfundamentals are the following:

EEL 6764 Computer Architecture
This course covers the following topics:
- Impact of VLSI technology on architecture;
- Instruction set principles, Fundamentals of computer design
- Memory hierarchy design
- ILP and Limits of ILP
- Data Level Parallelism
- Pipelining – Vector Processing
- Multiprocessors, TLP and
- Interconnection networks

CIS 6930 (special topics) Computer Networks, Fundamental principles and analysis
This is an introductory graduate course in computer networks covering the fundamental principles guiding the operation of the Internet, performance evaluation of computer networks using analytical methods, and selected hot topics.

CIS 6930 (special topics) Security & Privacy
Computer Security and Privacy is a course that will introduce computer security and privacy topics at the graduate student level (graduate students are assumed to have familiarity with operating systems and at least one programming language). The course will cover secure communication, authentication, operating system security, web security and privacy.

> F. *For degree programs in the science and technology disciplines, discuss how industry-driven competencies were identified and incorporated into the* curriculum *and indicate whether any industry advisory council exists to provide input for curriculum development and student assessment.*

Industry-drive competencies were identified and incorporated into the curriculum by consulting faculty on various occasions, external constituents in government, healthcare, financial services as well as many other leading companies in the industry located in the Tampa Bay area, the Provost, Ralph Wilcox, and the four Deans (Moez Limayem, Julie Serovich, Eric Eisenberg and Rafael Perez). The program will have an industry advisory council; however, it is not in place at this point. A relationship

between the program and industries it will serve are already in place. Industry leaders provided input into the development of competency based outcomes (see student learning outcomes). In a White Paper published by CompTIA on the credentialing of a cybersecurity workforce, competencies in cybersecurity professionals should measure both knowledge-based and performance-based competencies. Both levels are encompassed in the student learning outcomes of this program. Knowledge-based competencies focus on readiness for higher-level and more complex skills mirrored by performance-based skills at each level. Such competencies must be sensitive to and embedded in the physical, e.g. energy and hospitals; cyber, e.g. software and control systems; and critical, e.g. public health and transportation infrastructures. This interleaving of competencies is precisely why the cybersecurity program at USF must rest on partnerships between public, private, and academic institutions.

G. *For all programs, list the specialized accreditation agencies and learned societies that would be concerned with the proposed program. Will the university seek accreditation for the program if it is available? If not, why? Provide a brief timeline for seeking accreditation, if appropriate.*

The National Security Agency accredits Information Assurance programs for which the university will seek accreditation upon availability. This accreditation is anticipated by the year 2013-2014.

H. *For doctoral programs, list the accreditation agencies and learned societies that would be concerned with corresponding bachelor's or master's programs associated with the proposed program. Are the programs accredited? If not, why?*

Not applicable.

I. *Briefly describe the anticipated delivery system for the proposed program (e.g., traditional delivery on main campus; traditional delivery at branch campuses or centers; or nontraditional delivery such as distance or distributed learning, self-paced instruction, or external degree programs). If the proposed delivery system will require specialized services or greater than normal financial support, include projected costs in Table 2 in Appendix A. Provide a narrative describing the feasibility of delivering the proposed program through collaboration with other universities, both public and private. Cite specific queries made of other institutions with respect to shared courses, distance/distributed learning technologies, and joint-use facilities for research or internships.*

The proposed program is anticipated to be delivered entirely online. In accordance with USF policies, faculty participating in the program will undergo required training in online teaching. In its initial stages, it is neither necessary nor feasible to deliver this

program in partnership with other academic institutions in the state due to the specialized expertise available at USF, the fact that the program is already interdisciplinary within USF, and the relationships in the governmental, public, and private sectors USF has developed specifically for the development and implementation of this program.

IX.   *Faculty Participation*

A. *Use Table 4 in Appendix A to identify existing and anticipated ranked (not visiting or adjunct) faculty who will participate in the proposed program through Year 5. Include (a) faculty code associated with the source of funding for the position; (b) name; (c) highest degree held; (d) academic discipline or specialization; (e) contract status (tenure, tenure-earning, or multi-year annual [MYA]); (f) contract length in months; and (g) percent of annual effort that will be directed toward the proposed program (instruction, advising, supervising internships and practica, and supervising thesis or dissertation hours).*

B. *Use Table 2 in Appendix A to display the costs and associated funding resources for existing and anticipated ranked faculty (as identified in Table 2 in Appendix A). Costs for visiting and adjunct faculty should be included in the category of Other Personnel Services (OPS). Provide a narrative summarizing projected costs and funding sources.*

C. *Provide in the appendices the curriculum vitae (CV) for each existing faculty member (do not include information for visiting or adjunct faculty).*

See Appendix B as a summary of anticipated faculty CVs.

D. *Provide evidence that the academic unit(s) associated with this new degree have been productive in teaching, research, and service. Such evidence may include trends over time for average course load, FTE productivity, student HC in major or service courses, degrees granted, external funding attracted, as well as qualitative indicators of excellence.*

All of the academic units affiliated with the Master of Science in Cybersecurity proposed program have been very productive and interdisciplinary. The USF College of Engineering, the College of the Arts and Sciences, the College of Business, and the College of Behavioral and Community Sciences generate a substantial portion of the institution's research dollars and combined produce a significant proportion of the undergraduate, masters, and doctoral graduates at USF. Over the past five years, Masters Degrees were awarded: 2,039 in the College of Arts and Sciences; 1,685 in the College of Business; 1,166 in the College of Behavioral and Community Sciences; and 1,073 in the College of Engineering. In the 2011-2012 academic year, the University granted 416 doctoral degrees. In terms of Masters Degrees, in the 2011-2012 academic

year, USF granted 2,717 M.S. degrees. The enrollment and graduation trends at USF have been very positive over the last few years.

X. *Non-Faculty Resources*

A. *Describe library resources currently available to implement and/or sustain the proposed program through Year 5. Provide the total number of volumes and serials available in this discipline and related fields. List major journals that are available to the university's students. Include a signed statement from the Library Director that this subsection and subsection B have been reviewed and approved.*

Library resources that are currently available are abundant, and the university maintains subscriptions to databases, sources, journals, and other materials required for research and education within the proposed program, such as JSTOR, ProQuest, ScienceDirect, Business Source Premier, Academic Search Premier, Biotechnology, International Journal of Geographical Information Science, Computers & Security, IEEE Transactions on Dependable and Secure Computing, IEE Transactions on Information Forensics and Security, Security Technology Executive, Computer Law & Security Report, ACM Transactions on Computer Systems, Journal of Information Science, Computing and Control Engineering Journal, Systems Engineering, Wireless Networks, Structural Health Monitoring, The American Journal of Psychology, and many others. As the entire program is online and the library's holdings are accessible online, there are no additional costs for resources anticipated.

B. *Describe additional library resources that are needed to implement and/or sustain the program through Year 5. Include projected costs of additional library resources in Table 3 in Appendix A.*

There are no additional library resources that would be necessary to sustain a Master of Science in Cybersecurity program because the collections of the USF Tampa Library and affiliates are sufficient in supporting research. Sufficiency of these resources is preserved because the USF Tampa Library maintains recurring collections and purchases new published materials annually. Since the library already provides support for the Computer Science, Information Systems, and Engineering departments, no additional library resources are necessary to support the Master of Science in Cybersecurity program at USF.

_____   _____
Signature of Library Dean   **Date**

C. *Describe classroom, teaching laboratory, research laboratory, office, and other types of space that are necessary and currently available to implement the proposed program through Year 5.*

Given that the program will deliver a significant portion of the content online, the requirement for space is significantly minimized.

D. *Describe additional classroom, teaching laboratory, research laboratory, office, and other space needed to implement and/or maintain the proposed program through Year 5. Include any projected Instruction and Research (I&R) costs of additional space in Table 2 in Appendix A. Do not include costs for new construction because that information should be provided in response to X (J) below.*

None needed.

E. *Describe specialized equipment that is currently available to implement the proposed program through Year 5. Focus primarily on instructional and research requirements.*

The university provides technology support for both research and teaching. Research technology support comes from the Advanced Visualization Center at the University, and the research computing group at USF IT. Education technology support comes from the virtualized technology lab infrastructure developed at USF which makes hardware and licensed software available to students and faculty from a central hosted environment.

F. *Describe additional specialized equipment that will be needed to implement and/or sustain the proposed program through Year 5. Include projected costs of additional equipment in Table 2 in Appendix A.*

None needed.

G. *Describe any additional special categories of resources needed to implement the program through Year 5 (access to proprietary research facilities, specialized services, extended travel, etc.). Include projected costs of special resources in Table 2 in Appendix A.*

None needed.

H. *Describe fellowships, scholarships, and graduate assistantships to be allocated to the proposed program through Year 5. Include the projected costs in Table 2 in Appendix A.*

Not applicable.

I. *Describe currently available sites for internship and practicum experiences, if appropriate to the program. Describe plans to seek additional sites in Years 1 through 5.*

Current available sites for internships include government facilities, educational facilities at the university, and private facilities that exist within the Tampa Bay region.

J. *If a new capital expenditure for instructional or research space is required, indicate where this item appears on the university's fixed capital outlay priority list. Table 2 in Appendix A includes only Instruction and Research (I&R) costs. If non-I&R costs, such as indirect costs affecting libraries and student services, are expected to increase as a result of the program, describe and estimate those expenses in narrative form below. It is expected that high enrollment programs in particular would necessitate increased costs in non-I&R activities.*

Not applicable

COLLEGE OF BUSINESS

Manish Agrawal, Ph. D.
Associate Professor

Research Interests: Software quality, offshoring and outsourcing, e-commerce, extreme event response, social media analytics, decision fusion

Manish Agrawal teaches courses in business data communications, computer networks, information systems, the development of web applications and information. An associate professor in the Information Systems Decision Sciences Department, Agrawal was the recipient of USF's university-wide award recognizing teaching excellence in 2006. An expert in the areas of software quality, offshoring and outsourcing, and e-commerce, his research interests include extreme event response, social media analytics, decision fusion, software quality. An avid researcher, his work has been published in numerous academic journals, including *Management Science, INFORMS Journal on Computing, Journal of Management Information Systems, IEEE Transactions on Software Engineering, Decision Support Systems* and the *Journal of Organizational Computing and Electronic Commerce.* His research and teaching have been funded by the US National Science Foundation, the US Department of Justice, the Indo-US Science and Technology Forum and Sun Microsystems. Agrawal earned a PhD in information systems at SUNY Buffalo, and studied at the Indian Institute of Technology in Kanpur, India.

Education

SUNY Buffalo
Ph.D. in Information Systems   (2002)
"eCommerce sourcing: Drivers, business value and intermediation"

Master of Science, Computer Science   (coursework complete, anticipated …) Indian

Institute of Technology, Kanpur, India   (1986–1992)
Master of Technology, Electrical Engineering
Bachelor of Technology, Electrical Engineering

Professional positions
August 2008 – Present: Associate Professor, Department of Information Systems and Decision Sciences, College of Business Administration, University of South Florida
August 2002 – 2008: Assistant Professor, Department of Information Systems and Decision Sciences, College of Business Administration, University of South Florida
August 2001 – July 2002: Instructor, Department of Information Systems and Decision Sciences, College of Business Administration, University of South Florida

October 1992 – June 1997: Indian Police Service, Ministry of Home Affairs,

COLLEGE OF ENGINEERING
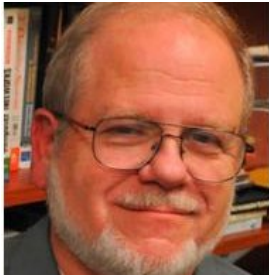
David Armitage
Former Director, Division of Information Technology, College of Engineering, Lakeland, FL

David Armitage is the former Director, Division of Information Technology, College of Engineering, Lakeland, FL, where he was responsible for overall coordination of activities of division, including course scheduling, credentialing faculty for courses, faculty evaluation and program development. Responsible for coordinating the integration of the unit and its academic programs, current and proposed, into the College of Engineering. David Armitage received his Doctor of Philosophy in Electrical Engineering from the University of Rhode Island in 1999. His dissertation is titled "On the Use of Undefined Logic Values in Digital VLSI." His research interests include the use of technology and advanced pedagogies to improve computing knowledge transfer to undergraduates, experimental application of electroencephalography to computing education, and Robotics applications.

SCHOOL OF INFORMATION

Randy Borum, Ph. D.
Professor

Research Interests: Behavior-based protocols for threat assessment, anti-terrorism training, protective intelligence, psychology of terrorism, performance under stress

Dr. Randy Borum is a Professor and Coordinator of Strategy and Information Analysis in the School of Information at the University of South Florida. He holds a joint appointment the College of Public Health and has previously served on the faculty of the College of Behavioral and Community Sciences. He regularly teaches and consults with law enforcement agencies, the Intelligence Community, and DoD, and has authored/ co- authored more than 140 professional publications. Dr. Borum has been an instructor with the BJA State & Local Anti-Terrorism Training (SLATT) Program since 1999, and worked as a Senior Consultant to the U.S. Secret Service for more than a decade helping to develop, refine and study behavior-based protocols for threat assessment and protective intelligence. He has previously served as a sworn police officer, Forensic Coordinator for a regional state psychiatric facility, and as full-time faculty at He has taught at the FBI Academy, FLETC; JFK Special Warfare Center and School (Ft. Bragg); Joint Special Operations University; CIA; and the US Army Intelligence Center and School (Ft. Huachuca). He was Principal Investigator on the "Psychology of Terrorism" initiative for an agency in the US Intelligence Community. He serves as an advisor to the FBI's Behavioral Analysis Unit-1 (Threat Assessment & National Security), the National Center for the Analysis of Violent Crime (NCAVC), the FLETC Behavioral Science Division, and is listed on the United Nations' Roster of Experts in Terrorism. Dr. Borum is a Past-President of the American Academy of Forensic Psychology, and currently serves as Senior Editor of the Journal of Strategic Security, and on the editorial boards of the American Intelligence Journal; Behavioral Sciences & the Law and Red Team Journal (online). Performance in High-Risk Encounters: Another facet of Dr, Borum's professional interest lies in improving human performance under stress, particularly in high risk and threatening encounters. In the mid-1980s he began applying principles of motor learning and behavior (and sport psychology) to enhance police officers' performance in high-risk situations, and taught courses on "Performance Under Stress" at the police academy. He has since become a Certified Sport Psychologist (National Institute of Sports Professionals), and has held NSCA certification as a Certified Strength and Conditioning Specialist (CSCS) and Copper-Level (Intro) Coaching certification with USA Wrestling. He has written a monthly sport psychology column for Black Belt Magazine, and has consulted with elite level combat sport athletes, special operations personnel in the military and law enforcement. You can find some related articles in the section titled: "Performance Psychology."

EDUCATION

NIMH Research Fellowship in Mental Health Services, Systems, and Policy Research, June, 1997
    Sponsored by the National Institute of Mental Health
    University of North Carolina - Chapel Hill & Duke University Medical Center

Post-Doctoral Fellowship in Forensic Psychology. August, 1993
    University of Massachusetts Medical Center
    Law-Psychiatry Program - Worcester, Massachusetts

Doctor of Psychology in Clinical Psychology. August, 1992
> Florida Institute of Technology, Melbourne, Florida
> APA Accredited Program
> Recipient: Outstanding Clinical Student Award.

Master of Science in Psychology. March, 1991.
> Florida Institute of Technology, Melbourne, Florida

Bachelor of Arts in Psychology. May, 1987
> Magna Cum Laude and With Distinction in Psychology
> Minors: Political Science and Criminal Justice
> James Madison University, Harrisonburg, Virginia

PROFESSIONAL EXPERIENCE

Professor – 4/2007 to Present
> Department of Mental Health Law & Policy
> Louis de la Parte Florida Mental Health Institute,
> University of South Florida, Tampa, Florida

Professor (Joint Appointment) – 4/2007 to Present
> Department of Community and Family Health
> College of Public Health,
> University of South Florida, Tampa, Florida

Associate Professor - 7/99 to 4/2007 (*Tenure Granted 5/19/2005*)
> Department of Mental Health Law & Policy
> Louis de la Parte Florida Mental Health Institute,
> University of South Florida, Tampa, Florida

Associate Professor – 3/2000 to 4/2007
> Department of Community and Family Health
> College of Public Health,
> University of South Florida, Tampa, Florida

Courtesy Professor - 12/99 to Present
> Department of Criminology
> University of South Florida, Tampa, Florida

Senior Research Scientist – 1/2000 to Present
> The James and Jennifer Harrell Center for the Study of Domestic Violence
> University of South Florida College of Public Health

Adjunct Assistant Professor of Medical Psychology 7/99 – 7/2001
> Duke University School of Medicine, Durham, N.C.
> Department of Psychiatry & Behavioral Sciences, Division of Medical Psychology

Assistant Professor of Medical Psychology – Full-time Faculty 6/95 to 6/99
> Department of Psychiatry and Behavioral Sciences
> Psychiatric Epidemiology and Health Services Research Program
> Duke University Medical Center, Durham, NC

Research Fellow - 1995-1997
UNC-Duke Post-doctoral Training Program in Mental Health Services and Systems Research

Chief Psychologist/Forensic Coordinator - 1993-1995
John Umstead Hospital, Adult Admissions Unit
Butner, North Carolina

Fellow in Forensic Psychology - 1992-1993
University of Massachusetts Medical Center
Law & Psychiatry Program, Worcester, Massachusetts

Psychology Intern - 1991-1992
James A. Haley V.A. Medical Center, Tampa, Florida (APA-Accredited)

Clinical Psychology Practica - 1989-1991
Florida Institute of Technology, Melbourne, Florida

F.I.T. Psychology Associates/Palm Bay Police Department
F.I.T. Psychology Associates
Osceola Evaluation and Treatment Center
Florida Tech Center for Student Development

Coordinator, Behavioral Science Services / Police Officer - 1989-1991
Palm Bay Police Department, Palm Bay, Florida

Police Instructor - 1989-1991
Brevard County Law Enforcement Academy, Melbourne, Florida

Outpatient Therapist - 1988
Circles of Care, Melbourne, Florida

Crisis Intervention Specialist - 1987-1988
Tidewater Psychiatric Institute, Norfolk, Virginia

Telephone Crisis Counselor/Trainer - 1985-1987
Listening Ear Services (CSB), Harrisonburg, Virginia

Seasonal Police Officer - 1986
Ocean City Police Department, Ocean City, Maryland

Police Cadet - 1985-1986
James Madison University Police Department, Virginia

COLLEGE OF BEHAVIORAL AND COMMUNITY SCIENCES

R. LeGrande Gardner, PhD, CFCE, CEDS, ACE
Department of Criminology
University of South Florida in Lakeland
Lakeland Technology Building (LTB)
3433 Winter Lake Road
Lakeland, Florida 33803-9807
863-667-7822 (office)

GRADUATE EDUCATION

Virginia Polytechnic Institute and State University, Blacksburg, VA
Ph.D. Degree in Sociology with a Criminology Specialization, December 1984.
Dissertation: *Social Bonding And Juvenile Delinquency: A Multivariate Analysis*

Georgia Southern University, Statesboro, GA
M.A. Degree in Sociology with a Research Methodology Specialization, August 1981

CURRENT ACADEMIC AND PROFESSIONAL EXPERIENCE

University of South Florida, May 2007 to present

- **Instructor**, June 2012 to present.
  Department of Criminology, University of South Florida in Lakeland, Florida.

  Develop and teach undergraduate courses in Law Enforcement Systems, Criminal Justice Administration, Ethics for Criminal Justice Professionals, Controversies in Criminal Justice, Criminal Investigations, and Race and Ethnic Relations.

- **Instructor/Director, USFP Digital Forensics Laboratory**, May 2011 to June 2012.
  University of South Florida Polytechnic, College of Applied Arts and Sciences, Criminology Department, Lakeland, Florida

  Developed and taught undergraduate courses in Digital Forensics, Introduction to Digital Evidence, Digital Forensic Examinations for the Criminal Investigator, Law Enforcement Systems, Criminal Justice Administration, Criminal Investigations, Ethics

2

for Criminal Justice Professionals, Controversies in Criminal Justice, and Race and Ethnic Relations. USFP ceased to exist effective July 1, 2012 in accordance with Florida Senate Bill 1994.

- **Adjunct Instructor**, May 2007 to May 2011
  University of South Florida Polytechnic, College of Applied Arts and Sciences, Criminology Department, Lakeland, Florida

  Developed and taught undergraduate courses in Criminal Investigations, Ethics for Criminal Justice Professionals, Juvenile Justice, Controversies in Criminal Justice, Criminal Justice Administration, American Law Enforcement Systems, and Race and Ethnic Relations. Developed and taught graduate level courses in Contemporary Issues in Law Enforcement and Theory, Research, and Practice in Law Enforcement.

Owner and Forensic Examiner, August 2011 to present
LeGrande PLLC, E-Discovery and Digital Forensic Specialists, Lakeland, Florida

LeGrande PLLC is a digital forensics firm serving Tampa Bay and Central Florida. We primarily provide digital forensics and E-Discovery services in support of civil litigation, corporate investigations, and private investigations. Our team is entirely comprised of skilled, experienced, and certified digital forensics examiners with prior sworn law enforcement investigative experience. FL LIC# A1100170

Instructor/Course Development, January 2006 to present
Web Investigator Inc., Vancouver, British Columbia

Web Investigator Inc. is a Canadian-based technology security firm that provides specialized courses in Internet investigations to government, business, and private entities worldwide. I have developed and teach an online course in Cyber Criminology through Web Investigator Inc.

Adjunct Faculty/Course Development, January 1993 to present
Saint Leo University, Center for Adult Education (formally Distance Learning), Saint Leo, Florida

I teach and facilitate courses in the graduate and undergraduate Criminology and Sociology programs to include: Criminal Investigations, Information Technology for Criminal Justice, Cyber Crime, Criminal Theory, Criminal Typologies, Drugs and Society, Prosecution and Adjudication, Law of Criminal Procedure, Criminal Justice Systems, Police Systems, Correctional Systems, Juvenile Justice Systems, Juvenile Delinquency, Social Problems, Senior Seminar (Capstone), and others in the fields of Criminology, Sociology, Criminal Justice and Criminal Law.

Saint Leo University, Center for Online Learning, San Antonio, Florida

I teach and facilitate courses in the online Criminology program to include Criminal Investigations, Criminal Typologies, Survey of the Criminal Justice System, Social Problems, Ethics for Criminal Justice Practitioners, Juvenile Justice, Correctional Systems, Cyber Crime, and the Senior Capstone Course. I have developed courses for the online program in many areas to include Cyber Crime, Criminal Typologies, and Ethics for Criminal Justice Practitioners, which have included lectures, study guides, instructional videos and other course materials.

IACIS Coach, July 2005 to present
International Association of Computer Investigative Specialists (IACIS)

I serve as a Coach and advisor to law enforcement officers in both the U.S. and European Sessions who are going through the IACIS examination process to become Certified Computer Forensic Examiners (CFCE). Committee service also.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

Jay Ligatti, Ph. D.
Associate Professor

Research Interests: Software security and programming languages, software monitoring, language-based security and reliability, security automata, type systems

Jay Ligatti received a Ph.D. in Computer Science from Princeton University (2006) and a B.S. in Computer Science and B.M. in Music Composition from the University of South Carolina (2001). Dr. Ligatti's current research projects include: Theory and practice of security-policy composition, theory and practice of monitoring software at runtime, principled definition and analysis of code injections, and proving the completeness of subtyping relations. Dr. Ligatti teaches Foundations of Software

Research Interests

Software security and programming languages, including runtime monitoring, enforcement models, policy-specification languages, code-injection attacks, firewalls and packet-classification algorithms, type systems, and tools for building and managing complex security policies.

Appointments
University of South Florida
Associate Professor, Department of Computer Science and Engineering (2012-present)
Assistant Professor, Department of Computer Science and Engineering (2006-2012)

Education

Princeton University (2001-2006)

Degrees: Ph.D., Computer Science (2006); M.A., Computer Science (2003)

Dissertation: Policy Enforcement via Program Monitoring

Adviser: David Walker

University of South Carolina (1997-2001)

Degrees: B.S., Computer Science (2001); B.M., Music Composition (2001)

Honors project: Scis te id plurimum amare: A thoroughly recursive piece
Adviser: Reginald Bain