BACCALAUREATE PROPOSAL APPLICATION
Form No. BAAC-02

Section 1007.33(5)(d), Florida Statutes, and Rule 6A-14.095, F.A.C., outline the requirements for a Florida College System baccalaureate program proposal. The completed Proposal form shall by submitted by the college president to the Chancellor of the Florida College System at ChancellorFCS@fldoe.org. In addition, a printed version shall be mailed to the Division of Florida Colleges at 325 West Gaines Street, Suite 1544, Tallahassee, Florida 32399-0400.

The proposal requires completion of the following components:

- Program summary
- Program description
- Workforce demand and unmet need
- Planning process
- Enrollment projections and funding requirements
- Student costs: tuition and fees
- Program implementation timeline
- Facilities and equipment specific to program area
- Library and media specific to program area
- Academic content
- Program termination
- Appendix tables
- Supplemental materials

Florida College System Institution Name: St. Petersburg College (SPC)
Florida College System Institution President: Dr. Tonjua Williams

PROGRAM SUMMARY

1.1	Program Name:	Cybersecurity	
1.2	Degree type:	☐ Bachelor of Science	✖ Bachelor of Applied Science
1.4	How will the program be delivered (check all that apply):	Face-to-face **X** Hybrid	Online only
1.5	List the counties in the college's service district:	Pinellas County	
1.6	Degree CIP code (6 digit):	11-1003	
1.7	Anticipated program implementation date:	August 1, 2020	
1.8	What is the primary associate degree pathway for admission to the program?	Associate of Science Degrees in: • Cybersecurity • Digital Forensics and Computer Investigations • Computer Networking • Computer Information Technology	
1.9	Is the degree a STEM focus area?	**X** Yes	☐ No
	List program concentration(s) (if applicable):	Cybersecurity Defense and Risk Mitigation	
1.10	Will the program be designated such that an eligible student will be able to complete the program for a total cost of no more than $10,000 in tuition and fees?	☐ Yes	☒ No

PROGRAM DESCRIPTION

2.1 Describe the program.

Security has long been an important element of information technology and systems. More recently however, cyber security has emerged as a separate and distinct discipline that covers multiple domains including physical security of computing resources, data loss prevention, security policy administration, vulnerability assessment, compliance, risk mitigation, and cyber defense.

In addition, organizations from every sector of the world economy have recognized the urgency of securing information resources. These same organizations have also recognized the tremendous gap between the need for security professionals and the available pool of qualified individuals. This program addresses this gap.

The Bachelor of Applied Science in Cybersecurity is a professional workforce degree program that focuses on technologies and practices designed to protect information

and physical resources such as computers, networks, programs and data from damage or unauthorized access. In a computing framework the term security indicates cybersecurity. This degree will offer Pinellas County residents the opportunity to earn a Bachelor of Applied Science in Cybersecurity, a degree that compliments the traditional workforce emphasis on baccalaureate programs in state colleges and will offer the opportunity for two-year graduates of St Petersburg College's cybersecurity and forensics A.S. degrees to move into leadership roles and/or to further their education in cybersecurity master's degree programs and certificates throughout the state. The program will also afford students the opportunity to demonstrate their technical career skills by obtaining higher-level security industry certifications.

The program has been designed to include a core set of foundational courses and an initial sub plan sequence called Defense and Risk Mitigation. This modular approach will enable the rapid development of future sub plans as workforce needs dictate.

This program provides an articulation path for those who complete the existing Associates Degree program to continue developing their academic careers through focused study of cyber security concepts, by gaining experience with additional security tools, and sitting for additional industry certification exams.

The Associates Degree program at SPC was recently designated a National Center of Excellence in Cyber Defense Education (see Exhibit L – page 186). The National Security Agency (NSA) and the Department of Homeland Security have designated St. Petersburg College as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) through the academic year 2024. This designation recognizes the college's contribution to meet the demands to provide a highly skilled cybersecurity workforce.

SPC is the fourth state college in Florida to receive the two-year designation for the Cybersecurity Associate in Science degree. SPC's Cybersecurity Associate in Science degree and the proposed Bachelor's degree program address the critical shortage of professionals with cybersecurity skills.

WORKFORCE DEMAND AND UNMET NEED

3.1 Describe the career path and potential employment opportunities for graduates of the program.

This BAS degree program will build upon students' core knowledge in cyber security and technical areas such as computer networking, digital forensics, and computer security with an upper division curriculum focusing on information security, risk assessment and mitigation compliance, disaster planning and recovery, advanced forensics, information assurance, and defense against cyber-

attack.

This proposed BAS degree in Cybersecurity would prepare students for a 'real world' experience as the program would align with multiple industry certifications related to cybersecurity and technology. Industry certifications validate a student's skills and knowledge in a specific area of study and are awarded by a professional group or a vendor. In many cases these require periodic renewal and therefore aligning curriculum to industry certifications is a way of keeping the curriculum current with technical workforce skills and practices. Industry certifications under consideration include, but are not limited to, CompTIA Pentest+, CySA+, Cloud+, (ISC)2 Certified Cloud Security Professional, and EC-Council Computer Hacking Forensic Investigator.

Graduates of this proposed BAS program would be prepared for jobs that align with the NICE Cybersecurity Workforce Framework. These jobs include Systems Security Analyst, Security Control Assessor, Vulnerability Assessment Analyst, Cyber Defense Analyst, and Security Architect. Other potential roles include senior positions such as Information Security Officer, Director Information Security, Chief Information Security Officer, and Principle Cybersecurity Practice Manager. These individuals need to best understand the evolving issues in the field of cybersecurity and are directly responsible for providing opportunities for sustainable employment in the workplace.

3.2 Describe the workforce demand, supply, and unmet need for graduates of the program that incorporates, at a minimum, the shaded information from appendix tables A.1.1 to A.1.3.

Security is a complex and growing field that has emerged as its own discipline. CompTIA's Trends in Information Security study that included insights from nearly 1,000 business and technology professionals, confirms that cybersecurity is moving away from being an embedded function under IT in many organizations. And this study cites data from the Bureau of Labor Statistics that predicts that Information Security Analysts (SOC 15-1122) will be the fastest growing job category, with about 37% overall growth through 2022 https://www.comptia.org/resources/trends-in-information-security-study.

Cybersecurity Ventures has reviewed and synthesized employment figures from multiple sources and estimates that there will be 3.5 million unfilled cybersecurity positions globally by 2021 https://cybersecurityventures.com/jobs/.

According to Cyberseek, there are currently 313,735 cybersecurity job openings in the nation. And there are 13,465 cybersecurity job openings in Florida alone

as of August 2019. Cyberseek further reports that 4,275 of those jobs are actually in the Tampa-St. Petersburg-Clearwater area https://www.cyberseek.org/heatmap.html.

These studies demonstrate that there is unmet need in the workforce globally, nationally, regionally, and most importantly, locally.

The Tampa Bay Technology Task Force (TBTF) in a 2015 Tampa Bay IT Workforce Analysis study reported the Economic Modeling Specialists, Inc. (EMSI) projections for Information Security Analysts (SOC 15-1122) alone will see a double digit growth 2015-2020 http://tampabaygapanalysis.com/it.html.

According to Cyberseek projected salaries for a sampling of cybersecurity roles are:

- Cybersecurity Specialist $75,000
- Incident Analyst $99,000
- Cybersecurity Analyst $85,000
- Penetration Tester $102,000
- Cybersecurity Manager $115,000
- Cybersecurity Architect $129,000

https://www.cyberseek.org/pathway.html.

The data gathered for Appendix Table A.1.1, A.1.1.2, and A.1.3 for the number of cybersecurity-related employment statistics represents county and region data from the Bureau Labor of Statistics and Florida Department of Economic Opportunity (DEO) labor statistics for the base year 2018 to the projected year 2026. Data from the EMSI Q1 2019 region report is included in this analysis.

Employment, meaning the number of jobs, for the job classification of Information Security Analysts (SOC 15-1122) is reported by the Florida DEO as 357 for the base year with a projection of 452 for the projected year. This represents 26.6% growth in this key, targeted job classification. The number of total job openings for Information Security Analysts is 310 or an average of 39 jobs per year over the eight year period from the base year to the projected year. The median hourly wage for this position is $39.90. For this same SOC code the EMSI Q1 2019 data for the Pinellas area reports 359 jobs in the base year and 428 in the projected year. The total number of openings in this data is reported to be 100 with an average hourly wage of $37.28. A Bachelor's degree is the recommended education level for this position.

Current cyber security programs are not providing enough graduates to meet the need even in this specific job classification. The University of Tampa has introduced a relatively new program and has graduated a total of 29 over the

past two years.

Florida's DEO employment data for the cluster of Computer Network Specialists (SOC 15-1152), Network & Computer System Administrators (SOC 15-1142) and Computer Network Architects (SOC 15-1143) reports the number of jobs to be 3,307 in the base year, 3,677 in the projected year, and total of job openings of 271 or an average of 34 jobs per year through the projected year of 2026.

The average hourly wage of for these three classifications is $35.22. A Bachelor's degree is recommended for SOC 15-1142 and SOC 15-1143.

The EMSI Q1 report lists data for SOC 15-1152 and shows 710 jobs in the base year and 745 in the projected year with 5 total openings. The average hourly wage is $26.76 and an Associate degree is the recommended education level. An Associate degree is sufficient for SOC 15-1152 primarily because the network specialist is typically a junior or entry level position. Some businesses use this position as a gateway job for those on a cybersecurity career path.

This cluster of network related positions is appropriately considered here because networking and cybersecurity are closely related and because cybersecurity graduates may begin their security careers in a network-related position.

The job title of Computer Systems Analyst (SOC 15-1121) is included in the EMSI data for the same reason. This position represents a potential entry point for those seeking a career in cyber security. The EMSI data shows 1,484 jobs in this classification for the base year and 1,609 in the projected year. The average hourly wage is $33.75 and a Bachelor's degree is recommended.

Computer and Information Systems Managers (SOC 11-3021) and Database Administrators (SOC 15-1141) are similarly considered because an understanding and working knowledge of security is essential for success in these positions. Florida DOE data for SOC 11-3021 shows 834 jobs in the base year, 955 in the projected year, and total job openings 637 or 80 job openings per year on average. The average hourly wage for a Computer and Information Systems Manager is $60.25 and a Bachelor's degree is the recommended educational level.

The EMSI Q1 data for SOC 11-30321 reports 1,024 job in the base year, 1,175 in the projected year with a total of 84 job openings. The average wage is shown as $53.27 per hour and the recommended educational level is a Bachelor's degree. This is consistent with the DEO data and supports the need for additional qualified graduates.

The demand for Database Administrators (SOC 15- 1141) is strong as well. The Florida DOE identifies 542 jobs for Database Administrators in the base year, growing to 628 in 2026. The total number of job openings is expected to be 379 or 47 per year. Database Administrators can expect to earn $41.74 per hour. This position requires a Bachelor's degree.

EMSI data reflects these trends as well. This data source shows 468 jobs in the base year and 500 in the projected year. The total number of job openings is 53. Once again a Bachelor's degree is recommended for those who aspire to this position.

This occupational data demonstrates the need for additional Bachelor's degree graduates to satisfy the employment demands of the workforce. Based on the Florida DOE data alone there are projected to be 437 job openings per year in the positions identified.

The University of Tampa offers a relatively new Bachelor's degree in Cybersecurity and has produced 29 graduates in the past two years. While these graduates do help to address the demand for cybersecurity professionals, employment in the cybersecurity field is projected to steadily increase in a majority of occupations correlated to the proposed BAS Cybersecurity program. The current supply of qualified graduates is not sufficient to meet the demand.

3.3 Describe any other evidence of workforce demand and unmet need for graduates as selected by the institution, which may include qualitative or quantitative data information, such as local economic development initiatives, emerging industries in the area or evidence of rapid growth, not reflected in the data presented in appendix tables A.1.1 to A.1.3. For proposed programs without a listed SOC linkage, provide a rationale for the identified SOC code(s).

Cybercrime costs the U.S. approximately $2 trillion per year, with some estimates as high $3 trillion through 2021 https://www.forbes.com/site/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#25f928eb3a91.

The Tampa Bay of region of Florida ranks as the states leading tech hub (http://www.tampabay.com/news/business/stem-jobs-tampa-bay=leads-florida-but-can-it-become-a-bigger-tech-player/2248874), and is home to 19 global corporate headquarters, four major military installations, and thousands of corporations and infrastructure agencies, all of which are vulnerable to cyberattack.

A recent report lists the Tampa Bay metro area as the 10th most cyber-insecure

community in the U.S. due in part to the large presence of defense and financial service firms, as well as an above average aging population https://www.bizjournals.com/tampabay/news/2018/05/22/where-tampa-ranks-among-the-cities-most-vulnerable.html.

Beyond financial and technology institutions, societal infrastructure systems such as public safety, transportation, and medical facilities also face their own weaknesses related to cyberterrorism and hacking. These agencies must be able to weather cyber threats as well. Former U.S. Secretary of Defense Leon Panetta has warned that a cyber-Pearl Harbor, in which extremist groups take over public networks to cause mass destruction may be only a matter of time http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html.

A well-prepared workforce is vital to meet these encroaching threats. Not only must cybersecurity employees understand the nature of the job, they must also remain flexible and keep their training up to speed in a rapidly-evolving field. The U.S. Department of Labor designates Florida as the fourth-largest cyber employment market behind only California, Virginia, and Texas (http://www.careerinfonet.org) and projects a 28% increase in employment of information security analysts through 2026 (https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6).

A Florida Center for Cybersecurity report states: “Even when compared with other high-demand IT jobs, demand for cybersecurity jobs (in Tampa Bay) is growing more than three times faster. Business leaders say they can’t hire skilled cybersecurity workers fast enough.” https://www.usf.edu/pdfs/final-cybersecurity-report.pdf.

As previously cited, experts have also noted a global shortage of cybersecurity skills. It’s estimated that the current global job market will have more than 3.5 million job openings for cybersecurity professionals by 2021 (www.aami-bit.org/doi/10.2345/0899-8205-50.5.381), with some fields showing a ratio as high as 3:1 of job openings to qualified applicants (https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6).

3.4 If the education level for the occupation identified by the Florida Department of Economic Opportunity presented in appendix table A.1.1 is below a bachelor’s degree, provide justification for the inclusion of that occupation in the analysis.

SOC 15-1152 was included in the data because as an emerging discipline not all companies have created entry level positions for cybersecurity professionals.

Network support roles are often the first stop for those who aspire to cybersecurity positions. This is often considered a gateway position that provides individuals an opportunity to gain experience within a company that views network support as a starting point for a cybersecurity career path.

PLANNING PROCESS

4.1 Summarize the internal planning process.

7-17-18	Meeting Dean Stewart of CCIT, John Duff of CCIT, and Katie Schultz to discuss grant opportunities to fund additional cyber security programs in response to the critical need for cybersecurity professionals as voiced repeatedly by the CCIT Business Advisory Council and as evident in industry trends
8-6-18	Meeting to discuss DOE Pilot Program Cybersecurity grant opportunity with Dean Stewart, Katie Schultz, and John Duff
8-8-18	DOE Cybersecurity Grant planning discussion with CCIT and Grants to plan what St. Petersburg College should propose in response to the DOE grant opportunity. SPC determines to propose using grant funds to develop a new cybersecurity BAS degree program.
8-10-18	Meeting – John Duff of CCIT and Jennifer McBride, Grant Writer to craft response to the DOE program opportunity
8-15-18	Meeting with Vice President of Academics Dr. Anne Cooper to discuss development of a new BAS program in Cybersecurity and to submit a proposal in response to the DOE grant opportunity to fund the effort. Structure of new degree program to be a core set of courses with multiple sub plans available over time
8-15-18	Meeting with CCIT programming faculty to discuss the need for a software assurance sub plan that would be part of new course development
8-18-18	Grant Department and CCIT personnel meet to discuss and review grant application
8-20-18	Letters of support requested from CCIT Advisory Committee members and local cybersecurity professionals

8-18-18	Grant formally submitted to Grants.gov for the DOE Pilot Program in Cybersecurity Education Technological Upgrades (Page 34)
9-12-18	CCIT Advisory Committee meeting that includes discussion of new programming planned and grant opportunity
9-28-18	Grant Award notification received by John Duff of CCIT (Page 114)
10-2-18	Registration on government G5 site to administer grant
10-12-18	Post award call with DOE to confirm grant logistics etc.
10-17-18	DOE Grant Kick-off meeting to discuss program implementation
11-26-18	CCIT meeting with Curriculum and Instruction to review state frameworks and to coordinate plans for development of new program and courses to be added through Curricunet
1-10-19	Planning meeting with Tina Fischer of the SPC Collaborative Lab to discuss format for DACUM with local cybersecurity professionals
1-29-19	The purpose of the DACUM (Page 116) was to elicit input from industry subject matter experts that would inform and direct the development of a new Bachelors of Applied Science program in Cybersecurity. A group of senior, cybersecurity professionals participated in the event. This group included representatives from local employers including KnowBe4, CITI, Honeywell, AMGEN, the City of St. Petersburg, the City of Largo, JPMorgan Chase, the Dellbridge Group, PSCU, and Sofia. During this facilitated session the group was asked to identify and prioritize specializations and core knowledge that graduates of a BAS program should study and understand in order to be ready for employment in cybersecurity related positions. The group was also asked to identify specific work roles as described in the NICE (National Institute for Cybersecurity Education) Cybersecurity Workforce Framework. The group identified and prioritized five NICE work roles. There were: Security Systems Analyst, Security Control Assessor, Vulnerability Assessment Analyst, Cyber Defense Analyst, and Security Architect. The curriculum development team is using this information as the basis for program and course development. A real time record of the DACUM is attached to this document as Appendix C.
2-14-19	CCIT faculty created an initial draft of new degree created based on input from the DACUM and shared with DACUM attendees for

comment. The faculty identifies an opportunity to develop an initial sub plan that could be offered within the existing Tech-Mgt BAS program should the new BAS proposal be denied. This sub plan to be titled Defense and Risk Mitigation. This strategy enables the faculty to begin course development while the formal BAS proposal process commences. Once state approval is received, the new sub plan would be migrated to the new BAS program. This reduces cycle time for development as the initial sub plan can be approved internally while approval for the BAS degree is pending.

2-22-19	Draft Letter of Intent created (Page 150)
3-19-19	Board of Trustee approves initiation of new BAS proposal (minutes attached) (Page 147)
3-25-19	CCIT Faculty assigned responsibility for new sub plan course development.
5-22-19	CCIT Faculty DACUM to identify the complete cybersecurity curriculum. This session was attended by Dr. John Sands who provided consultative support from the National Center for Systems Security and Information Assurance located at Moraine Valley Community College. The outcome is detailed in section 10.11 below.
5-30-19	New sub plan submitted to Curricunet for Review.
7-27-19	Comment period ends
9-25-19	Proposal submitted to State

4.2 Summarize the external planning process.

10-12-18	Review of grant award and discussion of next steps with Dr. John Sands of the National Center for Systems Security and Information Assurance (CSSIA) located at Moraine Valley Community College in Illinois
10-19-18	Discussion of resources available through CSSIA Center
11-1-18	Consultative support with Dr. John Sands – discussion of curriculum resources available
12-3-18	Review/Discussion of DACUM structure and format with CCIT Advisory Committee members

12-4-18	Review and comment on DACUM invitee list with CSSIA and CCIT Advisory Committee
12-5-18	Discussion of training resources available via CSSIA to support faculty development and new course development
1-16-19	CTF discussion regarding resources available at CSSIA (includes discussion with D. Durkee)
1-17-19	Meeting with CSSIA re: NICE resources available for curriculum and workforce mapping
2-8-19	Results of DACUM circulated to attendees for comment and feedback
4-24-19	Dr. Stewart attends CAE ELF conference in Pensacola and meets with other educational leaders to discuss cybersecurity needs
4-25-19	Consultative discussion with CSSIA to discuss resources available to support capture the flag and other virtual lab capabilities

4.3 List engagement activities; this list shall include APPRiSe, meetings, and other forms of communication among institutional leadership regarding evidence of need, demand, and economic impact.

	Date(s)	Institution	Description of activity
APPRiSe	March 2019	St. Petergburg College	St. Petersburg College submitted electronic APPRiSe notification
Public universities in college's service district	October 2018 February 2019 April 2019 May 2019 May 2019	University of South Florida	Attended & Presented at Florida Cyber Conference Sponsored by USF Dr. Williams meets with Dr. Judy Genshaft of USF – no concerns with SPC pursuing BAS in Cybersecurity Letter of Support Attached (Page 188) Attended Research Symposium at USF Discussed resources available via the cyber range at USF Letter of intent Review and Comment (Page 183)

Regionally accredited institutions in the college's service District	October 2018		Participated along with the University of Tampa (UT) in a Capture the Flag Competition at Raymond James. The proposed program would be significantly different than the program available at UT. The University of Tampa (UT) is a private institution that offers a Cybersecurity major within the College of Business. The program requires 24 hours of core courses. In both programs students may select several electives.
Eckerd College			Eckerd College does not offer a competing degree program

ENROLLMENT PROJECTIONS AND FUNDING REQUIREMENTS

5.1 Provide a brief explanation of the sources and amounts of revenue that will be used to start the program.

The development of this new BAS program is being funded by a grant from the Department of Education (DOE). SPC was awarded a total of $83,450 to support the development of new cyber security programming through the DOE Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges. This was a two year award and budgeted as follows:

Category	Year 1	Year 2	Total	Description
Personnel				
Deliverable Pay: Program Management	$ 2,613	$ 2,613	$ 5,225	Estimating 1 faculty/staff @ $1306.25 per deliverable x 2 deliverables per year to support program oversight including communicate with funder and partners, project management, reporting, budget management and program evaluation.
Deliverable Pay: Course Development	$ 10,450	$ 13,063	$ 23,513	Estimating $2,612.50 per faculty per course (2 deliverables @ $1,306.25 each) at institutional rate for upper level B.A.S course development for 4 courses developed in Year 1 and 5 courses in Year 2.
Total Expenses				
Total Personnel	$ 13,063	$ 15,675	$ 28,738	
Fringe	$ 2,090	$ 2,508	$ 4 ,598	Fringe for deliverable pay @ 16% includes Medicare 1.45%; Social Security 6.2%; Retirement 7.92%

Travel	$ 6,637	$ 6,607	$ 13,244	Conference, Workshop & Professional Development Travel - Estimating 2-3 trips per year for 2-3 staff to attend National Conferences and related training/professional development such as CompTIA Partner Summit + CompTIA Instructor Network Training Sessions, Community College Cyber Summit (3CS), the National Initiative for Cybersecurity Education (NICE) Conference, etc. Estimating $1,500 per person per trip to include airfare, hotel, registration, ground transportation, per diem, etc. Estimating Year 1 at $6,637 and Year 2: $6,607. Total $13,244
Equipment	$ 9,700	$ -	$ 9 ,700	Estimating cost of new server to provide an expanded platform for delivering virtual cybersecurity labs, allowing for the inclusion of additional curriculum such as that from Palo Alto as part of the Cybersecurity Academy and/or others. Estimating cost of server at $9,700.
Supplies	$ -	$ -	$ -	
Contractual	$ -	$ -	$ -	
Construction	$ -	$ -	$ -	
Other: Printing and Publicat	$ 2,000	$ 1,500	$ 3,500	Estimating cost for the design, publication and distribution of program materials such as brochures and advisements, online resources, website upgrades, etc. Primary production will take place in Year 1 after redesign of new Cybersecurity subplans/courses. Estimating $2,000 in Year 1 and $1,500 in Year 2.
Other: Consultant	$ 5,000	$ 5,000	$ 10,000	Estimating cost for Subject Matter Expertise provided through partner NSF ATE Center(s). Estimating all- inclusive hourly rate @ $50 per hour x 100 hours per year for consolations and support on curriculum alignment, workforce engagement, faculty development, etc.
Other: Faculty Development	$ 4,194	$ 2,097	$ 6 ,291	Estimating cost of Industry Certification Test Vouchers for certification required to teach newly developed courses (CISSP, SSCP, CCSP, etc.). Estimating 2 faculty receiving 3 additional certifications in Year 1 x $1500 per person = $3,000. Estimating 1 faculty in Year 2 @ $1,500. Estimating cost of Certification Prep Course and related professional development courses through ATE partner(s) at $199 per 1 week online course x 3 courses x 2 faculty in Year 1. Year 1 @ $1,194. Estimating 1 faculty in Year 2 @ $597.
Other: Facilitation	$ 2,000	$ -	$ 2 ,000	Estimating cost of hosting a Develop A Curriculum Meeting (DACUM). Estimating cost of half-day facilitated interactive session involving subject matter experts in the field of Cybersecurity and business leaders to support curriculum development, industry certification alignment, etc.
Subtotal	$ 44,684	$ 33,387	$ 78,071	
Indirect Costs	$ 2,799	$ 2,671	$ 5 ,470	8% of SPC's federally negotiated modified indirect cost rate with U.S. Health and Human Services (33% on-campus, less equipment and contracts over $25,000 and student support costs)
Total Costs	**$ 47,482**	**$ 36,058**	**$ 83,540**	

The program will be funded through tuition and fees, state and local dollars going forward.

5.2 Provide a narrative justifying the estimated and projected program enrollments, outcomes, revenues and expenditures as they appear in Appendix Table A.2.

Enrollment projections are based on 50 students in year one (16 FTEs) beginning in August of 2020, and increasing to 250 first time students (184 FTEs) by 2023 the fourth year of the program and 575 in total enrolled students by year four (See Appendix Table A.2).

These enrollment projections are conservatively based on enrollment data in the existing Technology Management BAS program. That program has averaged 224 new, incoming students per year. Of those students an average of 47% select the existing cybersecurity sub plan as their area of focus. This demonstrates a keen awareness of the opportunities in cybersecurity and provides a basis for projecting future enrollment in a BAS program that addresses cybersecurity in greater depth.

The proposed program will be substantially online and therefore will build on the existing infrastructure with minimal increase in costs. In addition, program development will be funded by a grant from the Department of Education totally $83,540. Revenue from student tuition is expected to be $1,295,712 for the 4-year start-up period. The program will be self-sustaining.

STUDENT COSTS: TUITION AND FEES

6.1 Anticipated cost for a baccalaureate degree (tuition and fees for lower and upper division credit hours) at the proposing FCS institution (tuition and fees x credit hours).

	Cost per credit hour			Number of credit hours		Total cost
Tuition & Fees for lower division:	$111.75	**X**	Credit hours	60	**=**	$6,705
Tuition & Fees for upper division:	$122.70	**X**	Credit hours	60	**=**	$7,362
Tuition & Fees (Total):	$	**X**	Credit hours	120	**=**	$14,067

6.2 Estimated cost for a baccalaureate degree (tuition and fees) at each state university in the college's service district.

Institution Name: University of South Florida

Tuition & Fees:	$211.19	**X**	Credit hours	120	**=**	$25,342

6.3 Estimated cost for a baccalaureate degree (tuition and fees) at each nonpublic institution in the college's service district (if available)*

Institution Name: University of Tampa

Tuition & Fees:	$596	**X**	Credit hours	120	=	$71,520

Institution Name: Eckerd College**

Tuition & Fees:	$45,452	**X**	Years	4	=	$181,808

**Annual Tuition Costs

Note. *If the institution does not provide the tuition cost per credit hour, please provide the cost information provided on the institution's website.

PROGRAM IMPLEMENTATION TIMELINE

7.1	APPRiSe notice:	March 20, 2019
7.2	Board of Trustees approval:	March 19, 2019
7.3	Notice of Intent:	April 3, 2019
7.4	Completed proposal submission:	August 30, 2019
7.5	Targeted State Board of Education consideration:	January 15,2020
7.6	Targeted SACSCOC approval (if applicable):	April 2020
7.7	Targeted initial teacher preparation program	N/A

Approval (if applicable):

7.8 Targeted date upper division courses are to begin: August 15, 2020

FACILIITES AND EQUIPMENT SPECIFIC TO PROGRAM AREA

8.1 Describe the existing facilities and equipment that will be utilized for the program.

The proposed program will leverage existing infrastructure and equipment. The DOE grant provides funding for a new server that will host virtual labs from vendors such as Palo Alto in support of the program. The existing cyber lab consisting of 16 computers will be available to the students enrolled in the program even though the program will be delivered substantially online. A computing lab is available to students at each of the main SPC campus locations including Tarpon Springs, Seminole, Gibbs, Midtown, and Downtown.

8.2 Describe the new facilities and equipment that will be needed for the program (if applicable).

The program will require a new Dell server that is funded by a DOE grant. This server will support the delivery of virtual labs and will also be used to host capture-the-flag and other cyber competitions at SPC.

The server is a high performance DELL PowerEdge R740 with an Intel® Xeon® Gold 5117 2.0G, 14C/28T, 10.4GT/s, 19.25M Cache, Turbo, HT (105W) DDR4-2400 processor, 5 1.8TB 10K RPM SAS 12Gbps 512e 2.5in Hot-plug Hard Drives, with a H330 RAID controller, and a 3 year warranty. It is capable of hosting multiple virtual machines that will support the proposed and future programs.

LIBRARY AND MEDIA SPECIFIC TO PROGRAM AREA

9.1 Describe the existing library and media resources that will be utilized for the program.

The College's current library's electronic book holdings and subscriptions to electronic technology databases are adequate to support the proposed program. The library provides access to many research databases relevant to cybersecurity. These databases include journal and news articles, ebooks, conference proceedings and streamed content from thousands of

sources which are accessible to students from any Internet connected computer on a 24 hour/7 day per week basis.

Databases include:

Research Starter – Cybersecurity Salem Press Encyclopedia

Academic Search Complete – Designed specifically for academic institutions, is the world's most valuable and comprehensive scholarly, multi-disciplinary full-text database, with more than 5,300 full-text periodicals, including 4,400 peer-reviewed journals.

Applied Science & Technology Source – Combines content from Computers & Applied Science Complete and Applied Science & Technology Full Text. It focuses on traditional engineering challenges and research, as well as research concerning the business and social implications of new technology.

CINAHL Complete - The world's most comprehensive source of full-text for nursing & allied health journals, providing full text for more than 1,300 journals indexed in CINAHL. It includes health literature dealing with risk management; data breach – prevention and control; electronic records; privacy and confidentiality; and other aspects of medical cybersecurity.

Computer Science - Offers access to today's most well-read and influential periodicals on the computer, telecommunications and electronics industries.

Education Source ¬- Designed to meet the needs of education students, professionals and policy makers. The extensive collection includes full text for more than 1,700 journals, 550 books and monographs, education-related conference papers, citations for over 4 million articles including book reviews. It includes educational specialties such cybersecurity as an upcoming area in the field of information technology.

Gale Academic OneFile – Provides peer-reviewed, full-text articles from leading journals and reference sources. Includes coverage of the physical sciences, technology, medicine, social sciences, the arts, theology and literature.

Gale General OneFile – Provides peer-reviewed, full-text articles from leading journals and reference sources.

JSTOR - Access to back issues of core journals in the humanities, social

sciences and sciences. Over 700 titles available.

MasterFILE Premier – Contains full text for nearly 1,700 periodicals covering general reference, business, health, education, general science and multicultural issues. This database also contains full text more than 500 reference books, over 107,000 primary source documents, and an Image Collection of over 510,000 photos, maps & flags.

MEDLINE with Full Text - Full text for nearly 1,200 journals with coverage dating back to 1965. Authoritative medical information on medicine, nursing, dentistry, veterinary medicine and health care systems. Topics include cybersecurity implications for hospital quality.

Military & Government Collection – Designed to offer current news and information to all branches of the military, with a thorough collection of military titles, trade publications and newsweeklies. Full text for nearly 350 titles.

Nexis Uni - Features more than 15,000 news, business and legal sources,

PsycARTICLES - Provides full-text, peer-reviewed scholarly and scientific articles in psychology. It contains more than 100,000 articles from 59 journals - 48 published by the American Psychological Association (APA) and 11 from allied organizations. It includes topics such as personality as a predictor of cybersecurity behavior

ScienceDirect - Elsevier's leading information solution for researchers, teachers, students, health care professionals and information professionals. It combines authoritative, full-text scientific, technical and health publications.

Springer Nature Journals – Scientific journals that feature original research articles across in wide range of scientific fields

Specific Journals available through the SPC library that will support the program include:

Computer Security Journal
Computers & Security
Information Systems Auditor
International Journal of Cyber-Security and Digital Forensics
International Journal of Information Security and Privacy
Journal of Cybersecurity
Secure Computing

Windows IT Security
Academy of Information and Management Sciences Journal
ACM Transactions on Information Systems

Existing faculty personnel will support the discipline with material selection and instructional needs. Furthermore, the current library's electronic learning spaces and the supporting hardware are adequate to support the needs of the proposed program for the enrollment projected in the Appendix Table A.2

9.2 Describe the new library and media resources that will be needed for the program (if applicable).

N/A

ACADEMIC CONTENT

10.1 List the admission requirements for the program.

The BAS degree program in Cybersecurity is designed to provide a seamless articulation for students who complete an Associate in Science degree in Cybersecurity or related field.

Admission to the Bachelor of Applied Science in Cybersecurity therefore requires:

- An Associates in Science degree in Cybersecurity or 60 hours in a related field and completion of prerequisite courses
- 60 credits from a regionally accredited institution, including:
  - 15 credits of transferable general education courses
  - ENC1101- Composition I or equivalent
  - a college Math Course: MAT 1033, MAT1100, STA 2023, STA 2023H OR any MAC, MGF, MTG, MAS math prefix
- A minimum GPA of 2.0 or higher on a 4.0 scale
- Foreign Language:
  - Students admitted to the baccalaureate degree program without meeting the foreign language admission requirement must complete 8 credits as a requirement prior to graduation.
  - If satisfying the requirement by high school courses, high school transcript must be presented.

10.2 What is the estimated percentage of upper division courses in the program that will be taught by faculty with a terminal degree?

In accordance with the Southern Association of Colleges and Schools Commission on Colleges (SACSCOC), at least 25% of the upper division coursework in the proposed BAS program in Cybersecurity will be taught by faculty with a terminal degree. A Ph.D. in Computer Science, Cybersecurity, Management Information Systems, Information Technology or similar program is considered a terminal degree in this context.

Currently three of sixteen faculty members in CCIT hold terminal degrees. CCIT has begun recruiting a pool of adjunct instructors who hold professional positions in cybersecurity. Five adjuncts with terminal degrees have been hired specifically to teach in the cybersecurity programs.

At minimum 25% of the courses will be taught by faculty with terminal degrees however, this number is likely to be higher based on the pool of qualified faculty hired specifically to teach in the program.

10.3 What is the anticipated average student/teacher ratio for each of the first three years based on enrollment projections?

The average student/teacher ratio is expected to 10:1 in year 1 with a maximum of 24:1 in all subsequent years. This ratio provides an optimal level of faculty-student engagement in an online modality.

10.4 What is the anticipated SACSCOC accreditation date, if applicable?
April 2020

10.5 What is the anticipated Florida Department of Education initial teacher preparation approval date, if applicable?
N/A

10.6 What specialized program accreditation will be sought, if applicable?
N/A

10.7 What is the anticipated specialized program accreditation date, if applicable?
N/A

10.8 Are there similar programs listed in the Common Prerequisites Manual for the CIP code (and track, if any) proposed for this program? **X** Yes ☐ No

Cybersecurity

10.9 List the established common prerequisites for this CIP code (and track, if any) as

listed in the Common Prerequisites Manual proposed for this program:

CIP 11.1003 Cybersecurity Track 1

Lower Level Courses	Credit Hours
Cisco CCNA Security (CET2614C)	3
Programming Concepts (COP1510)	3
Administering MS Windows Workstation (CTS1300C)	3
Install and Configure Windows Server (CTS1390C)	3
Security+ (CTS2120C)	3
Project Management (CTS2149)	3
Information Security Management (CTS2318)	3

CIP 11.1003 Cybersecurity Track 2

Lower Level Courses	Credit Hours
Analytical Geometry and Calculus I (MACX311)	4
Analytical Geometry and Calculus II (MACX312)	4
Physics 1 and Lab (PHYX048/X048L)	4
Elements of Statistics (STAX023)	3
Additional Science Course	3
Programming Course	3

CIP 11.1003 Cybersecurity Track 3

Lower Level Courses	Credit Hours
Introduction to Psychology (PSYX012)	3
Macroeconomics (ECOX013)	3
Introductory Statistics (STAX023 or STAX122)	3
Calculus (MACX147)	3
Physics (PHYXXXX)	3
Discrete Math (MADX104)	3
Database Technology Course	3
Programming Fundamentals Course	3
Object-Oriented Programming Course	3

10.10 Describe any proposed revisions to the established common prerequisites for this CIP (and track, if any).

CIP 11.1003 Cybersecurity Track 4

FOR ALL MAJORS: Students are strongly encouraged to select required lower division electives that will enhance their general education coursework and that will support their intended baccalaureate degree program. Students should consult with an academic advisor in their major degree area.

All Florida College System students are encouraged to complete the Associate degree. Students should consult with an academic advisor in their major degree area at the intended transfer institution.

Prerequisites for this program are:

Lower Level Courses	Credit Hours
CET2691 Laws & Legal Aspects of IT Security	3
CGS2811 Incident Response & Disaster Recovery	3
CIS1358 Operating System Security	3
CIS2352 Ethical Hacking	3
CTS1120 Network Security Foundations	3
CTS1314 Network Defense and Countermeasures*	3

*This course is pending approval to CTS2314

10.11 List all courses required once admitted to the baccalaureate program by term, in sequence. For degree programs with concentrations, list courses for each concentration area. Include credit hours per term, and total credits for the program:

Term	Course Title	Credit Hours
First Term		
CIS3083	Cloud Computing Foundations	3
ISM4330	Security Policy	3
CIS4253	Ethics for Information Technology	3
	GenEd Course	3
	Total Term Credit Hours	12
Second Term		
CIS4219	Human Aspects of Cyber Security	3
ISMXXXX	Compliance and Data Governance	3
ISM4321	Strategic Cyber Security Enforcement	3
	GenEd Course	3
	Total Term Credit Hours	12

Summer Term		
ISM4338	Advanced Cyber Forensics	3
	GenEd Course	3
	Total Term Credit Hours	6
Third Term		
CNT4416	Cyber War Gaming	3
ISM4041	Emerging Cyber Security Technologies	3
ISM4323	Security Essentials	3
	GenEd Course	3
	Total Term Credit Hours	12
Fourth Term		
CNT3421	Securing the Cloud	3
CTS4124	Threat Detection and Mitigation	3
CIS3XXX	Security Architectures	3
CIS4200	Pentration Testing	3
	Total Term Credit Hours	12
Summer Term		
ISM4915	Capstone	3
	GenEd Course	3
	Total Term Credit Hours	6
	Total Program Credit Hours	60

10.12 Is the program being proposed as a limited access program? (If yes, identify admission requirements and indicate enrollment capacity): ☐ Yes **X** No

PROGRAM TERMINATION

11.1 Plan of action if program must be terminated, including teach-out alternatives for students.

As mandated by the State Board of Education, St. Petersburg College will demonstrate diligence to individual needs in the event of program termination and will enact an approved degree completion plan to enable eligible students to complete the appropriate BAS degree program coursework following the termination decision to include transition services, “teach-out” options, and options for students to complete with other area institutions.

Appendix Table A.1.

INSTRUCTIONS FOR COMPLETING THE DEMAND SECTION OF APPENDIX TABLE A.1.1 and A.1.1.2: To complete the following table, use the CIP to Standard Occupational Classification (SOC) crosswalk of the U.S. Department of Education to identify the SOC codes for occupations associated with the proposed program's CIP code. Fill in Table A.1.1 using the employment projections data produced by the Florida Department of Economic Opportunity (DEO), pursuant to Section 445.07, F.S., for the workforce region aligned with the college's service district for each SOC code associated with the proposed program's CIP code. The employment projections data may be accessed at http://www.floridajobs.org/labor-market-information/data-center/statistical- programs/employment-projections. For proposed programs without a listed SOC linkage, identify the appropriate SOC codes for which the program prepares graduates. Insert additional rows as needed. The total job openings column value shall be divided by eight to reflect total annual job openings. The annualized salary shall be calculated by multiplying the average hourly wage times 40, and then multiplying that value times 52. Complete table A.1.1.2 in the same manner as A.1.1 for any additional sources of employment projections. Duplicate Table A.1.1.2 for additional sources as needed.

DEMAND: FLORIDA DEPARTMENT OF ECONOMIC OPPORTUNITY (DEO) EMPLOYMENT PROJECTIONS

A.1.1	Occupation			Number of Jobs				Salary		Education Level
	Name/Title	SOC Code	County/ Region	Base Year	Projected Year	Level Change	Total Job Openings (divided by 8)	Avg. Hourly Wage	Annualized Salary	
	Computer and Information Systems Managers	113021	14	834	955	121	80	$60.25	$125,320	Bachelor's Degree
	Information Security Analysts	151122	14	357	452	95	39	$39.90	$82,992	Bachelor's Degree
	Database Administrators	151141	14	542	628	86	47	$41.74	$86,819	Bachelor's Degree
	Computer Network Specialist	151152	14	808	925	117	77	$27.62	$57,450	Associate Degree
	Network & Computer System Administrators	151142	14	1,328	1,453	125	100	$36.41	$75,732	Bachelor's Degree
	Computer Network Architects	151143	14	1,171	1,299	128	94	$41.63	$86,590	Bachelor's Degree
						Total	437	$41.26	$85,800	

DEMAND: OTHER ENTITY INDEPENDENT OF THE COLLEGE – (EMSI Q1 2019 Data Set www.economicmodling.com)

A.1.1.2

Occupation			Number of Jobs				Salary		
Name/Title	SOC Code	County/ Region	Base Year	Projected Year	Level Change	Total Job Openings	Avg. Hourly Wage	Annualized Salary	Education Level
Computer & Information Systems Managers	11-3021	Pinellas	1,024	1,175	151	84	$53.27	$110.801	Bachelor's
Computer System Analysts	15-1121	Pinellas	1,484	1,609	125	229	$33.75	$70,200	Bachelor's
Information Security Analysts	15-1122	Pinellas	359	428	69	100	$37.28	$77,542	Bachelor's
Database Administrators	15-1141	Pinellas	468	500	32	53	$39.39	$81,931	Bachelor's
Computer Network Support Specialists	15-1152	Pinellas	710	745	35	5	$26.76	$55,660	Associates
					Total	471	$38.09	$79,227	

INSTRUCTIONS FOR COMPLETING THE SUPPLY SECTION OF APPENDIX TABLE A.1.2: To complete the following table, use the Integrated Postsecondary Education Data System of the National Center for Education Statistics to identify the number of degrees awarded by other regionally accredited postsecondary institutions in the college's service district under the same or related CIP code(s) as the proposed program. The data center is located at http://nces.ed.gov/ipeds/datacenter/. Include degrees awarded for the most recent year available and for the four prior years for each program. If the program has not had degrees awarded for five years or more, add the degrees awarded for the years available, and divide by that number of years, for the average.

SUPPLY: NATIONAL CENTER FOR EDUCATION STATISTICS, INTEGRATED POSTSECONDARY EDUCATION DATA SYSTEM

A.1.2

Program		Number of Degrees Awarded					
Institution Name	CIP Code	Prior Year 4	Prior Year 3	Prior Year 2	Prior Year 1	Most Recent Year	5-year average or average of years available if less than 5 years
The University of Tampa	11.1003	0	0	0	4	25	14.5
					Total	29	14.5

INSTRUCTIONS FOR COMPLETING THE ESTIMATES OF UNMET NEED SECTION OF APPENDIX TABLE A.1.3: To complete the following table, column A should be derived from Tables A.1.1 and A.1.1.2 and the totals in columns B and C should be derived from Table A.1.2. Input the figures in the "Total" row in Table A.1.1 and A.1.1.2 for total job openings and Table A.1.2 for most recent year and 5-year average (these figures should be same for all sources). The range of estimated unmet need should be derived from 1) subtracting the figure in column B from the figure in column A and 2) subtracting the figure in column C from the figure in column A. Add rows for additional sources as needed.

ESTIMATES OF UNMET NEED

A.1.3

	DEMAND	SUPPLY		RANGE OF ESTIMATED UNMENT NEED	
	(A)	(B)	(C)	(A-B)	(A-C)
	Total Job Openings (divided by 8)	Most Recent Year	5-year average or average of years available if less than 5 years	Difference	Difference
DEO	437	25	14.5	412	422.5
Other: (List here)					

Appendix Table A.2

INSTRUCTIONS FOR COMPLETING THE PROJECTED BACCALAUREATE PROGRAM ENROLLMENT SECTION OF APPENDIX TABLE A.2: To complete the following table, enter the projected enrollment information for the first four years of program implementation. Unduplicated headcount enrollment refers to the actual number of students enrolled. Full-time equivalent (FTE) refers to the full-time equivalent of student enrollment.

PROJECTED BACCALAUREATE PROGRAM ENROLLMENT

		Year 1	Year 2	Year 3	Year 4
A.2.1	Unduplicated headcount enrollment:				
A.2.1.1	Admitted Student Enrollment (First-time)	50	100	175	250
A.2.1.2	Total Admitted Student Enrollment	50	150	325	575
A.2.2	FTE Enrollment:				
A.2.2.1	Program Student Credit Hours (Resident)	480	1,440	3,120	5,520
A.2.2.2	Program Student Credit Hours (Non-resident)	0	0	0	0
A.2.2.3	Total Program Student Credit Hours	480	1,440	3,120	5,520
A.2.2.4	Program FTE (30 credits) - (Resident)	16	48	104	184
A.2.2.5	Program FTE (30 credits) - (Non-resident)	0	0	0	0
A.2.2.6	Total Program FTE	16	48	104	184

INSTRUCTIONS FOR COMPLETING THE PROJECTED DEGREES AND WORKFORCE OUTCOMES SECTION OF APPENDIX TABLE A.2: To complete the following table, enter the projected number of degrees awarded, the projected number of graduates employed and the projected average starting salary for program graduates for the first four years of program implementation.

PROJECTED DEGREES AND WORKFORCE OUTCOMES

		Year 1	Year 2	Year 3	Year 4
A.2.3	Degrees	0	25	70	152
A.2.4	Number Employed	0	20	63	136
A.2.5	Average Starting Salary	$0	$85,000	$85,000	$85,000

INSTRUCTIONS FOR COMPLETING THE REVENUES AND EXPENDITURES SECTION OF APPENDIX TABLE A.2: To complete the following table, enter the projected program expenditures and revenue sources for the first four years of program implementation.

REVENUES AND EXPENDITURES				
I. PROJECTED PROGRAM EXPENDITURES	Year 1	Year 2	Year 3	Year 4
INSTRUCTIONAL				
1. Faculty Full-Time FTE	0	.5	1.0	2.0
2. Faculty Part-Time FTE	1.5	2.0	2.0	2.0
1. Faculty Full-Time Salaries/Benefits	0	35,446	70,891	141,782
2. Faculty Part-Time Salaries/Benefits	28, 431	37,708	37,708	37,708
3. Faculty Support: Lab Assistants	0	0	0	0
OPERATING EXPENSES				
1. Academic Administration	9,195	9,195	18,390	18,390
2. Materials/Supplies	0	0	1,500	1,500
3. Travel	0	0	2,500	5,000
4. Communication/Technology	0	1,000	2,000	3,000
5. Library Support	0	0	0	0
6. Student Services Support	0	0	10,000	10,000
7. Professional Services	0	0	0	0
8. Accreditation	0	0	0	0
9. Support Services	0	0	0	0

CAPITAL OUTLAY				
1. Library Resources	0	0	0	0
2. Information Technology Equipment	0	1,000	2,000	3,000
3. Other Equipment	0	0	0	0
4. Facilities/Renovation	0	0	0	0
TOTAL PROJECTED PROGRAM EXPENDITURES	37,626	84,349	144,989	220,380
II. NATURE OF EXPENDITURES				
1. Recurring	37,626	83,349	142,989	217,380
2. Nonrecurring	0	1,000	2,000	3,000
TOTAL	37,626	84,349	144,989	220,380
III. SOURCES OF FUNDS				
A. REVENUE				
1. Special State Nonrecurring	0	0	0	0
2. Upper Level - Resident Student Tuition Only	58,896	176,688	382,824	677,304
Upper Level - Nonresident Student Fees Only	0	0	0	0
Upper Level - Other Student Fees	0	0	0	0
3. Contributions or Matching Grants	0	0	0	0
4. Other Grants or Revenues	47,482	36,058	0	0
5. Florida College System Program Funds	0	0	0	0
6. Unrestricted Fund Balance	0	0	0	0
7. Interest Earnings	0	0	0	0
8. Auxiliary Services	0	0	0	0
9. Federal Funds – Other	0	0	0	0
B. CARRY FORWARD	0	0	0	0
TOTAL FUNDS AVAILABLE	106,378	212,746	382,824	677,304
TOTAL UNEXPENDED FUNDS (CARRY FORWARD)	$0	$0	$0	$0

SUPPLEMENTAL MATERIALS

B.1 Summarize any supporting documents included with the proposal, such as meeting minutes, survey results, letters of support, and other supporting artifacts.

Attached as appendices are:

Appendix A	Page 34	Grant Application for DOE FIPSE Pilot Program in Cybersecurity Education Technological Upgrades for Community Colleges ***Note: Industry Letters of Support are included in the Grant Application***
Appendix B	Page 114	Email Notification of Grant Award
Appendix C	Page 116	Real Time Record of DACUM Session
Appendix D	Page 147	Board of Trustees (BOT) Agenda
Appendix E	Page 150	Notice of Intent Letter to SPC BOT
Appendix F	Page 156	Presentation for SPC BOT
Appendix G	Page 165	Program Comparison Worksheet
Appendix H	Page 168	Internal DACUM Program Worksheet
Appendix I	Page 171	Detail of Consultations with CSSIA
Appendix J	Page 174	Occupational Overview for Cybersecurity BAS Degree
Appendix K	Page 183	Feedback from State Institutions Regarding NOI
Appendix L	Page 186	Press Release – SPC Named Center of Excellence in Cyber Defense Education, NSA CAE-CDE designation
Appendix M	Page 188	Letter of Support for SPC BAS Proposal from the University of South Florida

B.2 List any objections or alternative proposal received from other postsecondary institutions for this program.

No Objections have been received (See Appendix K).

Appendix A

Grant Application for DOE FIPSE Pilot Program in Cybersecurity Education Technological Upgrades for Community Colleges

Note: Industry Letters of Support are included in the Grant Application

OMB Number: 4040-0004
Expiration Date: 12/31/2019

Application for Federal Assistance SF-424

* 1. Type of Submission:	* 2. Type of Application:	* If Revision, select appropriate letter(s):
☐ Preapplication Application	☒ New	
☒ Changed/Corrected Application	☐ Continuation	* Other (Specify):
☐	☐ Revision	

* 3. Date Received:	4. Applicant Identifier:
Completed by Grants.gov upon submission.	

5a. Federal Entity Identifier:	5b. Federal Award Identifier:

State Use Only:

6. Date Received by State:	7. State Application Identifier:

8. APPLICANT INFORMATION:

* a. Legal Name: Board of Trustees of St. Petersburg College

* b. Employer/Taxpayer Identification Number (EIN/TIN):	* c. Organizational DUNS:
59-1211489	0696742810000

d. Address:

* Street1:	PO Box 13489
Street2:	
* City:	St. Petersburg
County/Parish:	Pinellas
* State:	FL: Florida
Province:	
* Country:	USA: UNITED STATES
* Zip / Postal Code:	33733-3489

e. Organizational Unit:

Department Name:	Division Name:

f. Name and contact information of person to be contacted on matters involving this application:

Prefix:		* First Name:	Katie
Middle Name:			
* Last Name:	Shultz		
Suffix:			

Title: Executive Director of Grants Development

Organizational Affiliation:

* Telephone Number:	Fax Number:
727-341-3002	

* Email:	shultz.katie@spcollege.edu	

Application for Federal Assistance SF-424

*** 9. Type of Applicant 1: Select Applicant Type:**

H: Public/State Controlled Institution of Higher Education

Type of Applicant 2: Select Applicant Type:

Type of Applicant 3: Select Applicant Type:

* Other (specify):

*** 10. Name of Federal Agency:**

Department of Education

11. Catalog of Federal Domestic Assistance Number:

84.116

CFDA Title:

Fund for the Improvement of Postsecondary Education

*** 12. Funding Opportunity Number:**

ED-GRANTS-073018-002

* Title:

Office of Postsecondary Education (OPE): Fund for the Improvement of Postsecondary Education (FIPSE): Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges CFDA Number 84.116R

13. Competition Identification Number:

84-116R2018-1

Title:

Pilot Program Cybersecurity Education Technological Upgrades for Community Colleges

14. Areas Affected by Project (Cities, Counties, States, etc.):

Areas Affected.pdf | Add Attachment | Delete Attachment | View Attachment

*** 15. Descriptive Title of Applicant's Project:**

St. Petersburg College Cybersecurity Education Technological Upgrades Program

Attach supporting documents as specified in agency instructions.

Add Attachments | Delete Attachments | View Attachments

Application for Federal Assistance SF-424

16. Congressional Districts Of:

* a. Applicant FL-013 * b. Program/Project FL-013

Attach an additional list of Program/Project Congressional Districts if needed.

Congressional Districts.pdf | Add Attachment | Delete Attachment | View Attachment

17. Proposed Project:

* a. Start Date: 03/01/2019 * b. End Date: 02/28/2021

18. Estimated Funding ($):

* a. Federal	83,540.00
* b. Applicant	0.00
* c. State	0.00
* d. Local	0.00
* e. Other	0.00
* f. Program Income	0.00
* g. TOTAL	83,540.00

*** 19. Is Application Subject to Review By State Under Executive Order 12372 Process?**

☐ a. This application was made available to the State under the Executive Order 12372 Process for review on .

☐ b. Program is subject to E.O. 12372 but has not been selected by the State for review.

☒ c. Program is not covered by E.O. 12372.

*** 20. Is the Applicant Delinquent On Any Federal Debt? (If "Yes," provide explanation in attachment.)**

☐ Yes ☒ No

If "Yes", provide explanation and attach

Add Attachment | Delete Attachment | View Attachment

21. *By signing this application, I certify (1) to the statements contained in the list of certifications and (2) that thestatements herein are true, complete and accurate to the best of my knowledge. I also provide the required assurances** and agree to comply with any resulting terms if I accept an award. I am aware that any false, fictitious, or fraudulent statements or claims may subject me to criminal, civil, or administrative penalties. (U.S. Code, Title 218, Section 1001)**

☒ ** I AGREE

** The list of certifications and assurances, or an internet site where you may obtain this list, is contained in the announcement or agency specific instructions.

Authorized Representative:

Prefix:	Dr.	* First Name:	Tonjua
Middle Name:			
* Last Name:	Williams		
Suffix:			

* Title: President

* Telephone Number: 727-341-3241 Fax Number:

* Email: williams.tonjua@spcollege.edu

* Signature of Authorized Representative: Completed by Grants.gov upon submission. * Date Signed: Completed by Grants.gov upon submission.

Areas Affected by Project

Pinellas County, Florida

Congressional Districts of Program/Project

FL-013	FL-014

U.S. DEPARTMENT OF EDUCATION
BUDGET INFORMATION
NON-CONSTRUCTION PROGRAMS

OMB Number: 1894-0008
Expiration Date: 08/31/2020

Name of Institution/Organization

Board of Trustees of St. Petersburg College

Applicants requesting funding for only one year should complete the column under "Project Year 1." Applicants requesting funding for multi-year grants should complete all applicable columns. Please read all instructions before completing form.

SECTION A - BUDGET SUMMARY
U.S. DEPARTMENT OF EDUCATION FUNDS

Budget Categories	Project Year 1 (a)	Project Year 2 (b)	Project Year 3 (c)	Project Year 4 (d)	Project Year 5 (e)	Total (f)
1. Personnel	13,063.00	15,675.00				28,738.00
2. Fringe Benefits	2,090.00	2,508.00				4,598.00
3. Travel	6,000.00	6,000.00				12,000.00
4. Equipment	9,700.00	0.00				9,700.00
5. Supplies	0.00	0.00				0.00
6. Contractual	0.00	0.00				0.00
7. Construction	0.00	0.00				0.00
8. Other	13,194.00	8,597.00				21,791.00
9. Total Direct Costs (lines 1-8)	44,047.00	32,780.00				76,827.00
10. Indirect Costs*	3,435.00	3,278.00				6,713.00
11. Training Stipends						
12. Total Costs (lines 9-11)	47,482.00	36,058.00				83,540.00

Indirect Cost Information *(To Be Completed by Your Business Office):

If you are requesting reimbursement for indirect costs on line 10, please answer the following questions:

(1) Do you have an Indirect Cost Rate Agreement approved by the Federal government? ☐ Yes ☐ No

(2) If yes, please provide the following information:

Period Covered by the Indirect Cost Rate Agreement: From: 07/01/2016 To: 06/30/2020 (mm/dd/yyyy)

Approving Federal agency: ☐ ED ☒ Other (please specify): Department of Health and Human Services

The Indirect Cost Rate is 33.00 %.

(3) If this is your first Federal grant, and you do not have an approved indirect cost rate agreement, are not a State, Local government or Indian Tribe, and are not funded under a training rate program or a restricted rate program, do you want to use the de minimis rate of 10% of MTDC? ☐ Yes ☐ No If yes, you must comply with the requirements of 2 CFR § 200.414(f).

(4) If you do not have an approved indirect cost rate agreement, do you want to use the temporary rate of 10% of budgeted salaries and wages?

☐ Yes ☐ No If yes, you must submit a proposed indirect cost rate agreement within 90 days after the date your grant is awarded, as required by 34 CFR §75.560.

(5) For Restricted Rate Programs (check one) -- Are you using a restricted indirect cost rate that:

☐ Is included in your approved Indirect Cost Rate Agreement? Or, ☐ Complies with 34 CFR 76.564(c)(2)? The Restricted Indirect Cost Rate is ☐ %.

ED 524

☒ ☐

Name of Institution/Organization	Applicants requesting funding for only one year should complete the column under "Project Year 1." Applicants requesting funding for multi-year grants should complete all applicable columns. Please read all instructions before completing form.	
Board of Trustees of St. Petersburg College		

SECTION B - BUDGET SUMMARY
NON-FEDERAL FUNDS

Budget Categories	Project Year 1 (a)	Project Year 2 (b)	Project Year 3 (c)	Project Year 4 (d)	Project Year 5 (e)	Total (f)
1. Personnel						
2. Fringe Benefits						
3. Travel						
4. Equipment						
5. Supplies						
6. Contractual						
7. Construction						
8. Other						
9. Total Direct Costs (lines 1-8)						
10. Indirect Costs						
11. Training Stipends						
12. Total Costs (lines 9-11)						

SECTION C - BUDGET NARRATIVE (see instructions)

ED 524

OMB Number: 4040-0007
Expiration Date: 01/31/2019

ASSURANCES - NON-CONSTRUCTION PROGRAMS

PLEASE DO NOT RETURN YOUR COMPLETED FORM TO THE OFFICE OF MANAGEMENT AND BUDGET. SEND IT TO THE ADDRESS PROVIDED BY THE SPONSORING AGENCY.

NOTE: Certain of these assurances may not be applicable to your project or program. If you have questions, please contact the awarding agency. Further, certain Federal awarding agencies may require applicants to certify to additional assurances. If such is the case, you will be notified.

As the duly authorized representative of the applicant, I certify that the applicant:

1. Has the legal authority to apply for Federal assistance and the institutional, managerial and financial capability (including funds sufficient to pay the non-Federal share of project cost) to ensure proper planning, management and completion of the project described in this application.

2. Will give the awarding agency, the Comptroller General of the United States and, if appropriate, the State, through any authorized representative, access to and the right to examine all records, books, papers, or documents related to the award; and will establish a proper accounting system in accordance with generally accepted accounting standards or agency directives.

3. Will establish safeguards to prohibit employees from using their positions for a purpose that constitutes or presents the appearance of personal or organizational conflict of interest, or personal gain.

4. Will initiate and complete the work within the applicable time frame after receipt of approval of the awarding agency.

5. Will comply with the Intergovernmental Personnel Act of 1970 (42 U.S.C. §§4728-4763) relating to prescribed standards for merit systems for programs funded under one of the 19 statutes or regulations specified in Appendix A of OPM's Standards for a Merit System of Personnel Administration (5 C.F.R. 900, Subpart F).

6. Will comply with all Federal statutes relating to nondiscrimination. These include but are not limited to: (a) Title VI of the Civil Rights Act of 1964 (P.L. 88-352) which prohibits discrimination on the basis of race, color or national origin; (b) Title IX of the Education Amendments of 1972, as amended (20 U.S.C.§§1681- 1683, and 1685-1686), which prohibits discrimination on the basis of sex; (c) Section 504 of the Rehabilitation

Act of 1973, as amended (29 U.S.C. §794), which prohibits discrimination on the basis of handicaps; (d) the Age Discrimination Act of 1975, as amended (42 U. S.C. §§6101-6107), which prohibits discrimination on the basis of age; (e) the Drug Abuse Office and Treatment Act of 1972 (P.L. 92-255), as amended, relating to nondiscrimination on the basis of drug abuse; (f) the Comprehensive Alcohol Abuse and Alcoholism Prevention, Treatment and Rehabilitation Act of 1970 (P.L. 91-616), as amended, relating to nondiscrimination on the basis of alcohol abuse or alcoholism; (g) §§523 and 527 of the Public Health Service Act of 1912 (42 U.S.C. §§290 dd-3 and 290 ee- 3), as amended, relating to confidentiality of alcohol and drug abuse patient records; (h) Title VIII of the Civil Rights Act of 1968 (42 U.S.C. §§3601 et seq.), as amended, relating to nondiscrimination in the sale, rental or financing of housing; (i) any other nondiscrimination provisions in the specific statute(s) under which application for Federal assistance is being made; and, (j) the requirements of any other nondiscrimination statute(s) which may apply to the application.

7. Will comply, or has already complied, with the requirements of Titles II and III of the Uniform Relocation Assistance and Real Property Acquisition Policies Act of 1970 (P.L. 91-646) which provide for fair and equitable treatment of persons displaced or whose property is acquired as a result of Federal or federally-assisted programs. These requirements apply to all interests in real property acquired for project purposes regardless of Federal participation in purchases.

8. Will comply, as applicable, with provisions of the Hatch Act (5 U.S.C. §§1501-1508 and 7324-7328) which limit the political activities of employees whose principal employment activities are funded in whole or in part with Federal funds.

Previous Edition Usable

Authorized for Local Reproduction

Standard Form 424B (Rev. 7-97)
Prescribed by OMB Circular A-102

9. Will comply, as applicable, with the provisions of the Davis-Bacon Act (40 U.S.C. §§276a to 276a-7), the Copeland Act (40 U.S.C. §276c and 18 U.S.C. §874), and the Contract Work Hours and Safety Standards Act (40 U.S.C. §§327- 333), regarding labor standards for federally-assisted construction subagreements.

10. Will comply, if applicable, with flood insurance purchase requirements of Section 102(a) of the Flood Disaster Protection Act of 1973 (P.L. 93-234) which requires recipients in a special flood hazard area to participate in the program and to purchase flood insurance if the total cost of insurable construction and acquisition is $10,000 or more.

11. Will comply with environmental standards which may be prescribed pursuant to the following: (a) institution of environmental quality control measures under the National Environmental Policy Act of 1969 (P.L. 91-190) and Executive Order (EO) 11514; (b) notification of violating facilities pursuant to EO 11738; (c) protection of wetlands pursuant to EO 11990; (d) evaluation of flood hazards in floodplains in accordance with EO 11988; (e) assurance of project consistency with the approved State management program developed under the Coastal Zone Management Act of 1972 (16 U.S.C. §§1451 et seq.); (f) conformity of Federal actions to State (Clean Air) Implementation Plans under Section 176(c) of the Clean Air Act of 1955, as amended (42 U.S.C. §§7401 et seq.); (g) protection of underground sources of drinking water under the Safe Drinking Water Act of 1974, as amended (P.L. 93-523); and, (h) protection of endangered species under the

    Endangered Species Act of 1973, as amended (P.L. 93-205).

12. Will comply with the Wild and Scenic Rivers Act of 1968 (16 U.S.C. §§1271 et seq.) related to protecting components or potential components of the national wild and scenic rivers system.

13. Will assist the awarding agency in assuring compliance with Section 106 of the National Historic Preservation Act of 1966, as amended (16 U.S.C. §470), EO 11593 (identification and protection of historic properties), and the Archaeological and Historic Preservation Act of 1974 (16 U.S.C. §§469a-1 et seq.).

14. Will comply with P.L. 93-348 regarding the protection of human subjects involved in research, development, and related activities supported by this award of assistance.

15. Will comply with the Laboratory Animal Welfare Act of 1966 (P.L. 89-544, as amended, 7 U.S.C. §§2131 et seq.) pertaining to the care, handling, and treatment of warm blooded animals held for research, teaching, or other activities supported by this award of assistance.

16. Will comply with the Lead-Based Paint Poisoning Prevention Act (42 U.S.C. §§4801 et seq.) which prohibits the use of lead-based paint in construction or rehabilitation of residence structures.

17. Will cause to be performed the required financial and compliance audits in accordance with the Single Audit Act Amendments of 1996 and OMB Circular No. A-133, "Audits of States, Local Governments, and Non-Profit Organizations."

18. Will comply with all applicable requirements of all other Federal laws, executive orders, regulations, and policies governing this program.

19. Will comply with the requirements of Section 106(g) of the Trafficking Victims Protection Act (TVPA) of 2000, as amended (22 U.S.C. 7104) which prohibits grant award recipients or a sub-recipient from (1) Engaging in severe forms of trafficking in persons during the period of time that the award is in effect (2) Procuring a commercial sex act during the period of time that the award is in effect or (3) Using forced labor in the performance of the award or subawards under the award.

SIGNATURE OF AUTHORIZED CERTIFYING OFFICIAL	TITLE
Completed on submission to Grants.gov	President
APPLICANT ORGANIZATION	DATE SUBMITTED
Board of Trustees of St. Petersburg College	Completed on submission to Grants.gov

Standard Form 424B (Rev. 7-97) Back

CERTIFICATION REGARDING LOBBYING

Certification for Contracts, Grants, Loans, and Cooperative Agreements

The undersigned certifies, to the best of his or her knowledge and belief, that:

(1) No Federal appropriated funds have been paid or will be paid, by or on behalf of the undersigned, to any person for influencing or attempting to influence an officer or employee of an agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with the awarding of any Federal contract, the making of any Federal grant, the making of any Federal loan, the entering into of any cooperative agreement, and the extension, continuation, renewal, amendment, or modification of any Federal contract, grant, loan, or cooperative agreement.

(2) If any funds other than Federal appropriated funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this Federal contract, grant, loan, or cooperative agreement, the undersigned shall complete and submit Standard Form-LLL, ''Disclosure of Lobbying Activities,'' in accordance with its instructions.

(3) The undersigned shall require that the language of this certification be included in the award documents for all subawards at all tiers (including subcontracts, subgrants, and contracts under grants, loans, and cooperative agreements) and that all subrecipients shall certify and disclose accordingly. This certification is a material representation of fact upon which reliance was placed when this transaction was made or entered into. Submission of this certification is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required certification shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

Statement for Loan Guarantees and Loan Insurance

The undersigned states, to the best of his or her knowledge and belief, that:

If any funds have been paid or will be paid to any person for influencing or attempting to influence an officer or employee of any agency, a Member of Congress, an officer or employee of Congress, or an employee of a Member of Congress in connection with this commitment providing for the United States to insure or guarantee a loan, the undersigned shall complete and submit Standard Form-LLL, "Disclosure of Lobbying Activities," in accordance with its instructions. Submission of this statement is a prerequisite for making or entering into this transaction imposed by section 1352, title 31, U.S. Code. Any person who fails to file the required statement shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

* APPLICANT'S ORGANIZATION	
Board of Trustees of St. Petersburg College	
* PRINTED NAME AND TITLE OF AUTHORIZED REPRESENTATIVE	
Prefix: Dr.	* First Name: Tonjua Middle Name:
* Last Name: Williams	Suffix:
* Title: President	
* SIGNATURE: Completed on submission to Grants.gov	* DATE: Completed on submission to Grants.gov

DISCLOSURE OF LOBBYING ACTIVITIES

Approved by OMB
4040-0013

Complete this form to disclose lobbying activities pursuant to 31 U.S.C.1352

1. * Type of Federal Action:
- ☐ a. contract
- ☒ b. grant
- ☐ c. cooperative agreement
- ☐ d. loan
- ☐ e. loan guarantee
- ☐ f. loan insurance

2. * Status of Federal Action:
- ☐ a. bid/offer/application
- ☒ b. initial award
- ☐ c. post-award

3. * Report Type:
- ☒ a. initial filing
- ☐ b. material change

4. Name and Address of Reporting Entity:

☒ Prime ☐ SubAwardee

** Name* N/A

** Street 1* N/A *Street 2*

** City* N/A *State* *Zip*

Congressional District, if known:

5. If Reporting Entity in No.4 is Subawardee, Enter Name and Address of Prime:

6. * Federal Department/Agency:

N/A

7. * Federal Program Name/Description:

Fund for the Improvement of Postsecondary Education

CFDA Number, *if applicable:* 84.116

8. Federal Action Number, *if known:*

9. Award Amount, *if known:*

$

10. a. Name and Address of Lobbying Registrant:

Prefix ** First Name* N/A *Middle Name* N/A

** Last Name* N/A *Suffix*

** Street 1* N/A *Street 2*

** City* N/A *State* *Zip*

b. Individual Performing Services (including address if different from No. 10a)

Prefix ** First Name* N/A *Middle Name*

** Last Name* N/A *Suffix*

** Street 1* N/A *Street 2*

** City* N/A *State* *Zip*

11. Information requested through this form is authorized by title 31 U.S.C. section 1352. This disclosure of lobbying activities is a material representation of fact upon which reliance was placed by the tier above when the transaction was made or entered into. This disclosure is required pursuant to 31 U.S.C. 1352. This information will be reported to the Congress semi-annually and will be available for public inspection. Any person who fails to file the required disclosure shall be subject to a civil penalty of not less than $10,000 and not more than $100,000 for each such failure.

*** Signature:** Completed on submission to Grants.gov

***Name:** *Prefix* Dr. ** First Name* Tonjua *Middle Name*

** Last Name* Williams *Suffix*

Title: President **Telephone No.:** 727-341-3241 **Date:** Completed on submission to Grants.gov

Federal Use Only:

Authorized for Local Reproduction
Standard Form - LLL (Rev. 7-97)

NOTICE TO ALL APPLICANTS

The purpose of this enclosure is to inform you about a new provision in the Department of Education's General Education Provisions Act (GEPA) that applies to applicants for new grant awards under Department programs. This provision is Section 427 of GEPA, enacted as part of the Improving America's Schools Act of 1994 (Public Law (P.L.) 103-382).

To Whom Does This Provision Apply?

Section 427 of GEPA affects applicants for new grant awards under this program. **ALL APPLICANTS FOR NEW AWARDS MUST INCLUDE INFORMATION IN THEIR APPLICATIONS TO ADDRESS THIS NEW PROVISION IN ORDER TO RECEIVE FUNDING UNDER THIS PROGRAM.**

(If this program is a State-formula grant program, a State needs to provide this description only for projects or activities that it carries out with funds reserved for State-level uses. In addition, local school districts or other eligible applicants that apply to the State for funding need to provide this description in their applications to the State for funding. The State would be responsible for ensuring that the school district or other local entity has submitted a sufficient section 427 statement as described below.)

What Does This Provision Require?

Section 427 requires each applicant for funds (other than an individual person) to include in its application a description of the steps the applicant proposes to take to ensure equitable access to, and participation in, its Federally-assisted program for students, teachers, and other program beneficiaries with special needs. This provision allows applicants discretion in developing the required description. The statute highlights six types of barriers that can impede equitable access or participation: gender, race, national origin, color, disability, or age. Based on local circumstances, you should determine whether these or other barriers may prevent your students, teachers, etc. from such access or participation in, the Federally-funded project or activity. The description in your application of steps to be taken to overcome these barriers need not be lengthy; you may provide a clear and succinct description of how you plan to address those barriers that are applicable to your circumstances. In addition, the information may be provided in a single narrative, or, if appropriate, may be discussed in connection with related topics in the application.

Section 427 is not intended to duplicate the requirements of civil rights statutes, but rather to ensure that, in designing their projects, applicants for Federal funds address equity concerns that may affect the ability of certain potential beneficiaries to fully participate in the project and to achieve to high standards. Consistent with program requirements and its approved application, an applicant may use the Federal funds awarded to it to eliminate barriers it identifies.

What are Examples of How an Applicant Might Satisfy the Requirement of This Provision?

The following examples may help illustrate how an applicant may comply with Section 427.

(1) An applicant that proposes to carry out an adult literacy project serving, among others, adults with limited English proficiency, might describe in its application how it intends to distribute a brochure about the proposed project to such potential participants in their native language.

(2) An applicant that proposes to develop instructional materials for classroom use might describe how it will make the materials available on audio tape or in braille for students who are blind.

(3) An applicant that proposes to carry out a model science program for secondary students and is concerned that girls may be less likely than boys to enroll in the course, might indicate how it intends to conduct "outreach" efforts to girls, to encourage their enrollment.

(4) An applicant that proposes a project to increase school safety might describe the special efforts it will take to address concern of lesbian, gay, bisexual, and transgender students, and efforts to reach out to and involve the families of LGBT students.

We recognize that many applicants may already be implementing effective steps to ensure equity of access and participation in their grant programs, and we appreciate your cooperation in responding to the requirements of this provision.

Estimated Burden Statement for GEPA Requirements

According to the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless such collection displays a valid OMB control number. Public reporting burden for this collection of information is estimated to average 1.5 hours per response, including time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. The obligation to respond to this collection is required to obtain or retain benefit (Public Law 103-382). Send comments regarding the burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to the U.S. Department of Education, 400 Maryland Ave., SW, Washington, DC 20210-4537 or email ICDocketMgr@ed.gov and reference the OMB Control Number 1894-0005.

Optional - You may attach 1 file to this page.

FIPSE Cybersecurity GEPA.pdf | Add Attachment | Delete Attachment | View Attachment

The Department of Education General Education Provision Act (GEPA) Section 427 requires each applicant for funds to include in its application a **description of the steps the applicant proposes to take to ensure equitable access to, and participation in, its Federally-assisted program for students, teachers, and other program beneficiaries with special needs.**

GEPA Section 427 highlights six types of barriers that can impede equitable access or participation: gender, race, national origin, color, disability, or age. Based on local circumstances, (applicants) should determine whether these or other barriers may prevent (their) students, teachers, etc. from such access or participation in, the Federally-funded project or activity.

Local Circumstances

St. Petersburg College (SPC) ensures that the characteristics of gender, race, national origin, color, disability or age **does not** impede equitable access or participation in its numerous programs, including federally-assisted programs. SPC, in fact, was formed to address the educational needs of individuals underrepresented and underserved by four-year colleges. Established in 1927 as the first two-year institution of higher education in the state of Florida, SPC has grown exponentially, enrolling over 30,000 degree-seeking students every year and offering baccalaureate and associate degree programs and certificates at its nine campuses throughout Pinellas County, Fla., and online.

SPC's student body is non-traditional, and includes a high proportion of low-income, underrepresented, and underprepared students: approximately 43% of students are aged 26 or older; 74% are studying part-time, suggesting that most are balancing school with employment or personal obligations; 51% receive federal financial aid; 93% of First Time in College (FTIC) are enrolled in developmental/Gateway courses signifying under preparedness for college; and 62.5% identify as Caucasian, 13.2% as African American, 14.2% as Hispanic, 4% as Asian, and 3.7% as Pacific Islander, American Indian, or Multiple Races (2.4% did not report). An estimated 60.1% of students identify as female, and 39.9% male. In 2017-2018, approximately 5% (1,539) of students enrolled had a documented disability.

The College offers a wide array of individualized academic support as well as services targeted toward high-need student groups including students with disabilities, first generation and limited income, pre-college students, minorities, women and veterans. In addition, SPC's Disability Resources Department helps achieve that college-wide goal by working with students, faculty and staff to provide accommodations that ensure equal access, therefore making admission, academic programs, support services, student activities and campus facilities accessible to, and usable by, all.

Program Purpose

The purpose of the Cybersecurity Education Technological Upgrades program is to support projects at institutions of higher education that improve infrastructure for cybersecurity education programs at community colleges. Through this program, the Cybersecurity subplan of SPC's existing B.A.S. degree in Information Technology and Management will be enhanced with

a technically-focused subplan in Cyber Defense, which will lead to a standalone B.A.S. degree in Cybersecurity.

1

These courses will be offered online, allowing students to take courses in a format that accommodates multiple schedules and accessibility needs. SPC faculty will work with the Disability Resources department to ensure accessibility of all online content; in addition, in-person advising and tutorial sessions will be available to accommodate needs.

Curriculum updates and newly designed courses will be aligned with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, which seeks to broaden the pool of individuals prepared to enter the cybersecurity workforce and places special emphasis on recruitment of women and underrepresented minorities. To this end, programming will emphasize outreach and recruitment to diverse communities, as well as engagement with training and conferences that promote diversity for women and underrepresented minorities.

To evaluate the impact of these services on the students, including underserved populations, SPC will assess and analyze the program each year and make necessary adjustments to maximize the program's outcomes.

Steps to ensure equitable access to FIPSE Pilot Program in Cybersecurity Education Technological Upgrades for Community Colleges

To ensure equitable access to and participation in the Cybersecurity Education Technological Upgrades program, SPC will take the following actions:

1. Uphold college policies regarding equal access and equal opportunity.
   The Board of Trustees of St. Petersburg College affirms its equal opportunity policy in accordance with the provisions of the Florida Educational Equity Act and all other relevant state and federal laws, rules and regulations. The college will not discriminate on the basis of race, color, ethnicity, religion, sex, age, national origin, marital status, sexual orientation gender identity, genetic information, or against any qualified individual with disabilities in its employment practices or in the admission and treatment of students. Recognizing that sexual harassment constitutes discrimination on the basis of sex and violates this Rule, the college will not tolerate such conduct.
   http://www.spcollege.edu/eaeo/
   Under Section 504 of the Vocational Rehabilitation Act of 1973 and the Americans with Disabilities Act of 1990, SPC seeks to ensure that admission, academic programs, support services, student activities and campus facilities are accessible to and usable by students who document a qualifying disability with the College. Students with disabilities who desire accommodations need to provide appropriate documentation of a disability and request services from Disability Resources.
   http://www.spcollege.edu/pages/disabilityresources.aspx?id=2147484098

2. Include efforts on accessibility for all students in the design, development and/or reassessment of the College's support services.

3. Review all existing program communications, documents and policies to ensure the

language and procedures are inclusive of and welcoming to underrepresented groups and ensure online communication is provided in/on accessible formats.

4. Solicit recommendation and constructive feedback from the College's Disability Resources Department, Veteran Services Department and the Men Achieving Excellence and Women on the Way Programs – all departments that work closely with underserved populations – in the program outreach and administration process to ensure that all potential barriers are addressed.

5. Work with aforementioned departments and the College's Registrar, Financial Aid and Advising Offices in the identification of potential students, as they will have a clear understanding of the underserved populations and potential barriers and access points.

6. Solicit recommendation and constructive feedback from new program contacts regarding ways to improve equitable access and participation.

7. Hold advising sessions in ADA accessible facilities and make arrangements for any special accommodations in advance for group tutoring locations and cultural and educational outings.

8. Post this information online.

3

OMB Number: 1894-0007
Expiration Date: 09/30/2020

U.S. DEPARTMENT OF EDUCATION
SUPPLEMENTAL INFORMATION
FOR THE SF-424

1. Project Director:

Prefix:	First Name:	Middle Name:	Last Name:	Suffix:
Dr.	John		Duff	

Address:

Street1:	PO Box 13489
Street2:	
City:	St. Petersburg
County:	
State:	FL: Florida
Zip Code:	33733-3489
Country:	USA: UNITED STATES

Phone Number (give area code): 727-341-7176

Fax Number (give area code):

Email Address: duff.john@spcollege.edu

2. Novice Applicant:

Are you a novice applicant as defined in the regulations in 34 CFR 75.225 (and included in the definitions page in the attached instructions)?

☐ Yes ☐ No ☒ Not applicable to this program

3. Human Subjects Research:

a. Are any research activities involving human subjects planned at any time during the proposed Project Period?

☐ Yes ☒ No

b. Are ALL the research activities proposed designated to be exempt from the regulations?

☐ Yes Provide Exemption(s) #: ☐ 1 ☐ 2 ☐ 3 ☐ 4 ☐ 5 ☐ 6

☐ No Provide Assurance #, if available:

c. If applicable, please attach your "Exempt Research" or "Nonexempt Research" narrative to this form as indicated in the definitions page in the attached instructions.

Add Attachment | Delete Attachment | View Attachment

Abstract

The abstract narrative must not exceed one page and should use language that will be understood by a range of audiences. For all projects, include the project title (if applicable), goals, expected outcomes and contributions for research, policy, practice, etc. Include population to be served, as appropriate. For research applications, also include the following:

- Theoretical and conceptual background of the study (i.e., prior research that this investigation builds upon and that provides a compelling rationale for this study)
- Research issues, hypotheses and questions being addressed
- Study design including a brief description of the sample including sample size, methods, principals dependent, independent, and control variables, and the approach to data analysis.

[Note: For a non-electronic submission, include the name and address of your organization and the name, phone number and e-mail address of the contact person for this project.]

You may now Close the Form

You have attached 1 file to this page, no more files may be added. To add a different file, you must first delete the existing file.

* Attachment: FIPSE Cybersecurity Abstract.pdf | Add Attachment | Delete Attachment | View Attachment

1. Applicant Institution and Consortium Members: St. Petersburg College (Applicant); NSF ATE National Center for Systems Security and Information Assurance—CSSIA (Required Partner) **2. Project Title:** *St. Petersburg College Cybersecurity Education Technological Upgrades*

3. **Abstract:** Cybercrime costs have skyrocketed, reaching nearly $2 trillion per year; Tampa Bay metro area is the 10th most cyberinsecure community in the U.S. due in part to the large presence of defense and financial service firms, including 19 global corporate headquarters.[1] Florida is the fourth-largest cyber employment market behind only California, Virginia, and Texas,[2] and projects a 28% increase in employment of information security analysts through 2026.[3] Located in Tampa Bay, St. Petersburg College (SPC) strives to remain on the forefront of cutting-edge curriculum and technology to meet regional and global workforce demand. SPC's College of Computer Information and Technology offers a Certificate and A.S. Degree in Cybersecurity, and is currently applying for the Two-Year Education (CAE2Y) designation in Cyber Defense for the A.S. degree. These offerings enrolled over 400 students in the 2017-2018 academic year alone, nearly doubling enrollment since 2015. However, many employers require a bachelor degree as the minimum standard for hire in cybersecurity. SPC was the first two-year college in Florida to offer baccalaureate degrees, and currently offers a Bachelor of Applied Science (B.A.S) in Information Technology Management. However, cybersecurity has emerged as a distinct discipline, necessitating a more technically-focused, standalone cybersecurity baccalaureate degree. In response to rising workforce and student demand, SPC will collaborate with CSSIA and industry advisors to upgrade and innovate the existing cybersecurity program, ultimately leading to a new B.A.S. in Cybersecurity degree. Once developed, this online B.A.S. in Cybersecurity will be the first of its kind at the community college level in Tampa Bay and only the second in Florida. The goal of this project is to increase the number of students pursuing a cybersecurity credential to meet workforce needs in the Tampa Bay region and beyond. This goal will be accomplished over a two-year period through the following objectives and activities: 1) Redevelop existing B.A.S. in Information Technology Management's Cybersecurity subplan curriculum to increase training opportunities for students, including development of 4 new subplan courses, integration of Capture the Flag virtual competitions, and industry certifications such as CompTIA PenTest+; 2) Develop a new B.A.S. degree in Cybersecurity aligned with NSA/DHS National Centers of Academic Excellence in Cyber Defense Education, including approval of academic plan and development of 6 new program courses; and 3) Improve faculty training and ability to offer industry-linked certifications in cybersecurity. By meeting these objectives, the project will serve approximately 200 students in the year immediately following the project end. This initiative will also strengthen regional and national partnerships with institutions in cybersecurity education, sharing resources and best practices for other community colleges seeking to develop B.A.S. programs. Funding will support faculty and staff efforts for curriculum development, new equipment for virtual training activities, and faculty certification training.

---

[1] Manning, M. (2018, March 22). Where Tampa-St. Pete ranks. Retrieved from https://www.bizjournals.com/tampabay/news/2018/05/22/where-tampa-ranks-among-the-cities- most-vulnerable.html

[2] CareerOneStop. (2015, July 01). Retrieved from http://www.careerinfonet.org

[3] Occupational Outlook Handbook. (2018, April 13). Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security- analysts.htm#tab-6

Project Narrative File(s)

*** Mandatory Project Narrative File Filename:** FIPSE Cybersecurity Program Narrative.pdf

Add Mandatory Project Narrative File | Delete Mandatory Project Narrative File | View Mandatory Project Narrative File

To add more Project Narrative File attachments, please use the attachment buttons below.

Add Optional Project Narrative File | Delete Optional Project Narrative File | View Optional Project Narrative File

Table of Contents

Part I: SF 424 Form
Application for Federal Assistance (SF 424)
Department of Education Supplemental Information Form for SF 424

Part II: ED 524 Form

Department of Education Budget Summary Form (ED 524)
Section A Budget Summary - U.S. Department of Education Summary
Section B Budget Summary - Non Federal Funds
Section C Budget Narrative provided in Part III, Program Narrative

Part III: Application Narrative

ED Abstract Form
Table of Contents
Narrative (pages 1-12)

(A) Needs Statement 1
(B) Proposed Program 4
1. Redevelop the existing B.A.S degree program 5
2. Develop new B.A.S. degree program 7
3. Improve faculty training 8

(C) Adequacy of Resources 9
1. Institutional Resources 9
2. Personnel 9
3. Partnerships 10
4. Reasonableness of proposed expenditures 11

(D) Evaluation 11

Bibliography

Budget Narrative

Other Attachments
Curriculum Vitae
Letters of
Commitment

Part IV: Assurances and Certifications

ED-GEPA Section 427 Requirement
Assurances - Non-Construction Programs (SF-424B)
Grants.gov Lobbying Form (ED form 80-0013)
Disclosure of Lobbying Activities

In response to the Department of Education's *Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges* solicitation as well as rising workforce and student demand, St. Petersburg College (SPC) proposes to upgrade and innovate its existing cybersecurity program, ultimately leading to a new online B.A.S. in Cybersecurity degree. SPC will collaborate with the NSF ATE National Resource Center for Systems Security and Information Assurance (CSSIA) as well as industry partners to develop responsive and cutting-edge curriculum and training opportunities. Once developed, the B.A.S. in Cybersecurity degree will be the first of its kind at the community college level in the Tampa Bay region and only the second in Florida, providing students with an affordable, flexible option for high-wage, high-demand sustainable careers in cybersecurity.

Needs Statement

Cybercrime costs the U.S. approximately $2 trillion per year, with some estimates as high as $3 trillion through 2021 (Morga 2016). The Tampa Bay region of Florida (*Figure 1*) ranks as the state leading tech hub ("Stem Jobs," 2015), and is home to 19 global cor

Figure 1: Tampa Bay

headquarters, four major military installations, and th corporations and infrastructure agencies, all of which are vulnerable to

cyberattack. A recent report lists the Tampa Bay metro area as the 10th most cyberinsecure community in the U.S. due in part to the large presence of defense and financial service firms, as well as an above average aging population (Manning, 2018). Beyond financial and technology

institutions, societal infrastructure systems such as public safety, transportation, and medical facilities also face their own weaknesses related to cyberterrorism and hacking. These agencies must be able to weather cyber threats as well. Former U.S. Secretary of Defense Leon Panetta has

warned that a cyber-Pearl Harbor, in which extremist groups take over public networks to cause mass destruction, may be only a matter of time (Bumiller & Shanker, 2012).

A well-prepared workforce is vital to meet these encroaching threats. Not only must cybersecurity employees understand the nature of the job, they must also remain flexible and keep their training up to speed in a rapidly-evolving field. The U.S. Department of Labor designates Florida as the fourth-largest cyber employment market behind only California, Virginia, and Texas ("CareerOneStop," 2015) and projects a 28% increase in employment of information security analysts through 2026 ("Occupational Outlook Handbook," 2018). A Florida Center for Cybersecurity report states: *"Even when compared with other high-demand IT jobs, demand for cybersecurity jobs (in Tampa Bay) is growing more than three times faster. Business leaders say they can't hire skilled cybersecurity workers fast enough." (State University System, 2013).* Experts have also noted a global shortage of cybersecurity skills. It's estimated that the current global job market will have more than 3.5 million job openings for cybersecurity professionals by 2021 (Wirth, 2016), with some fields showing a ratio as high as 3:1 of job openings to qualified applicants (Occupational Outlook Handbook, 2018). According to Cyberseek, there were 13,504 cybersecurity job openings in Florida alone in August 2018 ("Cybersecurity Supply," n.d.).

Located in Tampa Bay on the west coast of Florida, St. Petersburg College (SPC) strives to remain on the forefront of cutting-edge curriculum and technology to meet regional and global workforce demand. In an attempt to meet the immense cybersecurity employment demand in this area, SPC's College of Computer Information and Technology currently offers a Certificate and

A.S. Degree in Cybersecurity. These offerings are among the most rapidly filled programs within the College, enrolling over 400 students in the 2017-2018 academic year alone and nearly doubling enrollment since 2015 (Pulse BI, 2018). Student demand has led to the need for multiple adjunct

faculty hires and new course section offerings. The curriculum in the A.S. degree program aligns with entry-level industry certifications such as CompTIA A+, CompTIA Net+, CompTIA Sec+, CCNA Cyber Ops, and EC-Council's Certified Ethical Hacking, which provide students a pathway of milestone opportunities in the field of cybersecurity. SPC is also currently applying for the Department of Homeland Security and National Security Agency's National Centers of Academic Excellence program in Two-Year Education (CAE2Y) designation in Cyber Defense for the A.S. Cybersecurity degree. Centers of Academic Excellence in Cybersecurity institutions meet rigorous requirements and are determined to have robust degree programs and close alignment to salient cyber-security related knowledge units, validated by subject matter experts in the field.

While demand for the A.S. in Cybersecurity degree continues to grow, a 2015 Tampa Bay IT Workforce Analysis study reported the majority of regional employer respondents (62%) require a bachelor degree as the minimum standard for hire for cyber-related roles ("Tampa Bay Workforce," 2015). Nationally, eight in ten job postings for cybersecurity workers ask for a bachelor's degree or higher (Restuccia, 2018). SPC was the first community college in Florida to offer Baccalaureate degrees beginning in 2001, and currently offers a Bachelor of Applied Science (B.A.S) in Information Technology Management as an avenue for CCIT A.S. degree students. Approximately 46% of the 506 students who have enrolled in the Information Technology Management B.A.S. over the last four terms have selected Cybersecurity as their subplan. The current B.A.S. program approaches the subject from a managerial perspective. However, cybersecurity has emerged as a distinct discipline and a high percentage of students and employers surveyed would welcome a more technically-focused, standalone cybersecurity baccalaureate degree. According to CompTIA's *Trends in Information Security* study that included

insights from

3

nearly 700 business and technology professionals, cybersecurity is becoming its own discipline and not solely an embedded function under IT ("Organizations Changing Strategies," 2015).

Currently, only one community college within the state of Florida offers a B.A.S. in Cybersecurity, and no community colleges offer a fully online degree program, representing a dearth of educational accessibility for students in a high-demand region. Students seeking a B.A.S. in Cybersecurity degree include both new workers and incumbent workers looking to move up within their industry who need greater expertise and certifications to match changing technology. To make this education a reality, feasible options such as online learning must be available. Online programming allows for rapid update of content as new technologies and certifications are developed to meet the ever-changing face of cyber threats, as well as flexibility in scheduling and course attendance. Degree attainment at a community college also allows for a lower-cost option than colleges or universities, maximizing student benefit.

For several years, SPC has sought to offer a more technical cybersecurity subplan in its current B.A.S. IT degree and develop a standalone B.A.S. program in Cybersecurity, but has lacked capacity in reorganizing and developing curriculum and in updating equipment and faculty professional development. Through this project, SPC will be able to enhance capacity to meet workforce and student demand at a regional level while building a model program for other two- year institutions developing baccalaureate programs in cybersecurity-related fields.

Proposed Program

The overarching goal of the SPC Cybersecurity project is to increase the number of students pursuing a cybersecurity credential to meet the workforce needs of employers in the Tampa Bay region and beyond. This goal will be accomplished over a two-year period through

the following objectives: 1) Redevelop the existing B.A.S. in Information Technology Management's

Cybersecurity subplan curriculum to increase training opportunities for students; 2) Develop a new B.A.S. degree in Cybersecurity aligned with NSA/DHS National Centers of Academic Excellence in Cyber Defense Education; and 3) Improve faculty training and ability to offer industry-linked certifications in cybersecurity. By meeting these objectives, SPC will also strengthen regional and national partnerships with institutions in cybersecurity education, sharing resources and best practices for other community colleges seeking to develop B.A.S. programs.

Objective 1: Redevelop the existing B.A.S. in Information Technology Management's Cybersecurity subplan curriculum to increase training opportunities for students.

Outcome 1.1: Addition of 3 industry certifications to subplans by Spring 2020

Outcome 1.2: Development of 4 new course offerings for students by Summer

2020 Outcome 1.3: Implementation of new subplan in Cyber Defense by Fall 2020

Outcome 1.4: Integration of new technology to support student training

Outcome 1.5: Serve a minimum of 48 students in new subplan by Spring 2021

Year 1 of the SPC Cybersecurity project will incorporate new curriculum, courses, and industry certifications to create a new Cyber Defense / Applied Cybersecurity subplan in the existing B.A.S. in Information Technology Management degree. This new subplan will serve as the foundation for a separate B.A.S. in Cybersecurity degree, and will be differentiated from the existing subplans in its focus on technical training in cyber defense. Led by Program Manager and College of Computer and Information Technology (CCIT) Academic Chair Dr. John Duff, CCIT Dean Dr. James Stewart, and CCIT Academic Chair Laura Malave, a faculty team from SPC will work with representatives from CSSIA to develop an appropriate curriculum plan and source curriculum materials. In addition, CSSIA, industry partners and members of the existing CCIT Industry Advisory Board will participate in a Developing a Curriculum (DACUM) planning event

to present a workforce analysis and industry input on curriculum guidance. The Division of Florida Colleges recommends the DACUM prior to submitting a B.A.S. program plan for approval.

Curriculum plans will be guided by the Centers of Academic Excellence in Cyber Defense Education (CAE-CDE) framework, which maps to the National Initiative for Cybersecurity Education (NICE) Workforce Framework endorsed by Cyberwatch West. An A.S. degree in Cybersecurity or Computer Information Technology, or an A.A. with a Cybersecurity Certificate will be acceptable pre-requisite qualifications for participation in this program, satisfying the core, foundational, and technical requirements as specified by the CAE-CDE model.

An estimated four new courses will be developed under SPC's current Cyber Defense subplan, such as *Threat and Vulnerability Analysis* and *Security Auditing and Vulnerability Assessment.* Final determination of subplan courses will be made in consensus with the ATE Centers as well as industry partners. All courses will align with the Quality Matters standards, ensuring course outcomes are learner-centric, measureable, and aligned to student achievement. SPC will also seek innovation in its curriculum development by incorporating Capture the Flag challenge activities such as web exploits, data recovery, and cryptography that align with course objectives and demonstrate real-world applicability for students. CSSIA will support this initiative by involving SPC students in national cybersecurity skills competitions. In addition, students will be prepared to sit for a minimum of three industry certifications: CompTIA CySA+, CompTIA PenTest+, and CompTIA CASP. Attaining these certifications will prepare students for a wide range of employment opportunities and demonstrate that graduates are on the forefront of modern cybersecurity training. Necessary for this training will be enhanced cybersecurity technology capabilities for students. Through this project, CSSIA will

support SPC by providing access to their virtual cybersecurity range. In addition, SPC will expand its platform for delivering virtual

cybersecurity labs with equipment like a NETLAB+ server, which will allow for inclusion of programs such as the Palo Alto Cybersecurity Academy.

During the program development phase, SPC will also work with its industry partners, community liaisons, and marketing teams to outreach to potential students through program flyers, information sessions, and social media, driving interest and enrollment in the Cyber Defense subplan and subsequent B.A.S. degree. An estimated 48 students will enroll in these courses in Year 2 of the program.

Objective 2: Develop a new B.A.S. degree in Cybersecurity aligned with NSA/DHS National Centers of Academic Excellence in Cyber Defense Education

Outcome 2.1: Submission of B.A.S. program plan to accreditation body by Summer 2020

Outcome 2.2: Developing estimated 6 new courses for B.A.S. Cybersecurity by Fall 2021

Development of the Cyber Defense subplan will ultimately build new academic pathways

and support plans for a new, standalone and fully online B.A.S. degree in Cybersecurity, greatly expanding capacity and student degree options to meet workforce demand. During the first quarter of the project, program faculty will work with SPC's Academic Services department, industry representatives, and CSSIA consultants to revise the existing CCIT core course set, decreasing the number of required core courses and developing a broader base of elective courses in each of the degree subplans to complete the 45 credit hour B.A.S. requirement. Developed through the DACUM, plans for the new B.A.S. Cybersecurity program will be submitted to the state accreditation board during the second quarter of the project period. Approval for a new B.A.S. degree plan will take approximately one year. Upon plan approval, program faculty will then develop an estimated six new cybersecurity courses while also

sourcing program curriculum from CSSIA and other institutional partners. An estimated 150 students will benefit from these courses.

7

SPC intends to begin offering the full B.A.S. in Cybersecurity by Fall 2022. SPC will then seek to apply for CAE-CAD designation, which requires a minimum of three years of program delivery, by Fall 2025. Not only will the development of this degree benefit SPC students, faculty, and the regional workforce, it could serve as a model program for other community colleges. SPC will work with CSSIA as well as NSF ATE Centers Cyberwatch and Cyberwatch West to disseminate best practices and curriculum resources nationally.

Objective 3: Improve faculty training to offer industry-linked certifications in cybersecurity.

Outcome 3.1: Minimum of two faculty trained in key cyber certifications by Fall 2019

Outcome 3.2: Ongoing faculty professional development through leveraged resources

In order to provide students with cybersecurity certification training such as CompTIA CySA+, PenTest+, and CASP, faculty must themselves be trained and certified. During Phase 1, SPC will work with CSSIA to determine appropriate training opportunities and subsequently train a minimum of two CCIT faculty in the first year of the funding opportunity. Trained faculty would then be eligible to teach cyber defense subplan courses as well as newly developed B.A.S. coursework, expanding capacity for SPC faculty and course offerings for students. Partnership with CSSIA will leverage the center's ability to offer professional development courses at a reduced rate from standard industry training providers. SPC will also support ongoing CCIT faculty professional development through training allocations to the project.

Table 1 demonstrates a two-year timeline of the proposed objectives and activities.

Table 1--Objectives	1st Qtr	2nd Qtr	3rd Qtr	4th Qtr	5th Qtr	6th Qtr	7th Qtr	8th Qtr
New Cyber Subplan	DACUM	Course Dev. (4)			Offer New Subplan		Monitor/Evaluate	
New B.A.S. Degree		Submit App.	Wait on state response				Course Dev. (6)	
Faculty Development	Faculty Training / Certifications (3)				Continued Prof. Dev. and Dissimination			

8

Adequacy of Resources

As proposal lead, St. Petersburg College (SPC) will oversee day-to-day management of the grant project and implementation of all project objectives, activities, and deliverables. Key SPC resources include Institutional Resources and Personnel. Partnerships will also play a critical role in collaborating on project activities and outcomes.

Institutional Resources: SPC is a multi-campus institution in Pinellas County, Fla., that serves approximately 40,000 students per year. SPC offers more than 100 degree and certificate programs, including two dozen baccalaureate degrees, and has the largest online program of any Florida state college. This proposal builds on SPC's extensive experience and resources developed with federal grant programs, including Department of Education Title III and Student Support Services grants as well as National Science Foundation Advanced Technological Education (ATE) funding. The project will be supported by SPC's Grants Accounting and Grants Departments, which have oversight of fiscal matters pertaining to the grant, including helping with adherence to funder regulations and reporting. SPC Academic Services staff will assist in guiding B.A.S. development to assure alignment with state and national curriculum standards. Program personnel will be able to draw from these resources to ensure that the program is able to achieve stated goals and outcomes and develop innovative outcomes for students and the larger academic community.

Personnel: The program will be managed by **Dr. John Duff**, Baccalaureate Academic Chair for SPC's College of Computer and Information Technology (CCIT), who has more than 30 years' experience in industry and in higher education instruction. Dr. Duff teaches core and cybersecurity courses and leads curriculum development for the B.A.S. program. Dr. Duff will have primary oversight for the scientific integrity and fiscal and administrative management

throughout the grant period. Also engaged in program leadership will be Academic Chair **Laura**

9

Malave, who has more than 15 years in computer and information technology instruction and coursework design, serves as a Co-PI on SPC's NSF ATE grant in Biomedical Engineering Technology, and holds more than 20 industry certifications. CCIT Dean **Dr. James Stewart** will also advise on the project. Prior to joining SPC, Dr. Stewart served as the Program Director for Cyber Security and Information Security Information Technology at Keiser University, and has more than 20 years' experience in industry leadership and cybersecurity research. The project team will work with additional CCIT faculty, SPC's existing CCIT Industry Advisory Board, and project partners to implement all facets of the program.

Partnerships: SPC's primary collaboration partner in the Cyber Defense project will be the **Center for Systems Security and Information Assurance** (CSSIA), an NSF ATE national resource center at Moraine Valley Community College. This project aligns with CSSIA's charter to maintain and develop cybersecurity related curriculum content including instructional materials, assessment instruments, lab activities and virtual student skills competition environments as well as to build a national infrastructure of qualified cybersecurity educators. Project member Laura Malave has mentored with CSSIA leadership in working toward the A.S. in Cybersecurity CAE2Y designation application; this project is a natural extension of those activities in continuing to support best practices and excellent education options in cybersecurity programs at SPC. Under this project, CSSIA will provide: 1) technical assistance and expertise in curriculum design as well as access to national student cybersecurity competitions; 2) faculty professional development for industry certifications; and 3) dissemination channels for developed curriculum and sharing of project results with other community colleges at a national level. As appropriate, SPC will also collaborate with Cyberwatch and Cyberwatch West to source

Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges
curriculum and share project results.

10

In addition to the NSF ATE resource centers, this project engages multiple industry partners at the forefront of global cyber security employment. SPC has built strong relationships with industry leaders through its CCIT Advisory Board to support program development and oversight, student engagement, training, and employment. For this project, SPC will work with the CCIT Advisory Board and partners such as **CISCO**, **CISCO Networking Academy**, and **ReliaQuest**. Each of these partners demonstrates a breadth of experience in information technology and cybersecurity, and will assist in the following activities: 1) advisement on development of program curriculum and participation in DACUM planning; 2) advisement on employer needs and emerging trends in cybersecurity workforce; 3) potential consideration of students for internships and employment opportunities.

Reasonableness of Proposed Expenditures: SPC has developed a cost-effective budget that reduces overall costs of expanding technological updates by leveraging internal and external resources, such as CSSIA's open source curriculum and reduced faculty training costs. The total proposed budget of $91,115 includes curriculum development, technology purchase, and faculty professional development, which aligns directly with the intent of the proposal. Expenditures will support long-term sustainability with tuition collected from new course offerings and programs. The budget is also justified in the project's potential for national significance; not only will other institutions benefit from shared curriculum resources, but students outside of Tampa Bay will be able to take advantage of the program's fully-online capabilities to earn a cybersecurity degree.

Evaluation

SPC anticpates enrolling a minimum of 200 students in the year immediately following the

grant period. To measure the success of the project and achievement toward outcomes outlined in the Program Plan, program staff will work with SPC's Institutional Research and Effectiveness,

Assessment, and Curriculum departments for formative and summative assessments of quantitative and qualitative data. SPC utilizes Pulse Business Intelligence (Pulse BI), a data tracking system that allows faculty and staff direct access to multiple layers of student data and outcomes. **Pulse BI data review** will inform on qualitative course enrollment and student outcomes, showing changes in enrollment and student success. On a course and program level, SPC's Curriculum Department promotes student success by reviewing program goals and outcomes and course outcomes and objectives. This **Comprehensive Academic Program Review** process aligns with the Quality Matters standards, a set of 8 general standards and 43 specific review standards to evaluate the design of a course. This collaborative process to analyze qualitative and quatitiative data results in the continuous improvement of academic programs and courses and ensures that students graduate ready to enter the workforce or excel in their current careers. During Year 2 of the project, monitoring and evaluation of the new subplan curriculum will allow for identification of and adjustment for any needed changes to improve student learning and outcomes. In addition, evaluation of partner and industry response to program objectives will be critical to determine program alignment with industry standards. Program staff will work with SPC Assessment to administer an **Annual Viability Report,** which includes industry partner review and feedback to ensure program alignment with industry standards in curriculum design and student training. Program staff will provide quarterly and annual progress reports, including actionable recommendations to college administration and the advisory board; and provide ongoing consultation with CSSIA staff and CCIT advisory board to address status of the project and any perceived barriers to progress toward objectives. Strategies and lessons learned will be disseminated to all project partners, as

well as to other institutions of higher education seeking to reevaluate or establish cybersecurity degree programming.

BIBLIOGRAPHY

Bumiller, E., and Shanker, T. (2012, October 11). Panetta Warns of Dire Threat of Cyberattack on U.S. *The New York Times*. Retrieved from nytimes.com/2012/10/12/world/panetta- warns-of-dire-threat-of-cyberattack.html

CareerOneStop. (2015, July 01). Retrieved from http://www.careerinfonet.org/

Cybersecurity Supply and Demand Heat Map. (n.d.). Retrieved from https://www.cyberseek.org/heatmap.html

Manning, M. (2018, March 22). Where Tampa-St. Pete ranks among the areas most vulnerable to cyberattacks. Retrieved from https://www.bizjournals.com/tampabay/news/2018/05/22/where-tampa-ranks-among-the- cities-most-vulnerable.html

Morgan, S. (2016, January 17). Cyber Crime Costs Projected To Reach $2 Trillion by 2019. Retrieved from https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime- costs-projected-to-reach-2-trillion-by-2019/#25f928eb3a91

Occupational Outlook Handbook. (2018, April 13). Retrieved from https://www.bls.gov/ooh/computer-and-information-technology/information-security-analysts.htm#tab-6

Organizations Changing Strategies and Tactics as Security Environment Gets More Complex, New CompTIA Study Finds. (2015, March 31). Retrieved from

https://www.comptia.org/about-us/newsroom/press-releases/2015/03/31/organizations- changing-strategies-and-tactics-as-security-environment-gets-more-complex-new- comptia-study-finds

Restuccia, D. (2018, March 29). How to Get a Cybersecurity Job in Three Charts: A Degree, a Certification, and a Clearance. Retrieved from https://www.burning-glass.com/blog/how- to-get-a-cybersecurity-job-in-three-charts-a-degree-a-certification-and-a-clearance/

State University System of Florida Board of Governors. (2013). Florida Center for Cybersecurity: Making Florida the Cyber State (Rep.). Tallahassee, FL.

STEM jobs: Tampa Bay leads Florida but can it become a bigger tech player? (2015, October 08). Retrieved from http://www.tampabay.com/news/business/stem-jobs-tampa-bay- leads-florida-but-can-it-become-a-bigger-tech-player/2248874

Tampa Bay Information Technology Workforce Analysis (Rep.). (2015, November). Retrieved http://www.careersourcetampabay.com/files/public/Tampa_Bay_IT_Workforce_Analysis _Report_2015.pdf

Wirth, A. (2016). The Importance of Cybersecurity Training for HTM Professionals. Biomedical Instrumentation & Technology, 50(5), 381-383. doi: 10.2345/0899-8205-50.5.381

2

Budget Narrative File(s)

*** Mandatory Budget Narrative Filename:** FIPSE Cybersecurity Budget Narrative.pdf

Add Mandatory Budget Narrative | Delete Mandatory Budget Narrative | View Mandatory Budget Narrative

To add more Budget Narrative attachments, please use the attachment buttons below.

Add Optional Budget Narrative | Delete Optional Budget Narrative | View Optional Budget Narrative

Personnel: $ 28,738

Faculty/Staff Deliverables –

Program Management: Funding is requested to support the time and effort of a staff or faculty member to oversee the project. Tasks would include communication with the funder and partners, project management, reporting, budget oversight and program evaluation.

Course Development: Funding is requested to support the development of additional courses related to the new Cybersecurity subplans and proposed Baccalaureate degree. Tasks would include engagement with ATE partners to align curriculum, alignment of curriculum with FL standards, development of course outlines, identification of major learning outcomes, creation of course syllabus/content, etc.

Category	Year 1	Year 2	Total	Description
Personnel				
Deliverable Pay: Program Management	$ 2,613	$ 2,613	$ 5,225	Estimating 1 faculty/staff @ $1306.25 per deliverable x 2 deliverables per year to support program.
Deliverable Pay: Course Development	$ 10,450	$ 13,063	$ 23,513	Estimating $2,612.50 per faculty per course (2 deliverables per course @ $1,306.25 per deliverable) at institutional rate for upper level B.A.S course development for 4 courses developed in Year 1 and 5 courses in Year 2.

Fringe Benefits: $4,598

SPC policy covers deliverable pay for staff/faculty at 16%, which includes Medicare 1.45%; Social Security 6.2%; Retirement 7.92%. Yr 1: $12,613 x 16% = $2,090; Yr 2: $15,113 x 16% = $2,508. **Total = $4,598**

Travel: $12,000

Funding is requested for travel to attend offsite meetings, as well as to support travel to and attendance at conferences for the purpose of training, professional development, partner engagement, dissemination and learning. Estimating 2 trips per year for 2-3 staff to attend National Conferences and related training/professional development such as CompTIA Partner Summit + CompTIA Instructor Network Training Sessions, Community College Cyber Summit (3CS), the National Initiative for Cybersecurity Education (NICE) Conference, etc. Estimating $1,500 per person per trip to include airfare, hotel, registration, ground transportation, per diem, etc. x 2 trips per year x 2 staff. Estimating Yr 1: $6,000; Yr 2: $6,000. **Total = $12,000.**

All travel is consistent with SPC Policies and Procedures and reviewed by the College's Grants Accountant to ensure it complies with grant expenditure guidelines.

1

Equipment: $9,700

Funding is requested to support the purchase of a server, which will provide an expanded platform for delivering virtual cybersecurity labs. This technological upgrade will allow for the inclusion of additional curriculum such as that from Palo Alto as part of the Cybersecurity Academy and/or others. Estimating cost of server Yr 1: $9,700. Total= $9,700

Other Direct Costs: $21,791

Printing: Funding is requested to support the design, publication and distribution of program materials, such as brochures and advisements, online resources, website upgrades, etc. Primary production will take place in Year 1 after SPC has redesigned the new Cybersecurity subplans/courses. Estimating Yr 1: $2,000; Yr 2: $1,500. **Total = $3,500.**

Consultant(s): Funding to support Subject Matter Expert(s) provided through partner NSF ATE Center(s) including consolations and advisement on curriculum alignment, workforce engagement, faculty development, etc. Estimating all-inclusive rate hourly rate of $50 per hour x 100 per year. Estimating Yr 1: $5,000; Yr 2: $5,000. **Total = $10,000.**

Faculty Development: Funding to support faculty as they gain the necessary industry certifications required to teach additional and/or updates courses including the cost of Certification Prep Courses and related professional development courses through ATE partner(s) and cost of Industry Certification Test Vouchers. *Test Prep*: Estimated at $199 per 1-week online course x 3 courses x 2 faculty in Yr 1 =$1,194; Yr 2 = $597. *Test Vouchers:* Estimated at 2 faculty receiving 3 additional certifications x $1500 per person in Yr 1 = $3,000; 1 faculty in Yr 2 = $1,500. Certification may include Certified Information Systems Security Professional (CISSP), Systems Security Certified Practitioner (SSCP), Certified Cloud Security Professional (CCSP), etc. Estimating Yr 1: $4,194; Yr 2: $2,097. **Total = $6,291.**

Facilitation: Funding is requested to cover the cost of serves and expenses related to hosting a Develop a Curriculum Meeting (DACUM). Estimating cost of half-day facilitated session including interactive technology, strength-based techniques and real-time documentation involving subject matter experts in the field of Cybersecurity and business leaders to support curriculum development, industry certification alignment, etc. Estimating Yr 1: $2,000. **Total =**

$2,000.

Total Direct Costs: $76,827
Total Direct Costs Yr 1: $44,047; Total Direct Costs Yr 2: $32,780. **Total = $76,827**

Indirect Costs: $6,713

SPC is requesting indirect support in the amount of $6,713 over the two-year grant period. This amount is calculated using 10% of SPC's federally negotiated modified indirect cost rate with U.S. Health and Human Services of 33% on-campus, less equipment and contracts over $25,000. Yr 1: $34,347 x 10% = $3,435. Yr 2: $32,780 x 10% = $3,278. **Total = $6,713**

Total Request: $83,540

Total Request Yr 1: $47,482; Total Request Yr 2: $36,058. **Total = $83,540**

Other Attachment File(s)

*** Mandatory Other Attachment Filename:** FIPSE Cybersecurity CVs.pdf

Add Mandatory Other Attachment | Delete Mandatory Other Attachment | View Mandatory Other Attachment

To add more "Other Attachment" attachments, please use the attachment buttons below.

Add Optional Other Attachment | Delete Optional Other Attachment | View Optional Other Attachment

John A. Duff, Ph.D.
Baccalaureate Academic Chair--St. Petersburg College
727-341-7176; duff.john@spcollege.edu

Employment History

St. Petersburg College, St. Petersburg, FL **2017-Current**
Baccalaureate Academic Chair - College of Computer and Information Technology

Responsible for the delivery of the college's Bachelors of Science program within the College of Computer and Information Technology. Teach primarily core and cyber security courses, recruit, equip, and guide adjunct faculty. Advise and mentor students. Review and revise BAS curriculum. Course owner for multiple courses. Participate on college committees and groups as required.

Eckerd College, St. Petersburg, FL **2007-2017**
Director – Information Technology Services

Responsible for all aspects of the colleges' Information Technology and information resources including computing, media services, academic resource center, back-end web services, telecommunications, classroom technology systems, administrative software systems, Banner team, printing and copier services, etc. Responsible for aligning IT with the strategic direction of the college.

Led conversion effort to Google Apps, wrote grant proposals that delivered over $400,000 in technology to the college, transitioned the college to the Florida Lambda Rail network for Internet services, oversaw expansion and upgrade of wireless network access to all areas of campus, increased Internet bandwidth from 40mbs to 1.5gbs, participated in the design and implementation of network and advanced classroom technology for several major building projects, renegotiated Cable TV and Print/Copy contracts resulting in substantial savings to the college, led the first successful document imaging and management project on campus, led upgrade of the campus telephone system and began a successful conversion to VOIP, initiated the transition to cloud-based services (AWS) as a strategic direction and in support of the college's business continuity plans, led deployment of print management software for student printing resulting in a reduction of over 30% in paper consumption, led upgrade of the college's core network service architecture, coordinated the implementation of a mass texting system, siren, and digital signage to support emergency notifications. Leading a complete replacement of the residential network.

Eckerd College, St. Petersburg, FL **2001-2007**
Director – Program for Experienced Learners

Responsible for all support and administrative processes for the Program for Experienced Learners (PEL) at Eckerd College. PEL is a Bachelor's degree program that targets adult students 23+ years old, operates on five campuses, enrolls over 700 students. Initiated PEL's web-based education program. Chaired online working group, developed course standards, deployed first Eckerd College blended format courses. Chaired the PEL strategic planning committee. Established first ever PEL Student Advisory Group. Directed program marketing. Initiated online advertising campaign for the program. Reversed several years of declining registrations. Wrote winning grant proposal for Benard Osher Reentry Scholarship program.

Also served as Discipline Coordinator for the Information Systems Concentration and in this role developed the Information Systems (IS) major for PEL. Responsible for all aspects of this academic program including curriculum development, instruction, and faculty recruitment. Regularly taught four courses per year in Information Systems.

Created both a certificate and degree program for the intelligence community at U.S. Central Command (CENTCOM) at MacDill AFB in Information Management and Analysis. Worked with the CENTCOM Regional Joint Training Facility to design, develop, and deliver the program to the local intelligence community. The program is designed to develop skill sets required by Intelligence Analysts.

Largo Electronic Commerce Resource Center and Eckerd College, Largo, FL 1997- 2001
Director of Education and Training

Managed all aspects of Eckerd College's participation in the Electronic Commerce Resource Center (ECRC) program. The ECRC program was funded by the Department of Defense (DoD) and charged with the mission of providing education and consultative, technical support to DoD suppliers in support of the DoD's electronic commerce initiatives. Managed a staff of professional trainers/consultants who provided services to DoD suppliers throughout Florida and Puerto Rico. Developed, coordinated, and maintained a curriculum of over 20 courses in support of DoD initiatives and underlying technologies. Served as Florida's representative to the national ECRC Education and Training Working Group. Trained over 5,000 individuals representing over 2,500 organizations in Florida each fiscal year.

Ameritech Corporation – Electronic Commerce Business Unit, Brecksville, Oh 1995-1997
E-Commerce Architect

E-Commerce Application Architect for Ameritech's Electronic Commerce Business Unit. Architect for a unique electronic commerce application delivered to the Superior Court of Los Angeles County, Los Angeles, CA. Managed the participation of three consulting groups supporting the CivicLink project across multiple geographic locations. This application automated the workflow of legal documents and enabled attorneys to search, retrieve, review, and file legal documents from remote locations. This was one of the first implementations of digital signatures in the U.S. and required significant changes in the court rules for the Superior Court. Led development of integrated workflow and imaging system to support the application. Application piloted and delivered to Probate Court and Santa Monica Civil Court.

Ameritech Corporation, Brecksville, Oh 1990-1995
Lead Data Analyst

Served as an internal consultant to software development teams across Ameritech Corporation for data modeling and data base design. Accumulated over 200 hours as a JAD facilitator in a wide variety of contexts. Built and maintained logical and physical data models using a variety of CASE tools. Developed data modeling standards for Ameritech systems development. Coordinated Customer Data Model for Ameritech Business Units.

Ameritech Corporation, Brecksville, Oh 1989-1990
Senior Analyst

Provided project management and systems development support for Ameritech migration to a new Order/Billing Systems. First analyst selected in Ohio to support this project. Project integrated five Order/Billing systems deployed throughout the five-state Ameritech Region. Also participated on the design team for Ameritech's Marketing Information Warehouse database.

Ameritech Corporation, Brecksville, Oh 1984-1989
Analyst

Programmer/Analyst supporting financial systems. Lead programmer for Mechanized Accounts Payable Systems (MAPS). Negotiated, designed, implemented, and tested numerous system enhancements. System executed 20,000 transactions per month, paid, and journalized over $1 billion.

Ohio Bell - Ameritech Corporation, Columbus, Oh 1981-1984
Bell System - Certified Account Executive – Industry Consultant

Certified Bell System Account Representative at Industry Consultant Level within 12 months of initial hire as Account Executive. Demonstrated expertise in Transportation Industry Segment and exceeded all sales objectives for voice and data products. Participated on national account teams to execute sales to railroad and trucking company accounts. Managed a team of support personnel who designed, ordered, and implemented solutions.

Bowling Green State University, Bowling Green, Ohio **1978-1981**
Instructor - Department of Management
Accepted invitation to remain at Bowling Green State University to teach required sections of undergraduate management courses. Taught management theory and organizational behavior.

Education

- **Kent State University:** *Ph.D.* Major: Management Information Systems; Minor: Int'l Business
- **Bowling Green State University:** *Masters of Business Administration*
- **Westminster College:** *Bachelor of Arts*

Teaching Experience

Currently teaching Information Security Policy Administration, Security Essentials, Management Information Systems, Systems Development Methodologies, Core Security Principles, Application Security, Senior Capstone. Have taught: various Information Systems courses, including MIS, Systems Analysis, Advanced Systems Analysis, Database, Advanced Database, Networking, Internet Programming, and E-Commerce; MIS for the MBA program at Kent State University; Introduction to Business and Organizational Behavior at Bowling Green State University.

Professional Awards, Honors, Certifications

- Department of Defense Electronic Commerce Day Recognition for development and deployment of an innovative electronic commerce solution in the small business category.
- Awarded U.S. Central Command J2 (Intelligence) Commander's Coin of Excellence for implementing a degree and certificate program.
- Awarded Commander's Coin of Excellence from the Defense Contract Management Agency for delivering exceptional training.
- Received Ameritech's Call to Excellence Award on three occasions. Call to Excellence Awards signify outstanding achievement or innovative problem solving.
- Certified Account Executive – Industry Consultant: Highest level of professional marketing certification established by the Bell System and resulting deregulated entities.
- Certified - ITIL Foundation
- Quality Matters - Applying the QM Rubric - Certificate of Completion
- Certificate - Teaching an Online Course - St. Petersburg College

Publications and Conference Proceedings

- Ph.D. Dissertation - A study of the Differences between the Relational Data Model and the Entity-Relationship Model in the Context of Integration, defended November 1994.
- Electronic Commerce and the Judicial System, White Paper published by Ameritech Corporation
- Integrating Data Models into the Corporate Logical Data Model, White Paper published by Ameritech Corporation
- Data Management Handbook – Systems Standard published by Ameritech Corporation
- Data Management Toolsbook – Systems Standard published by Ameritech Corporation
- Howard, Geoffrey S. and Duff, John A. "An Experimental Comparison of the Integratability of EER versus RDM Data Models," submitted to Decision Sciences, February, 2000.
- Duff, John A. and Howard, Geoffrey S. "Task Difficulty and Semantic Strategies for EER versus RDM Data Model Integration," submitted to Journal of Database Management, March, 2000, invited for revision and resubmission, July 2000.
- Howard, Geoffrey S. and Duff, John A. "Data Model Integration: A Review of the Research State of the Art," submitted to Journal of Information Technology, April, 2000.

Laura Malavé
P.O. Box 340234, Tampa, FL 33694--(813)416-1126—malave.laura@spcollege.edu

Areas of Expertise

- Industry Certifications:
  - Juniper: JNCIA-JUNOS
  - LPI: Linux Essentials
  - Microsoft Office Specialist: 2010 Master Specialist, Word 2010, Excel 2010, PowerPoint 2010, Access 2010, Outlook 2010, Word Expert 2010, OneNote 2010, SharePoint 2010, Office 365, Excel Expert 2010, Word 2013, Excel 2013, PowerPoint 2013, Outlook 2013, Access 2013, OneNote 2013, SharePoint 2013, Office 365
  - Microsoft Technology Associate: Windows Operating Systems Fundamentals, Windows Server Administration Fundamentals, Networking Fundamentals, **Security Fundamentals**, Software Development Fundamentals, Database Fundamentals
  - Microsoft: Technology Literacy for Educators
  - CIW: Web Design Professional, Web Design Specialist, E-Commerce Specialist
  - CompTIA: A+ CE, Network+ CE, Server+, **Security+ CE, Cyber Security Analyst+**, Project+, Cloud+, Mobility+, Healthcare IT Technician, Cloud Essentials, Strata IT Fundamentals
  - Ec-Council: **Certified Ethical Hacker**
  - VMware Certified Associate: Data Center Virtualization, Workforce Mobility, Cloud
  - Adobe: Dreamweaver CS4
- Programming Languages: Alice, ASP.NET, C/C++/C#, Java, JavaScript, PHP, SQL, VB, Shell Scripting
- Quality Matters: Development Facilitator, Internal/External Peer-Reviewer, Higher Ed Publisher Review, Information Technology, Computer Science, **Cybersecurity QM Subject Matter Expert**

Professional Experience

Academic Chair, Computer and Information Technology
St. Petersburg College, Midtown/Downtown Campuses – July 2015 – present
Developed Computer Repair Program/Lab at the Midtown Campus. Doubled enrollment in 1 year.

Course Owner: CTS1120 Network Security Foundations, CIS1358 Operating Systems Security, CGS2811 Incident Response and Disaster Recovery, CTS1314 Network Defense and Countermeasures, and CIS2352 Ethical Hacking.

Taught: CTS1120, CIS1358, CIS2352, COP1000 Introduction to Computer Programming, CGS1100 Computer Applications, CET1171 Computer Repair Essentials, CET1172 Computer Support Technician, CTS2940 Cybersecurity Internship, ISM4320 Core Security Principles, ISM4321 Strategic Cybersecurity Enforcement

Assists the Dean at the campus level, overseas the cybersecurity AS and Certificate program
Assist the college in developing and maintaining a quality program of instruction, provide service to the college and continuing professional development.
Interviews, recommends, mentors, and evaluates adjunct instructors

Committees: Women2STEM, Academic Assessment Sub-Committee, Academic Chairs Committee, CCIT Faculty and Chair Hiring Committees, Communications Chair Hiring Committee, Midtown Hispanic Heritage Committee, CETL Adjunct Advisory Board, Midtown Technical Support Specialist Hiring Committee

Initiatives:

Cybersecurity/Digital Forensics Club Advisor
Club placed 3rd at the Raymond James Capture the Flag Competition
Summer 2016 Delta Leadership Academy Participant
Added NetLab+ Virtual Labs and Cengage MindTap Digital Platform to CTS1120, and CIS2352

Summer Institute 2016 – SPC Academic Pathways
SPC Fall STEM Festival committee member and volunteer
Midtown QEP Ambassador

Awards:

2016 League of Innovation Excellence Awards in Teaching and Learning in the category of: Innovation in the Use of Technology. (Awarded for the addition of NetLab+ and Cengage MindTap to CTS1120 and CIS2352 to enhance the experience of online and blended learners using virtual machines, and a digital platform.)

Grants:

NSF-ATE Grant Application Co-PI, Biomedical Engineering & Cybersecurity
SPC Innovation Grant 2016, Digital Forensics & Cybersecurity Lab

Information Technology Instructor
Keiser University – Tampa Campus May 2011 – present

Prepared course plans and materials:

CGS 1000 Introduction to Computers (on-ground and hybrid)
CTS1305C Essentials of Networking (CompTIA Network+)
CTS1328C Managing and Maintaining Server Operating System (Microsoft 70-411 Administering Windows Server 2012)
CTS2106C Multi-User Operating Systems (CompTIA Linux+)
CTS2306C Implementing a Network Infrastructure (Microsoft 70-412 Configuring Advanced Windows Server 2012 Services)
CTS2153C Application Support (70-688 Managing and Maintaining Windows 8.1)
CTS2302C Implementing Directory Services (Microsoft 70-411 Administering Windows Server 2012)
CTS2304C Internetworking Technologies (Cisco CCENT)
CET1171C PC Service and Support I (CompTIA A+)
CET1172C PC Service and Support II (CompTIA A+)
CET2350C Principles of Information Security (CompTIA Security+)
CTS1156C Supporting Client Operating Systems (Microsoft 70-680 Windows 7, Configuring)
COP2843 Web Systems (PHP/SQ, L)

New initiatives implemented:

Associates in Information Technology student population growth by 400+%
Certiport Testing Center
Hybrid Associates Information Technology degree
Monthly Center for Advanced Technology guest speakers
Monthly class fields trips to local industry partner locations
Create/update Blackboard content for ASIT courses, and CGS1000 hybrid

Additional duties include: (MAKE LIST WITH SEMI-COLONS)

Academic Advising; Liaison with Information Technology community in the Tampa Bay Area
Coordinate bi-annual ASIT Advisory Board; Deliver Information Technology High School workshops
Manage and maintain ASIT classroom and lab equipment; Deliver Product Knowledge presentation for Academic Advisors; Supervise student repair of student, staff, and faculty personal PCs and laptops
Conduct Information Technology Industry Certification Test Preps; Manage campus Microsoft IT Academy
Manage CompTIA Authorized Academy Partnership; Manage LPI (Linux Professional Institute) Academy Program; Mentoring of Center for Advanced Technology faculty

Instructional Multimedia Developer
University of South Florida, eTeaching & Technology Group, Tampa, Fl March 2010 – March 2011

Support faculty use of instructional software and technology.
Conduct faculty development workshops on the effective use of technology in the classroom and through distance learning.
Develop eLearning materials for faculty support in technology and teaching.

Computer Science Instructor
Hillsborough Community College – Brandon Campus, Tampa, Florida January 2006 - May 2009
Designed Coursework and Taught (on-ground, online, and hybrid):
CGS 1000 Introduction to Computers & Technology
CGS 1550 Introduction to Networking
COP 1000 Programming Logic
COP 1220 C Programming
COP 2939 Programming Capstone
CGS 2541 Database Design
CGS 1555 Introduction to Internet
COP 2360 C# Programming
CET 1172C Computer Hardware & Repair
OST 1100 Beginning PC Typing

Committees: Hispanic Heritage Celebration - Chair, Campus Advisory Council, Institutional Advisory Council, Safety Committee, HCC Foundation Mini-Grant Panel

Adjunct Computer Science Instructor
Hillsborough Community College – Dale Mabry Campus, Tampa, Florida August 2003 - December 2006
Designed Coursework and Taught:
COP 2244 C++ Programming
COP 2344 Shell Scripting
CGS 1107 Introduction to Computers
CGS 1936 Perl & CGI
SLS 1502 College Success
CGS 1000 Introduction to Computers and Technology

Teaching Assistant
University of South Florida, Tampa, Florida Summer 2001
Introduction to Computers and Programming in Basic
Training Program for International Teaching Assistants Summer 2000, 2001, 2002, and 2003

Volunteer Academic Advisor
University of South Florida's President's Academy of Advisors 2004 – 2005

Education

Ph.D. Student in Computer Science and Engineering Summer 2003 - Fall 2004
Department of Computer Science and Engineering, University of South Florida
NSF/USF IGERT-SKINS Fellow and Latino Graduate Fellowship Recipient

Masters of Science in Computer Science Summer 2003
Department of Computer Science and Engineering, University of South Florida
Latino Graduate Fellowship Recipient and Departmental Research Assistantship
Master's Thesis: *Silhouette based gait recognition research resource and limits*. The generation of a database of manual silhouettes of gait sequences, an evaluation and comparison of their performance.
Publications: SPIE 2004 - Manual Gait Silhouettes Creation and Gait Recognition
CVPR 2004 - Studies on Silhouette Quality and Gait Recognition

Additional Graduate Coursework: Community College in America, Seminar in College Teaching

Bachelor of Science in Computer Science - Magna Cum Laude - Spring 2001
Department of Computer Science and Engineering, University of South Florida

Professional Organizations:

ACM
(ISC)² Tampa
OWASP Tampa
Tampa Bay Electronic Crimes Taskforce
Women Who Code Tampa Bay
IEEE-CS
Tampa Bay Technology Forum
Infragard Tampa
Florida Association of Community Colleges
ISSA Tampa
ISACA
DefCon813

JAMES H. STEWART Jr., D.Sc., MA, ITIL
Stewart.James@spcollege.edu

EDUCATION

- **Doctor of Computer Science,** Colorado Technical University; Emphasis: Information Assurance
- **Master of Arts**, Antioch University, McGregor School; Emphasis: Management
- **Bachelor of Science Business Administration**, Xavier University; Emphasis: Business Administration, Finance

ACADEMIC CAREER

St. Petersburg College, July 2, 2018 – To Present
Dean, College of Computers and Information Technology
Provide governance and oversight for the College of Computers and Information Technology. Provide vision and plans, develops and coordinates implementation of short and long-term strategies for the School of Computer and Information Technology. Assist in the implementation of the St. Petersburg College mission, vision, goals, academic standards and policies of the St. Petersburg College. Approve and provide direction for new program development and program/course revisions. Work to improve and enhance the curriculum to address the needs of the community, students and industry. Lead program level assessment of student learning and oversight of efforts on accreditation.

Keiser University- Fort Myers, Florida, August 2016 – to July 2018
Program Director/Department Chair Information Technology & Cyber Forensics/Information Security
Provide the resources for a quality learning experience for students by ensuring coherence in the discipline and relevance to the practice. Provide and initiate activities that support student learning outcomes, program quality, and discipline integrity, all of which focus on student learning and retention. Collaborate with the Academic Deans to provide a comprehensive learning experience for students and a cohesive work environment for faculty. Responsible for program curriculum quality and continuous improvement in existing programs and curricular evaluation and development by overseeing assessment and academic program review activities. Update and develop program content and materials and/or delivery methods, based on information such as emerging practice changes in the discipline, instructional effectiveness data, current or future performance requirements, feasibility, and costs.

Accomplishments

- Maintained 100 percent retention of students in the information technology and cyber forensics program
- Within 3 months, recruited Six National C-level executives in the Cyber forensics domain for the cyber forensics Advisory Board.
- Increased the number of students in the information technology and cyber forensics program by 20 percent in three months

Committees & Memberships

- Member, US Secret Service - Tampa Bay Electronic Crime Task Force - (ISC)²® Tampa Chapter
- Reviewer, International Journal of Hyperconnectivity and the Internet of Things (IJHIoT)
- Fort Myers- Retention Committee, Fort Myers -Chair Information Technology & Cyber Forensic Advisory Committee
- Fort Myers - Program Expansion/Marketing Recruitment Committee,
- University Department Committee for Information Technology
- University Department Committee for Cyber Forensics/Information Security

External Service

- Technology panel member for the Southwest Florida Chamber of Commerce Technology Forum2016 Technology Breakfast Seminar. 11-2016

Conferences

- Cyber Ready, 2016 Cybersecurity Conference, 10-2016
- The 2016 Techno Security & Forensics Investigations Conference / Mobile Forensics World.6-2016

Florida SouthWestern State College – Fort Myers, Florida, August 2015 –August 2016
Professor Computer Science

- **Committees include**: Academic Research Committee, Business Professor Selection Committee and Computer Science Professor Selection Committee, New Faculty Experience Advisory Group and Assessment Quality Group.

Adjunct Teaching positions:

Roosevelt University – Chicago, Illinois, August 2013 to present (Affiliation)
Adjunct Professor Information Systems, (Graduate Courses – Management and Information Systems)

Colorado Technical University – Online; 2008 to present (Affiliation)
Associate Professor - Adjunct, Computer Science & Information technology (Undergraduate and Graduate Courses)

Xavier University – Cincinnati, OH; 1999 to 2000
Adjunct Professor, Business & Computer Science (Undergraduate and Graduate Courses)

Regis University – Bolder, Bolder Colorado 2016
Affiliate Professor, College of Information Systems

Research Interest
Social Engineering Susceptibility
Cyber Security
Management Enterprise Corporate Governance

Course Development
CTS2142 Project Management
SWE440 Software Project Management
CFI4473 Digital Media Forensics
CFI4477 Computer System Forensic Analysis
CFI4479 Network Defense and Countermeasures

Awards
Department Of Defense – Computer Security Program
• Accommodation - Knowledge of Computer Systems (1987)

General Electric Aircraft Engines – ATO Group (1987)
• Achievement Award - Developed operating system procedures approved by the Department of Defense to allow multi-level classified processing on a single computer system. This resulted in utilizing only one Digital VAX 8700 computer instead of using two computers systems. This procedure reduced the cost to fulfill the Department of Defense contract, received award from the engineering department for designing and implementing the method (1987).

Mr. Charles Scheper, President Great American Insurance Company (Scheper Commission)
• Certificate of Appreciation – Volunteer services for Covington Kentucky operational efficiency project (2000)

Publications
Stewart, J., & Dawson, M. (2018). How the Modification of Personality Traits Leave One Vulnerable to Manipulation in Social Engineering, *International Journal of Information Privacy, Security and Integrity* (IJIPSI), Vol. 3, No. 3, 2018, DOI: 10.1504/IJIPSI.2018.10013213

Social engineering deception susceptibility: Modification of personality traits susceptible to social engineering manipulation to acquire information through attack and exploitation – Dissertation (2015)

Integrated cycle analysis risk model (ICARM) - Copy write registration number: TXu-460-937 (June 1990)

Certifications
IT Infrastructure Library (ITIL) Foundation

Professional Organizations

Association for Computing Machinery
IEEE Standards Association

INDUSTRY WORK EXPERIENCE

UNIVERSITY CENTRAL FLORIDA FOUNDATION - Orlando, Florida June 2008 to July 2012
AVP & CHIEF INFORMATION OFFICER

- Provide strategic direction, responsible for management of key corporate relationships.
- Liaison to the external community, individuals, agencies, engage and collaborate with high-level institutional officials, policy board members and colleagues.
- Implemented cloud computing solution infrastructure as a service, which resulted in increased reliability, availability, cost containment and cost reduction.
- Lead development and execution of an enterprise-wide disaster recovery and business continuity plan
- Replaced process and integrity challenged ERP\CRM System and implement CRM\ERP system,data warehouse, and Business Intelligence successfully and under project budget.
- Replace static website with dynamic e-commerce class website utilizing open source content software
- Reduced operational costs 25% while increasing hardware uptime from 70% to 99%
- Transitioned firm to employ reusable object oriented programming modules for applications development slashing time-to-deliver by 75%
- Implemented cloud computing solutions: infrastructure as a service, software as a service, platform as a service that resulted in increased reliability, availability, cost containment and cost reduction of core business applications.
- Implemented rigorous development and testing processes decreasing software defects by 90%

ROBERT HALF MANAGEMENT RESOURCES \ Protiviti - Orlando, Florida & Chicago Illinois October 2004 to August 2015 – contract consultant
INTERIM CIO /TECHNOLOGY CONSULTANT/ IT RISK & SOX CONSULTANT

- Provide strategic direction, responsible for management of key corporate relationships.
- Liaison to the external community, individuals, agencies, engage and collaborate with high-level institutional officials, policy board members and colleagues.
- Delivered technology management and consulting expertise for a wide array of clients ranging from startup entities in the non-profit business sectors.
- Engagements included interim Chief Information Officer, Interim Information Security Officer, business continuity plan development, implementation of IT governance structure, Sarbanes Oxley, HIPPA security and compliance, general computer controls, application control development and testing.
- Project management, JAD sessions, automation, business analysis, business and Information technology process reengineering.
- Reverse business cease and decease government orders by implementing compliance directives
- Create engagement economics to ensure profitability and margin schedule. Create, document and test both SOX business operational and information technology controls.
- Worked with client to create engagement add on business (sales), by bring in additional staff and identify new projects for the company to service. Applicable clients First American Financial – Credco, Provident BankCorp, Merchants National Bank

COLLEGIS– Maitland, FL June 2003 to October 2004
REGIONAL MANAGER

NORTH CAROLINA CENTRAL UNIVERSITY - Durham, NC April 2000 to June 2003
CHIEF INFORMATION OFFICER

FIDELITY INVESTMENTS - Covington, KY 1997 to April 2000
DIRECTOR, SYSTEMS MANAGEMENT (Fidelity Wide Processing Division)

ANTHEM- Cincinnati, OH November 1988 – December 1994
DIRECTOR, NETWORK OPERATIONS & DISTRIBUTED SYSTEM SUPPORT

LETTERS OF SUPPORT

NSF ATE Cybersecurity Resource Center

1. National Center for Systems Security and Information Assurance (CSSIA)

Industry

2. CISCO
3. CISCO Networking Academy
4. ReliaQuest

MORAINE VALLEY COMMU TY COLLEGE

August 20, 2018

Dear Laura Malave:

Our staff received your request for a support letter from an ATE Program Center official. This letter deems your organization eligible to apply for funding for the Improvement for Post-Secondary Education {FIPSE)-Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges.

After reviewing your proposal we would like to enthusiastically support the idea of expanding your AAS Degree in Cybersecurity into a BAS. This type of program provides a model pathway for cybersecurity students that graduate with an AAS Degree. There is a national need for an articulation infrastructure in cybersecurity for students pursuing a baccalaureate degree. We feel this model could be replicated across the country and that the BAS program will provide an articulation option for students at other schools graduating with an AAS Degree in Cyber securit y.

We have a working relationship with your staff as a result of mentoring your institution in the application process for the Center for Academic Excellence for Cyber Defense. We are confident that you have the technical expertise and grant management support to be successful in this proposed project. Your institution has an impressive outreach and serves a significant and diverse student population. Your program also aligns to many of the nationally recognized industry certifications. We feel this project is very worthy of funding.

Moraine Valley Community College and the faculty and staff from the Center for Systems Security and Information Assurance (CSSIA) will provide technical expertise in support of this project if you receive funding. This support would include faculty development, access to our virtual cybersecurity range and assistance in involving your students in national cybersecurity skills competitions.

Feel free to contact Dr. John Sands if you need further information.

Sincerely,
John Sands, Ph.D.

CSSIA Pl
Moraine Valley Community College
708-974-5426

August 22, 2018

Pearson Owens, Senior Program Officer
U.S. Department of Education
Office of Postsecondary Education
550 12th Street, SW - Room 7041, Potomac Center Plaza
Washington, DC 20202-4260

Re: Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges

Dear Mr. Owens:

On behalf of Cisco Systems**,** I am pleased to support St. Petersburg College (SPC) and sign this letter of commitment for their application to the U.S. Department of Education's *Pilot Program for Cybersecurity Education Technological Upgrades* solicitation. Cybersecurity has become a prevailing issue on a national and global scale, and the need for trained cybersecurity professionals with middle and high-level skills grows exponentially each year. SPC's plan to expand its cybersecurity curriculum and training offerings is a direct and welcomed response to cyber personnel needs.

Founded in 1984, Cisco remains an industry leader in IT security solutions. As cyber-attacks grow in complexity, Cisco is dedicated to providing comprehensive advanced-threat protection against today's cybersecurity threats. Employing over 70,000 people in 380 locations worldwide, Cisco remains on the forefront of cybersecurity solutions. Currently, Cisco employs IT security professionals with certifications such as Certified Cloud Security Professional, Certified Information Systems Security Professional, Cisco Certified Internetwork Expert, or other cybersecurity related certifications. Additionally, we anticipate the need to fill significantly more cybersecurity-related positions in the foreseeable future.

Cisco has worked closely with SPC's College of Computer and Information Technology, particularly in curriculum development and hands-on student training. SPC is the largest Cisco Academy in Florida, and was one of the first Cisco Academies to offer the Cisco CCNA in Cyber Operations curriculum, aligning with the CCNA Cyber Operations industry certification. SPC students were also able to explore digital futures at the national Cisco Live Conference in 2018, engaging with more than 1,800 leaders in IT. Cisco is excited to continue this partnership, and to also strengthen collaborations with partners such as the National Science Foundation's ATE Centers for cybersecurity and other institutions of higher education. Together, we can ensure that today's students are on the cutting edge of cybersecurity technological training to meet demand for tomorrow's workforce.

This letter of support demonstrates Cisco's involvement and support around the SPC project but does not constitute a specific financial or resource commitment. We look forward to hearing of your successful award in this important endeavor.

Sincerely,

Jody Gordon
Director of Strategy and Planning
Cisco US Public Sector

August 21, 2018

Pearson Owens
Senior Program Officer
U.S. Department of Education
Office of Postsecondary Education
550 12th Street, SW
Room 7041, Potomac Center Plaza
Washington, DC 20202-4260

Dear Mr. Owens:

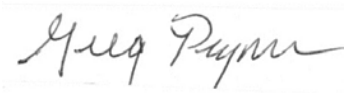
We are writing to demonstrate our support of St. Petersburg College (SPC) for their application to the U.S. Department of Education's Pilot Program for Cybersecurity Education Technological Upgrades solicitation. Cybersecurity has become a prevailing issue on a national and global scale, and the need for trained cybersecurity professionals with middle and high-level skills grows exponentially each year. SPC's plan to expand its cybersecurity curriculum and training offerings is a direct and welcome response to cyber personnel needs.

As a global leader in corporate citizenship, Cisco supports programs that improve access to education and promote economic empowerment in communities around the world. The Cisco Networking Academy program is the largest and longest running private-public partnership Corporate Social Responsibility program at Cisco. The Cisco Networking Academy is a comprehensive set of learning programs that enables students to develop valuable information and communication technology skills and, in turn, enables increased access to opportunities in the global economy.

The Cisco Networking Academy program has more than one million active students and is present in more than 170 countries around the world. In the United States, there are over 3,000 instructors and nearly 120,000 students in more than 1,700 academies located in high schools, colleges and universities. We continue to look for ways to ensure that a diverse student population understands the opportunity for career pathways in Science, Technology, Engineering and Math.

Please note that nothing in this letter constitutes a financial or resource commitment on behalf of Cisco.

Sincerely,



Greg Prynn
Senior Director
Corporate Affairs
Cisco

RE L I AQUES T

August 28, 2018

Pearson Owens
Senior Program Officer
U.S. Department of Education
Office of Postsecondary Education
550 12th Street, SW
Room 7041, Potomac Center Plaza
Washin gton, DC 20202-4260

Reference: Pilot Program for Cybersecurity Education Technological Upgrades for Community Colleges

Dear Mr. Owens:

On behalf **of ReliaQuest,** I am pleased to support St. Petersburg College (SPC) and sign this letter of commitment for their application to the U.S. Department of Education' s *Pilot Program for Cybersecurity Education Technological Upgrades* solicitation . We strongly believe this proposal will deliver cutting edge curriculum and training for current and future employees in cybersecurity.

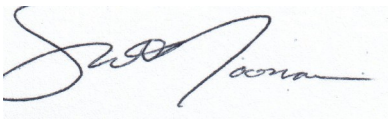
As a pioneer in IT security solutions, ReliaQuest empowers IT professionals and businesses with the latest relevant security technology innovations and services to streamline the complex interactions between securit y, risk and compliance. With two locations in the United States, and a third in Dublin Ireland, including our corporate headquarters in Tampa, Florida, ReliaQuest has grown considerably since its late 2007 launch.

We rely on our talented staff to deliver optimal results through documented best practices in IT security and service deli very, unifying people, process and technology. Workers with middle and high-level skills and industry certifications are in high demand for the Cybersecurity field, and we anticipate needing to fill as many as 250 jobs over the next year (2019) alone in cybersecurity-related occupations.

ReliaQuest has employed multiple SPC interns in IT-related fields. As a partner of the Cybersecurity Education Technological Upgrades program, ReliaQuest will commit to assisting SPC to ensuring alignment with current industry standards and certifications for the B.A.S. in Cybersecurity degree. We will also consider hiring eligible graduates for internships, full-time employment opportunities or other appropriate work experiences during and after the grant period.

Thank you for considering this application for the Pilot in Cybersecurity Education Technological Upgrades grants program. ReliaQuest is committed to hiring only the most talented and skilled employees, and, therefore, we are supportive of innovative training and skill development programs that meet the ongoing need for cybersecurity professionals.

Sincerely,



Scott Noonan

Vice President of Development

Appendix B

Notification of Grant Award

From: pearson.owens@ed.gov <pearson.owens@ed.gov>
Sent: Friday, September 28, 2018 5:50:50 PM
To: John Duff; Tonjua Williams; pearson.owens@ed.gov
Cc: pearson.owens@ed.gov
Subject: G5 Notification - New Grant Award Notification P116R180012

Dear Grantee:

The U.S. Department of Education (ED) is pleased to notify you that your grant has been selected for funding. You may access your electronically signed Grant Award Notification (GAN) documents for this new award, P116R180012 & GAN action number 1, at https://na01.safelinks.protection.outlook.com/?url=http%3A%2F%2Fwww.g5.gov&data=02%7C01%7CDuff.John%40SPCollege.edu%7Ceff861040dbb4f57761b08d6258c792c%7C575038c8ac704295810e0df79c005f41%7C0%7C0%7C636737682601719274&sdata=uTXlHh5Rcxk6T2cmrX6kT9RHhjA0xg9fiFow3rbqVmQ%3D&reserved=0 under Grant Maintenance, Award Documents.

You will need to sign in to G5 to access your GAN. If you don't already have an account in G5, please go to the link on the top left of the home page that says "Not Registered? Sign up" and follow the instructions. To register, you will need your institution's DUNS number. You must also use the exact same name (no nicknames) and email address that is listed on this email. If you are a project director, or state director, select "Project Director" or "State Director" when prompted to choose a role in your profile. Please note: Only recipients of this email (the project director and certifying official or state director and authorizing official) can access the GAN in G5. If someone else at your organization requires a copy, you may print out a copy or forward the PDF to them.

Please review your GAN documents carefully, including any attachments to the GAN and any terms and conditions appearing in Box 10 of the GAN. Your grant may be subject to special conditions or your grant or organization may have been designated as high-risk. You should review your GAN carefully to see if any of the following circumstances apply:

-If your grant is subject to special conditions, the special conditions may be included in Box 10 or as an attachment to the GAN.

-If your grant has been designated high-risk, the special conditions may be included in Box 10, or may be included in the high-risk designation that is attached to the GAN.

-If your entity has been designated a high-risk grantee, the high-risk special conditions are also applicable to this grant and may be included in Box 10 of the GAN, or may be included in the high-risk designation that is attached to the GAN.

Your grant is subject to any special conditions and/or high-risk designation that are attached to your GAN and must be carried out in accordance with those requirements. Your understanding of the GAN documents helps to ensure proper program and fiscal management of your grant.

If you have questions regarding accessing G5 or your GAN documents, please contact the G5 help desk at 888-336-8930. Questions regarding the next steps for your grant implementation should be directed to the ED Program Contact listed on your GAN (Box 3).

Please acknowledge receipt of this e-mail by sending a reply to the Education Program Contact listed on your GAN (Box 3). We wish you success on your grant.

Appendix C

Real Time Record of Industry DACUM Session

St. Petersburg College
Business Leaders Convening to help SPC Build a Bachelor's Degree in Cybersecurity

January 29, 2019
Real-time Record

CollaborativeLabs
St. Petersburg College
Facilitated Solutions. Immediate Results

Executive Summary

Thank you for participating in the **Business Leaders' Convening to help SPC Cybersecurity build a Bachelor's Degree in Cybersecurity** engagement held on January 29, 2019. Below are highlights of your discussion. The subsequent pages of this Real-time Record provide the supporting details.

The first brainstorming activity centered focused on identifying the possible Career Pathways and/or Specializations for a Cybersecurity graduate. The following lists the top three as determined through polling from the group:

Top Three Career Pathways/Specializations for a Cybersecurity Graduate

- **Cybersecurity Architecture/Information Security Architecture**/Understands SDLC, how to build security systems, programming and secure development practices (gap), Database Security
- **Management Orientation:** budgeting, project management, presentation skills, risk management
- **Specialization ideas:** pentest/hacking, auditing/compliance, software security, cloud security, IR/forensics

The same list was then re-prioritized to identify if any of the areas should be included in the core curriculum of the Cybersecurity Bachelor's degree, prior to branching out into the sub-plans. The following lists the top three as determined through polling:

Top Three Core Knowledge for a Cybersecurity Graduate

- **Core Courses**=network security, routing, hardening win and Linux OS, core management (compliance/legal/auditing), software
- **Cybersecurity Architecture/Information Security Architect:** understands SDLC, how to build security systems, programming and secure development practices (gap), Database Security
- **Management Orientation:** budgeting, project management, presentation skills, risk management

Next, the group heard about the NICE (National Institute of Cybersecurity Education) framework and brainstormed the Work Roles that could be filled by SPC Cybersecurity graduates.

Top Three Work Roles Could Be Filled by SPC Cybersecurity Graduates

- Systems Security Analyst/Cybersecurity Analyst/Cyber Defense Analyst
- Control Assessor/Security Control Assessor
- Vulnerability Assess Analyst/Threat Analyst

Table of Contents

Welcome & Overview 120
Building the Ideal SPC Cybersecurity Bachelor's Degree Program 128
Building the Ideal SPC Cybersecurity Bachelor's Degree Program – Team Reports130
Top 3 Career Pathways/Specializations for a Cybersecurity Graduate..... 134
Top 3 Core Curriculum Knowledge for a Cybersecurity Graduate..... 136
Overview of the NICE (National Institute of Cybersecurity Education) Framework137
Top Three Work Roles Could be Filled By SPC Cybersecurity Graduates – Team Reports 140
Discussion Wrap-Up & Next Steps 143
Attendees – Sign-in Sheets 145

St. Petersburg College

Business Leaders Convening to help SPC Build a Bachelor's Degree in Cybersecurity!

Purpose: To create a four-year BAS degree in Cybersecurity that fills the needs of local organizations by generating ready-for-workforce graduates with needed skillsets.

9:00am – 9:30am	**Welcome & Overview** Welcome: **Dr. James Stewart**, Dean, College of Computer & Information Technology Introductions: **Tina Fischer**, Collaborative Labs at SPC Overview of the Vision for SPC's Cybersecurity program: **Dr. John Duff**, Baccalaureate Academic Chair, College of Computer & Information Technology **Laura Malave**, Academic Chair, College of Computer & Information Technology Collaborative Labs' Team will share the Objectives and Collaborative Process.
9:30am – 11:15am	**Building the Ideal SPC Cybersecurity Bachelor's Degree Program** We will envision how we can build the **Ideal Cybersecurity Bachelor Degree Program** to address our local Cybersecurity workforce needs. **Round 1:** In teams, we will brainstorm: • What would the **Ideal Cybersecurity Bachelor's degree graduate** look like **(Skills, Knowledge, Industry Certifications)?** Participants will report out on their brainstorming and **prioritize the Top Skills** needed for a Cybersecurity graduate. **Overview of the NICE (National Institute of Cybersecurity Education) Framework** **Round 2:** In new teams, we will brainstorm: • Which of these **Work Roles from the NICE Framework could be filled by SPC Cybersecurity graduates** at your organization? Participants will report out on their brainstorming and **prioritize the Top Work Roles** needed for a Cybersecurity graduate.
11:15am– 11:30am	**Discussion Wrap-Up & Next Steps**

Welcome & Overview

Welcome & Introductions: **Tina Fischer**, Collaborative Labs at SPC
Overview of the Vision for SPC's Cybersecurity program:
Dr. John Duff, Baccalaureate Academic Chair, College of Computer & Information Technology
Laura Malave, Academic Chair, College of Computer & Information Technology

Collaborative Labs' Team will share the Objectives and Collaborative Process.

Tina Fischer, Manager, Collaborative Labs, St. Petersburg College (SPC): Good morning. We are so thankful to have you here today. We would like to hear from you what you are looking for in a skilled workforce. Things like social engineering? Digital forensics? Stopping hacks before they happen? This will help St. Petersburg College create a curriculum to provide graduates who are prepared to assimilate into your culture. We would like to learn who is in the room.

Bill Dalzell, Honeywell: I am the manager of System Security (cybersecurity and IT protection). We do hardware defense, and I represent seven sites from Florida to California.

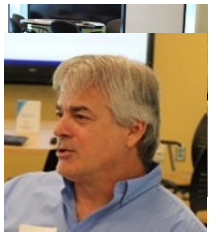
David Bryant, PSCU: I am VP of Information Security and Compliance. We do backend processing for credit unions.

John Sands, CSSIA: I help schools build these types of programs. I am a professor and Department Chair at Moraine Valley Community College.

Jeff Youmans, Citigroup: I am VP of the Western Hemisphere Utility and IS Security. My team looks at structure, breaks it down, and makes it into what it should be.

Andy Swenson, DelBridgeGroup: I am a Fractional CIO, Fractional CISO.

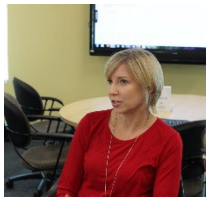
Brian Campbell, City of St. Petersburg: I am Chief Information Security Officer.



Roger Grimes, KnowBe4: I have been in computer security since ’87 and am a published writer on the topic of data analytics, risk management, and how companies are attacked the most. My company does security awareness training.

Dawn Ellis, SPC-CCIT: I am Academic Chair and oversee computer programming and analysis.

Angela Ashe, SPC: I am Academic Services Coordinator, ensuring we can implement and maintain curriculum.



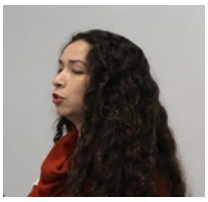
Tina Kuhn, SPC: I am a research analyst.

Susan Biszewski-Eber, SPC: I am the coordinator of the apprentice grant through The Department of Labor

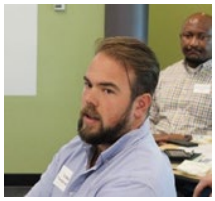
and I am on the National Institute of Cybersecurity Education (NICE) taskforce for apprenticeships.

John Long, SPC-CCIT: I am responsible for the computer networking degree and the general computer information technology degree.

Ryan Irving, Hillsborough County Board of County Commissioners: I am Division Director and an adjunct instructor at SPC.

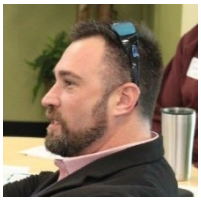


Laura Malave, SPC-CCIT: I am Academic Chair and lead for the associate's and certificate in Cybersecurity.



Ty Bond, JP Morgan & Chase: I am on the cyber education and awareness team.

Djuan Fox, SPC: I am Director of Academic Services, and I am here to listen and find out how to support you.

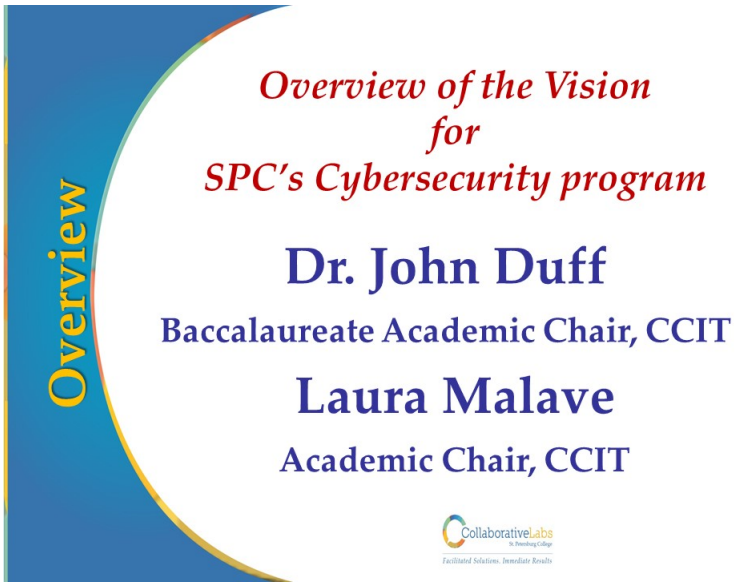


James Quilty, SofiaITC: I am CEO of SofiaITC and also contract with SOCOM. I am coordinating efforts with high school programs to get them engaged now with cybersecurity and certifications.

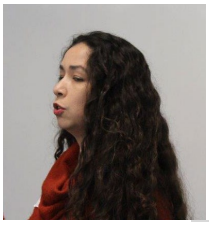
Kevin Thomas, SPC: I am lead instructor for the digital forensics program.

Derrick Thomas, Amgen: I am a Senior Security Engineer and I am a Tampa native who remembers when we were a call center hub.

Tina: Thanks for those great introductions. James's work with high schools drives home the importance of apprenticeships and internships. Now I would like to welcome Dr. John Duff and Laura Malave who will provide you with some information about current cybersecurity programs and SPC's vision for the future.



Dr. John Duff, Baccalaureate Academic Chair, College of Computer & Information Technology: We have a lot of expertise in the room. We got a grant from The Department of Education that will help expand SPC's cybersecurity offerings since there is demand in the marketplace for standalone cybersecurity programs. We have ideas, but you should be driving this effort. And today is just the beginning.



Laura Malave, Academic Chair, College of Computer & Information Technology: Our current cybersecurity offerings include Associate in Science in Cybersecurity (ITSC-AS) and Bachelor of Applied Science in Technology Development and Management (TMGT-BAS) with Cybersecurity Subplan (ISA). These handouts [next page] give you an idea of what students will be equipped with when they come into the Cybersecurity BAS degree program.

Associate in Science

Cybersecurity (ITSC-AS)

Graduates of this two-year program meet the growing need for college-educated specialists who can tackle increasingly complex networking information technology security concerns. As part of the A.S. degree, you complete an internship, providing invaluable experience for your career.

CCIT - COLLEGE OF COMPUTER AND INFORMATION TECHNOLOGY

Career Opportunities

Our program prepares you for entry-level positions such as:

- Information Security Analyst
- Information Management Specialist
- Network Security Administrator

Highlights

Our program helps you:

- Prepare for the IT Certification Exams: CompTIA A+ and Security+, CISCO CCENT, and EC Council Ethical Hacker
- Develop an organizational network and security program using risk management strategies
- Develop a strategy to address the increase growth of informational technology security concerns from regional to international environments
- Evaluate security techniques that assist in the prevention of hackers and cyber-attacks
- Transfer to SPC's Bachelor's Degree in Technology

Career Outlook

Demand for information security analysts is expected to be very high as employment is projected to grow 22 percent from 2010 to 2020.
Source: U.S. Bureau of Labor Statistics

Skills

What you will learn:

- Security policies
- Intrusion detection systems
- Router security and protocols
- Transmission Control Protocol/Internet Protocol
- Network security basics
- Firewall implementation and management
- Auditing tools
- Basic cryptography, biometrics and file encryption
- Hardware and software designed to secure information network systems
- Legal aspects of IT security
- Funcamentals of Linux/Unix operating system

Learn more

www.spcollege.edu/ccit | 727-341-4641

YOUR PATHWAY TO SUCCESS

Follow this checklist to set and achieve clear career goals

CYBERSECURITY

COURSE PLAN
1 TO 15 CREDITS

1	COS 1309	COMPUTER AND INFORMATION TECHNOLOGY CONCEPTS
2	ENC 1131	COMPOSITION I
3	SPC 1060	BUSINESS AND PROFESSIONAL SPEAKING
4	MAT 1033	INTERMEDIATE ALGEBRA
5	CET 1770	COMPUTER REPAIR ESSENTIALS

MILESTONES

- Visit Career Services & complete Focus 2 assessments
- Research careers using BLS & ONET
- Explore degree options & requirements
- Visit Advising, declare a major, & create a MLP
- Familiarize yourself with MySPC, MyCourses, & SPC email
- Volunteer & join Student Government or a club
- Start a basic resume

16 TO 30 CREDITS

6	MAC 1105	COLLEGE ALGEBRA
7	CET 1725C	COMPUTER SUPPORT TECHNICIAN
8	CET 1600	INTRODUCTION TO NITWORKS
9	CET 1610	ROUTING PROTOCOLS & CONCEPTS
10	PHI 1600	STUDIES IN APPLIED ETHICS
11	CJE 1883	FORENSIC COMPUTER RELATED CRIME INVESTIGATIONS

- Confirm a degree plan that matches your career goals
- Update My Learning Plan (MLP), if necessary
- Explore degree options & requirements
- Add Volunteer activities & clubs to your resume
- A.S. Program: Attend events related to program & prepare for industry certifications & exams
- Visit Career Services to discuss work-based learning opportunities
- Tune-up your interviewing skills

31 TO 45 CREDITS

12	CTS 2105	FUNDAMENTALS OF THE LINUX/UNIX OPERATING ENVIRONMENT
13	POS 2041	AMERICAN NATIONAL GOVERNMENT
14	CTS 1123	NETWORK SECURITY FOUNDATIONS
15	HUM 2270	HUMANITIES (EAST-WEST SYNTHESIS)
16	CGS 2811	INCIDENT RESPONSE & DISASTER RECOVER
17	CET 2691	LAWS & LEGAL ASPECTS OF IT SECURITY

- Build relationships and practice interviewing
- Create LinkedIn profile & clean up your online presence
- Complete all required courses for credit internship
- Make plans for continuing at SPC in TMGT-BAS
- Complete degree audit with an advisor
- Update MY Learning Plan and resume
- Attend events related to specific program
- Prepare for industry certification and exams

46 TO 60 CREDITS

18	CIS 1368	OPERATING SYSTEM SECURITY
19	CTS 1314	NETWORK DEFENSE AND COUNTERMEASURES
20	CIS 2362	ETHICAL HACKING
21	CTS 2943	CYBERSECURITY INTERNSHIP

- Research jobs and companies
- Get references or letters of recommendation
- Finalize plans for continuing at SPC in TMGT-BAS
- Gain experience in your field by doing an internship
- Update your resume again to include keywords
- Continue to develop relationships and go to targeted events
- Complete a graduation check with adviser
- Apply for GRADUATION and order your cap

Total Program Credits 60
Total Pathway Credits 63

SPC St. Petersburg College — Graduation

Bachelor of Applied Science

Technology Development and Management (TMGT-BAS) Cybersecurity Subplan (ISA)

Our Technology Development and Management bachelor's degree gives you a solid credential in the evolving field of technology management. You will receive a balance of technology and management education to make you a front-runner in today's competitive environment. Technology development and management professionals are skilled at increasing businesses efficiency through technology solutions.

CCIT - COLLEGE OF COMPUTER AND INFORMATION TECHNOLOGY

Career outlook

Employment of computer and information systems managers is projected to grow 18 percent through 2020 as organizations switch to newer, faster and more mobile networks requiring managers to help with the transition.

Source U.S. Bureau of Labor Statistics

Career opportunities

Our programs prepare you for the following careers:

- Computer and Information Systems Managers
- Computer Programmers
- Computer Systems Analysts
- Information Security Analysts, Web Developers and Computer Network Architects
- Business and Web Data Analysts

Skills

What you will learn:

- Effectively lead and manage small to medium-sized project teams
- Execute, evaluate and manage projects
- Develop and implement innovative technology solutions to enhance the profitability of an organization
- Manage technology, security, information assurance and/or at-risk areas in an organization
- Create optimal value of information and technology through the use of data analytics
- Protect the information and technology resources and provide leadership to the organization to ensure security and reduce risks
- Understanding the role programming languages play in software development

Highlights

Our program offers:

- An accelerated learning environment with eight week online courses
- The most current technology and learning tools
- Caring faculty members with outstanding credentials and industry certification experience
- Collaborating with local industry leaders on projects through a capstone experience
- Active Advisory Committee members who ensure the program matches current industry needs and emerging topics

Learn more

www.spcollege.edu/ccit | 727-341-4641

YOUR PATHWAY TO SUCCESS

Follow this checklist to set and achieve clear career goals

CYBERSECURITY SUB PLAN

COURSE PLAN
0 TO 12 CREDITS

1	ENC 1102	COMPOSITION II
2	GEB 3213	BUS COMM FOR PROF EFFECTIVENESS
3	ISM 3011	MGMT OF INFORMATION SYSTEMS
4	MAN 3302	MGMT & LEADERSHIP PRACTICES

MILESTONES

- Complete My Learning Plan (MLP) for TMGT-BAS
- Visit Career Services & complete Focus 2 assessments
- Research careers using BLS & ONET
- Explore degree options & requirements
- Update resume
- Update LinkedIn profile & clean up your online presence

13 TO 24 CREDITS

5	STA 2023	ELEMENTARY STATISTICS
6	ISM 3252	APPLIED SYSTEMS ANALYSIS
7	ISM 4361	IT SERVICES MANAGEMENT
8	ISM 4113	SOFTWARE DESIGN METHODOLOGIES

- Confirm a sub plan that matches your career goals
- Update My Learning Plan (MLP), if necessary
- Attend events related to program
- Visit Career Services to discuss work-based learning opportunities
- Attend events related to specific program

25 TO 30 CREDITS

9	PHI 1010	INTRODUCTION TO PHILOSOPHY
10	OCE 2001	INTRODUCTION TO OCEANOGRAPHY

31 TO 42 CREDITS

11	ISM 4213	DATABASE DESIGN AND ADMINISTRATION
12	BUL 3981	LEGAL ASPECTS OF MAN. TECHNOLOGY
13	ISM 4323	SECURITY ESSENTIALS
14	ISM 4330	INFO SEC POLICY ADMIN & MANAGEMENT

- Build relationships and practice interviewing
- Complete all major core courses in order to register for Senior Capstone Project
- Complete degree audit with CCIT BAS advisor
- Update MY Learning Plan and resume

43 TO 54 CREDITS

15	ISM 3503	RISK ANALYSIS & DECISION MAKING
16	ISM 4915	SPN CR CAPSTONE PROJECT
17	ISM 4320	CORE SECURITY PRINCIPALS
18	ISM 4391	STRATEGIC CYBER SECURITY ENFORCEMENT

55 TO 60 CREDITS

19	BSC 1005C	BIOLOGICAL SCIENCE WITH LAB
20	ISM 4324	APPLICATIONS IN INFORMATION SECURITY

- Research jobs and companies
- Get references or letters of recommendation
- Update your resume again to include keywords
- Continue to develop relationships and go to targeted events
- Complete a graduation check with CCIT BAS advisor
- Apply for GRADUATION and order your cap

Total Program Credits 60
Total Pathway Credits 60

SPC St. Petersburg College — Graduation

Tina: Let me introduce our team. I will be facilitating the discussions. Michael is our technology guru, and he will guide us through some cool technology today. Dina is documenting the discussion that will form the Real-time Record we mentioned earlier that you will receive, so there is no need to take notes.

Before we start with the first round of brainstorming, are there any questions?

Roger Grimes: What is the difference between the handouts and the ideal cybersecurity graduate?

The group engaged in discussion about Roger's question that included: *In the program now, there are only 5 courses in the bachelor's degree related to cybersecurity. Currently, there are four subplans: Cybersecurity, Project Management, Software Development, and Data Analytics, now Data Science. There is enough content and variety in Cybersecurity that we can focus an entire bachelor's degree, BAS, on that. It is not an ES or BA degree.*

Andy Swenson: We talked about a lot of disciplines of cybersecurity and there are very deep disciplines. Does it make sense to have a cybersecurity with specialization? Can we delve into that?

John Long: That is what we are thinking: a core set of courses then majors/subplans/specializations.

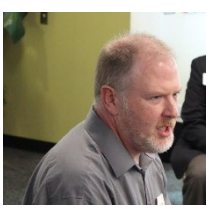
Andy Swenson: That would help a lot with employability.

John Duff: Depth is a key term.

Ryan Irving: I graduated in 2010 from the program. It was primarily a lot of management, ethics, and project management courses essentially for business acumen, but I wished I had more hands-on technical ability. Other specializations are really key here.

Andy Swenson: And it provides a dual career path, which is rewarding both financially and personally.

John Duff: Laura's program students are required to have an internship.

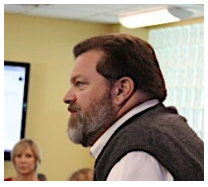


David Bryant: We talked about specializations. In hiring, sometimes we get people who are too specialized. Especially in information security. We do not have large amounts of staff, so we want people who are not so specialized. The core layer at the top is the most important piece.

Bill Dalzell: We will get stacks of resumes of people myopically trained. We make money with cyber. I am not compliance. With my company, they will not sit in front of a bunch of monitors.

Jeff Youmans: I have watched this progress from DC to SOCOM to the public sector, and information security is catchall, then technical security, then information assurance. There are different skillsets and personalities. Some can talk, some can code. None of us said we wanted to be security guys in the '90s. Kids today say they are.

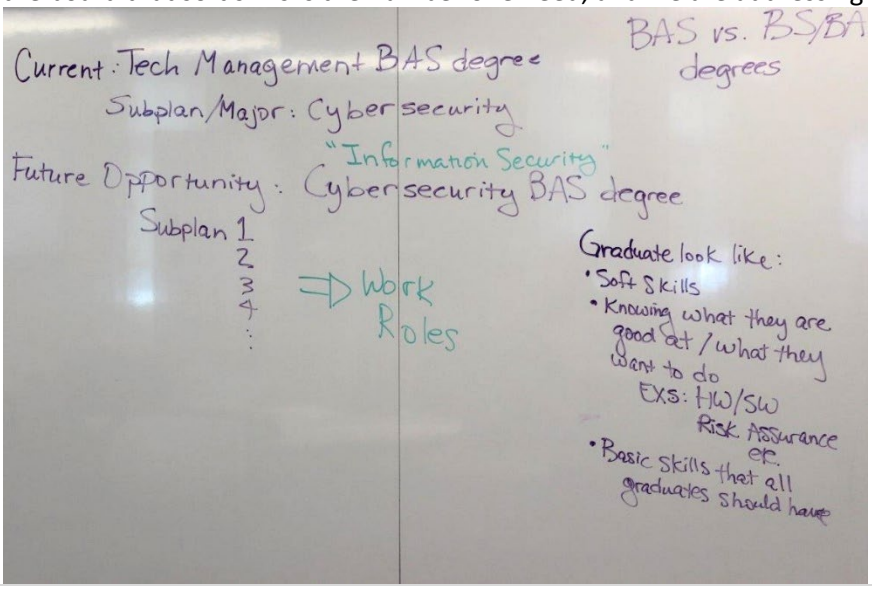
John Duff: That is all the kind of input we need and why you are here.



Brian Campbell: I do not disagree with you, but typical shops are small. Or we outsource to you, the big problem-solvers. I need regular staff to be skilled, intelligent, excellent problem-solvers, and analytical, but it has to be wide. I interview people and tell them it is a very boring job. We are not doing forensics. Then one day, now I need you to do forensics. Specific skills in a siloed technical area of expertise does not buy me anything. I will hire out for that. The majority of employers in the Tampa Bay area have small teams of one to three people and hire out accordingly.

I want a wide breadth of concepts to augment the skills I do not have. What are the biggest holes in the marketplace? I do not think they are technical silos. But having some of all of it, not generalists but understanding and communicating with technical experts and management or the press. When Atlanta got hacked, who stood in front of the press? Not the mayor. Not the CIO. It was the CISO who was on the job for a very short time. So those skills are important.

Tina: From your conversation, I captured these high-level concepts: you are looking for graduates to know what they are good at and what they want to do, and for them to have basic skills that all graduates should have plus soft skills. We have been hearing from groups across the board that soft skills is the number one need, and we are addressing that.



Jeff Youmans: I hate the term Cybersecurity. It is Information Security.

Brian Campbell: If you say Information Security, I will not hire you. Words have value.

Bill Dalzell: Has anyone hired someone with a cybersecurity degree? I have hired a lot of people. I just hired my first cybersecurity person last year. Am I alone?

Andy Swenson: This is a new discipline. As a long time CIO, I hired my first cybersecurity person one and a half years ago and more on the GRC side for compliance things. The cybersecurity degree has not been around long, so you will not have hired a lot with that degree. University of Tampa has a cybersecurity track and a bachelor's degree too. The first one came from Norwich University.

Ryan Irving: That term is an industry seller. It was called information assurance, information security years ago. Then cybersecurity stuck. Cybersecurity is what people who make decisions understand. If I need budget, that is the word I am using.

John Long: Cybersecurity is sexy and cool, cyber threat too. It is a millennial term. And it is booming.

Tina: Let's keep this discussion going in teams and have conversations in small groups. The subplan discussion is our second question. We want to raise it up and free flow ideas about what the graduate looks like in general. What basic skills all graduates should have in core classes?

Ty Bond: I propose that we switch the order of the questions. Skills related to the roles will dictate, and tiers within the subplans. Let's not limit ourselves.

John Duff: We can do that.

The order of questions was revised. The second question was changed to add "Specializations."

Building the Ideal SPC Cybersecurity Bachelor's Degree Program

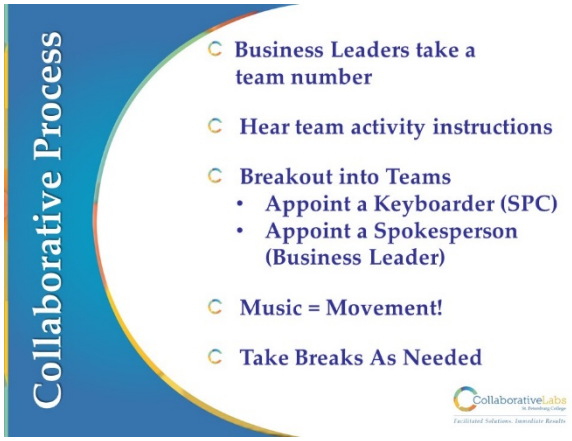
We will envision how we can build the **Ideal Cybersecurity Bachelor Degree Program** to address our local Cybersecurity workforce needs.

Round 1: In teams, we will brainstorm:

- Which of these **Career Pathway/Specializations** could be filled by SPC Cybersecurity graduates at your organization?

Participants will report out on their brainstorming and **prioritize the Top Career Pathway/Specializations** needed for a Cybersecurity graduate.

Tina: Great idea. We will do that. There will be three teams. I will be passing out a bucket of numbers. When you get to your team areas, select someone to be your keyboarder and select a spokesperson to share your team's work with all of us. Each team will come up with a list of ideas in ThinkTank, then pick their top three. Afterwards, we will do report outs from each team and use polling to get to the top three over all. Music is your cue to move. There are not any scheduled breaks, so take them as you need to. Help yourself to the refreshments too.


Collaborative Process
Business Leaders take a team number
Hear team activity instructions
Breakout into Teams
Appoint a Keyboarder (SPC)
Appoint a Spokesperson (Business Leader)
Music = Movement!
Take Breaks As Needed
CollaborativeLabs


Collaborative Labs
at St. Petersburg College
Deploy To Teams!
CollaborativeLabs

Building the Ideal SPC Cybersecurity Bachelor's Degree Program – Team Reports

TOP CAREER PATHWAYS/SPECIALIZATIONS

These are the top ideas selected by each team.

1. Risk management/mitigation
2. Management Orientation: budgeting, project management, presentation skills, risk management
3. Specialization ideas: pentest/hacking, auditing/compliance, software security, cloud security, IR/forensics
4. Data analytics
5. Core courses=network sec, routing, hardening win and Linux OS, core management (compliance/legal/auditing), software
6. Cyber Security Architecture/Info Security Architect: understands SDLC, how to build security systems, programming and secure development practices (gap), Database Security
7. Digital Defense: Red/Blue Team (pen testing, etc.), emphasis on both roles, forensics - technical/legal, cloud security
8. Requirements Analysis
9. How to speak cybersecurity, how to SPIN an incident, communications, translate between tech and regular people, CI Security, internal marketing/PR, how to communicate with board level people

CAREER PATHWAYS/SPECIALIZATIONS

These are the remaining ideas brainstormed by each team.

1. Developer/Help Desk/Network as entry points
2. DevOps/SecOps
3. Blockchain
4. AI, IoT, RPA, Machine Learning,
5. Governance and Compliance (GRC) - cloud environment, control frameworks
6. Data records management
7. Log analysis
8. Product Support
9. Cloud computing
10. Be able to articulate verbally
11. Technical writing capability
12. Core component=security person needs to understand hardware and software
13. Students need core tech skills, Linux, kali apps, Windows, Mac, mobile Ios and Android
14. Invulnerable to social engineering
15. Windows more important than Linux? Perhaps desktop not on server side
16. Exposure to IS automation
17. Framework implementation
18. Linux command line skills, how to maneuver through it SSH command line skills
19. Windows desktop and server admin skills also important
20. Separate courses for windows desktop, windows server, mobile devices
21. Technical Audit principles
22. IPv6 need in future
23. Cryptography knowledge
24. Ip v 6 part of network courses, not separate class dedicated to it

25. Bring skills no one else has, fill skill holes=auditing, vuln mgmt., basic Incident Response skills, CISSP management skills, how read packet capture
26. Tech networking, software development technical skills=understand code, troubleshoot code already written
27. Read event logs, troubleshooting incident
28. Network class, software class, database class, voip
29. Policy, procedure, GRC also with tech skills
30. Email security/troubleshooting/IR, reading email headers
31. Workflow for IR, recognize alerts, need to escalate incident for help desk type position
32. Alert response in core courses, how collect logs/auditing skills, set up syslog, how read a log in IR context
33. Start a company, build IT from scratch, harden it and use hands on activity to pentest it
34. Solid understanding of compliance HIPAA/GDPR, PCI, legal issues, NIST/RMF how apply standards, SOX, NY DFS
35. Process management

Team 1


Andy Swenson: Our three areas were:

- Core Courses
- Specialization (ability to manage an audit; there are a lot of differences in cloud management, especially in shared services environments; and when the inevitable happens, can they respond appropriately with the right partnerships)
- How to speak cybersecurity (people need to understand the ramifications of the decisions they make in response to incidents)

Team 2


Bill Dalzell: Our top three were:

- Risk Management/Mitigation (a lot is interpretation of rules and regulations; minimum best practices; you do not want a $100,000 lock on a $1,000 piece of data)
- Data Analytics (everyone has their own data path to go down; you have to quantify the data for customers to understand, and bosses to understand risk and how to solve, here are the holes you have, here are the ones we think we can patch, here are the ones we cannot)
- Requirements Analysis/System Engineering (security engineers get to do something cool and different; we flow shells out to other people: do not open emails with the words "are you" on the end, do not throw things into the recycle bin, some of us actually do dumpster diving; that is a requirements analysis)

Team 3


David Bryant: The ones we thought were most important were:

- Management Orientation (most will want to climb the ladder, they need to know how management works: I want new IPS, but how will you deploy that IPS? They need to understand how to run something beginning to end; they need presentation skills to get budget; they cannot talk technical terms to upper management; they need to know what risks they are working around, managing, tracking, and who's reporting on them)
- Cybersecurity Architecture/Information Security Architect (They need to understand the sum of the whole, not just component parts; how does SDLC factor into this? Programming DNA secure development practices is a real gap now; they need to know the different methods – Agile, Waterfall; how to talk apdev language to people; understand how to program and how to secure all three tiers of an architecture.
- Digital Defense/Red/blue team (We recommend that in the curriculum, red and blue teams are defenders and attackers and halfway through they flip; they need to understand how bad guys think to be able to stop them, so an emphasis on both roles is important; along with forensics, technical/legal, cloud security; with forensics, it is not just tools; many think it is what they see on TV but it is not, it is very procedural; they would better understand the chain of custody and how evidence was collected; they need to be able to sit in a courtroom and testify that they collected it forensically sound; the cloud will be a key security competency; on-prem security is different than cloud security; cloud security is moving more toward containerization of applications; they need to understand the security differences between public, private, and hybrid clouds)

Tina: Let's give a round of applause to the keyboarders and the team speakers. Next, get your clickers. You are going to vote on your top three, and then Michael will show us the combined results.

Top 3 Career Pathways/Specializations for a Cybersecurity Graduate

Top 3 Career Pathways/Specializations for a Cybersecurity Graduate

1. Risk management/mitigation – 10%
2. **Management Orientation: budgeting, project management, presentation skills, risk management – 16%**
3. **Specialization ideas: pentest/hacking, auditing/compliance, software security, cloud security, IR/forensics – 16%**
4. Data analytics – 3%
5. Core courses=network sec, routing, hardening win and Linux OS, core management (compliance/legal/auditing), software – 10%
6. **Cyber Security Architecture/Info Security Architect: understands SDLC, how to build security systems, programming and secure development practices (gap), Database Security – 26%**
7. Digital Defense: Red/Blue Team (pen testing, etc.), emphasis on both roles, forensics - technical/legal, cloud security – 12%
8. Requirements Analysis – 0%
9. How speak cyber security, how to SPIN an incident, communications, translate between tech and regular people, CI Security, internal marketing/PR, how to communicate with board level people – 6%

Top Three Career Pathways/Specializations for a Cybersecurity Graduate

- **Cybersecurity Architecture/Information Security Architecture/Understands SDLC, how to build security systems, programming and secure development practices (gap), Database Security – 26%**
- **Management Orientation: budgeting, project management, presentation skills, risk management – 16%**
- **Specialization ideas: pentest/hacking, auditing/compliance, software security, cloud security, IR/forensics – 16%**

John Duff: That was a lot of valuable discussion. You have already changed some of my thinking about where we should go. The second round is about NICE, who has published a comprehensive framework. Is anyone familiar with it?

A few participants raised their hands.

John Duff: We want to be recognized at our associate's degree level as a Center of Excellence, and Laura is putting

together a comprehensive application. We need to show we are filling the needs in the workplace. This framework has categories, then specialty areas, then work roles for each. For the BAS program, we want you to help us identify the work roles that need to be addressed.

John Sands: When I do these across country, I like to hear two things: 1. Which work roles would you like someone coming out of a bachelor's degree program to have, and 2. What do you think is realistic to teach within four years.

The group discussion about John's comment included: *On-the-job training, how much emphasis to put on a 4-year degree, public vs. private hiring, skillsets vs. degree.*

Tina: Please keep in mind that this is a graduate of a bachelor's degree program. Consider whether a bachelor's degree would fit in with the roles in your workplace. Sometimes it does take years of experience. And we have to consider how many credit hours are in the degree.

Angela Ashe: They will articulate into the BAS program from the AS. In theory, students would come out of the AS program going right to work, then come into the BAS program so they will have some content knowledge and work experience. The structure of the BAS is 45 credits: 28-30 are usually in core curriculum, 12-15 are built into the specialization areas. So it amounts to 4-6 classes.

Bill Dalzell: We have salary ranges. With a BA there is a range I can pay. My HR department will ask me what to do with a BAS. What are they coming out with?

Angela Ashe: A BAS – it is structured differently because we expect they are coming from the workforce with an AS degree.

John Duff: The right answer is you pay them more.

The group laughed.

Based on the information participants received, we recommended they revote using the top career pathways list to find out which ones fit in the core curriculum.

Tina: Some of the specializations you just came up with sound like they should be in the core curriculum, so we changed the title of the poll and kept the same concepts. Let's revote and see what top three core courses you think every cybersecurity graduate should graduate with from this list of nine.

Top 3 Core Curriculum Knowledge for a Cybersecurity Graduate

Top 3 Core Curriculum Knowledge for a Cybersecurity Graduate

1. Risk management/mitigation – 16%
2. **Management Orientation: budgeting, project management, presentation skills, risk management – 17%**
3. Specialization ideas: pentest/hacking, auditing/compliance, software security, cloud security, IR/forensics – 6%
4. Data analytics – 0%
5. **Core courses=network security, routing, hardening win and Linux OS, core management (compliance/legal/auditing), software – 24%**
6. **Cyber Security Architecture/Info Security Architect: understands SDLC, how to build security systems, programming and secure development practices (gap), Database Security – 24%**
7. Digital Defense: Red/Blue Team (pen testing, etc.) - emphasis on both roles, forensics - technical/legal, cloud security – 3%
8. Requirements Analysis – 3%
9. how speak cyber security, how to SPIN an incident, communications, translate between tech and regular people, CI Security, internal marketing/PR, how cmu with board level people – 6%

Top Three Core Curriculum Knowledge for a Cybersecurity Graduate

- **Core Courses=network security, routing, hardening win and Linux OS, core management (compliance/legal/auditing), software – 24%**
- **Cybersecurity Architecture/Information Security Architect: understands SDLC, how to build security systems, programming and secure development practices (gap), Database Security – 24%**
- **Management Orientation: budgeting, project management, presentation skills, risk management – 17%**

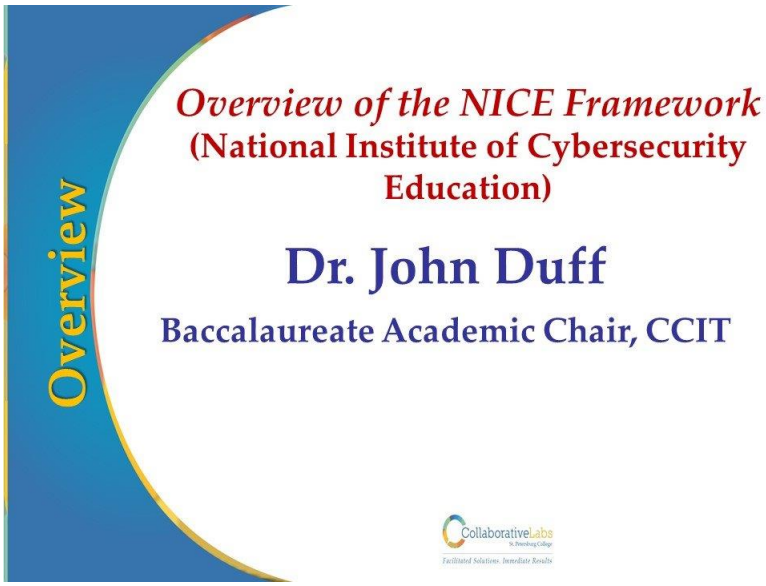
The group agreed that they saw a lot of overlap between 5 and 6, and between 1 and 2.

Overview of the NICE (National Institute of Cybersecurity Education) Framework

Round 3: In new teams, we will brainstorm:

- Which of these **Work Roles from the NICE Framework could be filled by SPC Cybersecurity graduates** at your organization?

Participants will report out on their brainstorming and **prioritize the Top Work Roles** needed for a Cybersecurity graduate.



John Duff: Let's get back to the NICE framework that we talked about before that second vote.

Tina: For the third question, which of these work roles from the NICE framework could be filled by SPC cybersecurity grads at your organization? Keep in mind we are talking about bachelor-level grads, not master's. If your organization has a role that does not appear in the chart, put that in. We are not trying to force you into this framework; just which jobs are you trying to fill, what skillsets you will need, and how can SPC provide that. Please take a new team number from the bucket while John gives you an overview of the NICE work roles. And when you get into your teams, you will again choose a keyboarder and a speaker who will share your ideas with the group.

John Duff: The actual NICE framework is a huge stack of papers, so I condensed them into what you have here. We want the list of the work roles that you think your organization will need the most when these graduates come to you.

NICE Category	Specialty Area	Work Role
Securely Provision	Risk Management	Authorizing Official Security Control Assessor
	Software Development	Software Developer Secure Software Assessor
	Systems Architecture	Enterprise Architect Security Architect
	Technology R&D	R&D Specialists
	Systems Requirements Planning	Systems Requirements Planner
	Test and Evaluation	Systems Testing & Eval Specialist
	Systems Development	IS Security Developer Systems Developer
Operate and Maintain	Data Administration	Database Administrator Data Analyst
	Knowledge Management	Knowledge Management
	Customer Service & Tech Support	Technical Support Specialist
	Network Services	Network Operations Specialist
	Systems Administration	System Administrator
	Systems Analysis	Systems Security Analyst
Oversee and Govern	Legal Advice & Advocacy	Cyber Legal Advisor Privacy Officer/Privacy Compliance
	Training, Education, & Awareness	Cyber Instructional Curriculum Specialist Cyber Instructor
	Cybersecurity Management	Information Systems Security Manager Communications Security Manager (COMSEC)
	Strategic Planning & Policy	Cyber Workforce Developer & Manager Cyber Policy & Strategic Partner
	Executive Cyber Leadership	Executive Cyber Leadership
	Program/Project Mgt & Acquisition	Program Manager IT Project Manager Product Support Manager IT Investment/Portfolio Manager IT Program Auditor
Protect & Defend	Cybersecurity Defense Analysis	Cyber Defense Analyst
	Cybersecurity Defense Infrastructure Support	Cyber Defense Infrastructure Support Spec.
	Incident Response	Cyber Defense Incident Responder
	Vulnerability Assessment & Management	Vulnerabilty Assessment Analyst

NICE Category	Specialty Area	Work Role
Analyze	Threat Analysis	Threat/Warning Analyst
	Exploitation Analysis	Exploitation Analyst
	All-Source Analysis	All-Source Analysist Mission Assessment Specialist
	Targets	Target Developer Target Network Analysts
	Language Analysis	Multi-Discipline Language Analyst
Collect & Operate	Collection Operations	All Source-Collection Manager All Source-Collection Requirements Manager
	Cyber Operational Planning	Cyber Intel Planner Cyber Ops Planner Partner Integration Planner
	Cyber Operations	Cyber Operator
Investigate	Cyber Investigation	Cyber Crime Investigator
	Digital Forensics	Law Enforcement/Counter Intell Forensics Analyst Cyber Defense Forensics Analyst

Brian Campbell: If I am hiring, what skills does a BAS degree graduate come out of school with? What does that mean to me as a hiring manager?

Tina: SPC fills a valuable need in our community. Our job is to put people to work. This next exercise will help answer how we will address your question with what NICE work roles will fit within your organizations. Each team will again come up with a list, then choose your top three from that list. Then we will regroup, do report outs and vote on the top three.

To Brian's point before you broke into teams: How do you know a graduate comes out with the skills you need? Angela gave me an example. This is the Cybersecurity AA degree. They get a set of standards from the state for each associate's degree. Students must meet these learning outcomes; that is assessed by the state. Some bachelor's degree programs have learning outcomes/standards, and some do not. John Sands sits on a board to help define those standards.

Top Three Work Roles Could be Filled By SPC Cybersecurity Graduates – Team Reports



TOP WORK ROLES

These are the top ideas selected by each team.

1. Systems security analyst
2. Control assessor
3. Cyber Defense Analyst
4. Vulnerability assess analyst
5. Security Control Assessor
6. Systems security analyst/cybersecurity analyst
7. Vulnerability assessment analyst
8. Security architect
9. Software/systems Development

WORK ROLES

These are the remaining ideas brainstormed by each team.

1. Cyber legal advisor
2. Systems test and eval specialist
3. IS security developer
4. Threat/warning analyst/cyber defense analyst - junior level
5. Information systems security officers
6. Junior developer
7. Cyber defense incident responders
8. System Security Analyst
9. Pen tester
10. Systems Development
11. Customer Service and Tech Support
12. Security control assessor
13. Cybersecurity Defense Infrastructure support
14. Cyber ops planner
15. Data analyst
16. Technical support specialist
17. Network ops specialist
18. IT Program Auditor
19. IT program auditor
20. Cyber operator

21. All source analyst
22. Threat and warning analyst
23. Cyber defense analyst
24. Cyber policy planner (jr)
25. Info sys sec developer
26. Secure software assessor

Team 1


Ty Bond: We chose System Security Analysts, Control Assessors, and Vulnerability Assessment Analyst. We agreed there were a lot of roles that would work, but going in as a junior member of the team.

Tina: I heard that in a lot of conversations.

Ty Bond: It goes along with the apprentice model which I am a huge fan of. Because many places are so specific to the tools, systems, software, and language they use, the hands-on experience at the company is key.

Tina: It used to be that on indeed.com, you would skip a listing that had criteria you did not possess, but now companies are taking that in-house with the apprenticeship model.

Team 2


Ryan Irving: Our team went with Cyberdefense Analyst (level 1 people doing alerting and initial triage), Security Control Assessor (which was Derrick's idea – they are new, coming into the auditing space, coordinating, and collecting evidence), and Software and Systems Development (with the hope that it is more of an engineering field since there was not an engineering term on there that would be beneficial; engineering/software/infrastructure with security as the mindset and goal). There is a lot of overlap between the teams, as you can see.

Team 3


Dan Brown: Similar to team 1, we went with Security Analyst, Vulnerability Assessment Analyst (with multiple tiers in the group that use these types of positions; OJT is key in that environment), and Security Architect (there seems to be a shortage; putting groups of systems together; a broad background out of school is good, maybe junior level architect).

The group combined some of the ideas generated.

Brian Campbell: Does anyone have a job title of Vulnerability Assessment Analyst?

Dan Brown: We did for three years and just changed it to Threat Analyst.

Roger Grimes: I still see a lot in Fortune 500 companies.

Tina: Now we will open the poll for you to choose your top three from this list of five.

Top 3 Work Roles Could Be Filled by SPC Cybersecurity Graduates

1. **Systems Security Analyst/Cybersecurity Analyst/Cyber Defense Analyst – 41%**
2. **Control Assessor/Security Control Assessor – 28%**
3. **Vulnerability Assess Analyst/Threat Analyst – 18%**
4. Security Architect – 3%
5. Software/Systems Development – 10%

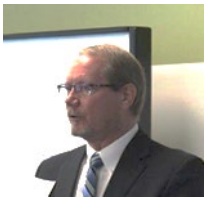
Top Three Work Roles Could Be Filled by SPC Cybersecurity Graduates
• **Systems Security Analyst/Cybersecurity Analyst/Cyber Defense Analyst – 41%**
• **Control Assessor/Security Control Assessor – 28%**
• **Vulnerability Assess Analyst/Threat Analyst – 18%**

Tina: Give yourselves a round of applause.

Discussion Wrap-Up & Next Steps

Tina: You have done a lot of important work today. Thank you. You will receive a Real-time Record within 48 hours that will contain some hi-res pictures and details of what we did here today.

If you have any questions about Collaborative Labs and what we can do for your organization, please come chat with me.



John Duff: Our job is to prepare students to work for folks like you. Your input drives this process. Thank you for helping us put things together today. This is a starting point for us. We will do a sanity check with you as we progress, including putting together an advisory team.

Tina: John, how long is the process to create a degree like this?

John Duff: We would like to move quickly, but it is difficult to predict the cycle time. We will develop a plan that will fit within the existing degree program. We send the proposal to the state, which begins a yearlong process. All other schools in the state review it. We think we are doing something unique. USF has a bachelor's degree in cybersecurity that is very engineering oriented and requires calculus. We believe there is a fit for what we are trying to do here. The state's processes are very rigorous, and we end up with a good product in the end. Through the spring, we will turn this into candidates for courses working with Dr. Sands and his team, then we will develop courses and our faculty who will need development and possibly certification. We think the subplan will be ready next spring and the degree program next fall.

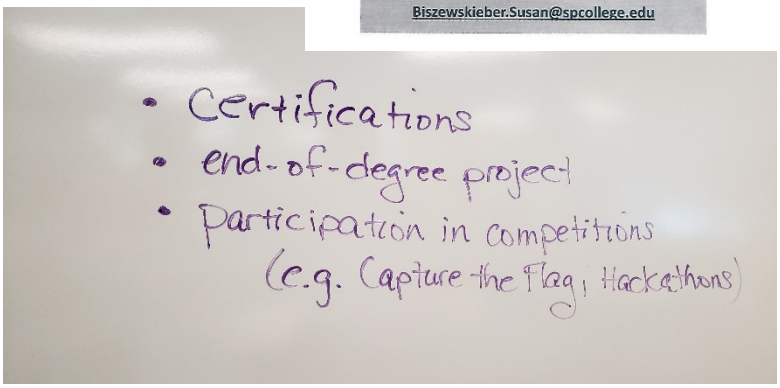
Andy Swenson: Dr. Sands, how does this compare with other groups you work with?

Dr. Sands: Very similar. When looking for junior analysts, internships and apprenticeships are important. That helps build the strongest potential programs. Nothing replaces experience.

Susan: You can make that receptionist to give her the chance she deserves; let the incumbent worker her climb that ladder.

Participants received this handout about SPC's IT apprenticeships.

After the session concluded, Ty Bond and James Quilty included in the recommended these three items be included in the cybersecurity bachelor's degree program. (Note: End-of-degree project = thesis project.)



Attendees – Sign-in Sheets

Attendees:

Business Leaders

Collaborative Labs' Engagement at St. Petersburg College
Participant Sign-In

Name of Engagement: **Business Leaders Convening - SPC Cybersecurity** *Date of Engagement:* **1/29/2019**

As a Participant of the Collaborative Labs at St Petersburg College, information from my participation in this Collaborative Labs' engagement will be kept by the College as proprietary information for the sponsoring client, not open to the public record, except as may be required as a student record and by law.

I hereby authorize St Petersburg College, the Collaborative Labs' engagement and its employees or representatives to photograph, record, tape, film or capture in permanent form my name, likeness, image, voice, and work products captured during the course of this Collaborative Labs' engagement/class for the sponsoring client. I further grant SPC my full permission to edit and reproduce any images, recordings or videos for use in any documentation relating to this Collaborative Labs' engagement and to provide such documentation to the sponsoring client. The sponsoring client and/or its legal representatives may allow for the reproduction and public publishing of any information presented and captured during the Collaborative Labs' engagement through separate written authorization.

As a willing participant, I hereby release SPC and the sponsoring client to freely use my name, information, images and digital recordings captured during this event in any print, video or digital publishing's related to this Collaborative Labs' engagement.

	Name	Organization	Email Address	Signature
1	**Keith Archibald**	Vology	karchibald@vology.com	
2	**Ty Bond**	JP Morgan & Chase	Bond, Ty	
3	**Dan Brown**	Depository Trust & Clearing Corp.	dbrown2@dtcc.com	
4	**David Bryant**	PSCU	dbryant@pscu.com	
5	**Brian Campbell**	City of St. Petersburg	Brian.Campbell@stpete.org	
6	**Bill Dalzell**	Honeywell	Dalzell, Bill (ESEA)	
7	**Lauren Deren**	Raymond James	Lauren.Deren@RaymondJames.com	
8	**Dan Doyle**	Bayside Solutions	Dan.Doyle@bsius.com	
9	**Roger Grimes**	KnowBe4	KnowBe4	
10	**Erich Kron**	KnowBe4	KnowBe4	
11	**Scott Noonan**	Rellaquest	snoonan@rellaquest.com	
12	**Joseph Pokropski**	Chase	joseph.pokropski@chase.com	
13	**Mario Ricatti**	Netwolves	mario.ricatti@netwolves.com	
14	**Daniel James Scott**	Tampabay Technology Forum	djs@tbtf.org	

Business Leaders

Collaborative Labs' Engagement at St. Petersburg College
Participant Sign-In

Name of Engagement: **Business Leaders Convening - SPC Cybersecurity** *Date of Engagement:* **1/29/2019**

As a Participant of the Collaborative Labs at St Petersburg College, information from my participation in this Collaborative Labs' engagement will be kept by the College as proprietary information for the sponsoring client, not open to the public record, except as may be required as a student record and by law.

I hereby authorize St Petersburg College, the Co
likeness, image, voice, and work products captur
reproduce any images, recordings or videos for
sponsoring client and/or its legal representatives
separate written authorization.

As a willing participant, I hereby release SPC an
publishing's related to this Collaborative Labs' en

	Name
15	Eric Sessums
16	Gary Sevelin
17	Andy Swenson
18	Derrick Thomas
19	Mathew Thomas
20	Kathy Wattman
21	Jeff Youmans
22	Ryan Irving
23	James Quilty
24	
25	
26	
27	
28	
29	

SPC

Collaborative Labs' Engagement at St. Petersburg College
Participant Sign-In

Name of Engagement: **Business Leaders Convening - SPC Cybersecurity** *Date of Engagement:* **1/29/2019**

As a Participant of the Collaborative Labs at St Petersburg College, information from my participation in this Collaborative Labs' engagement will be kept by the College as proprietary information for the sponsoring client, not open to the public record, except as may be required as a student record and by law.

I hereby authorize St Petersburg College, the Collaborative Labs' engagement and its employees or representatives to photograph, record, tape, film or capture in permanent form my name, likeness, image, voice, and work products captured during the course of this Collaborative Labs' engagement/class for the sponsoring client. I further grant SPC my full permission to edit and reproduce any images, recordings or videos for use in any documentation relating to this Collaborative Labs' engagement and to provide such documentation to the sponsoring client. The sponsoring client and/or its legal representatives may allow for the reproduction and public publishing of any information presented and captured during the Collaborative Labs' engagement through separate written authorization.

As a willing participant, I hereby release SPC and the sponsoring client to freely use my name, information, images and digital recordings captured during this event in any print, video or digital publishing's related to this Collaborative Labs' engagement.

	Name	Organization	Email Address	Signature
1	Angela Ashe	SPC		
2	John Duff	SPC - CCIT	DUFF.JOHN@spcollege.edu	
3	Dawn Ellis	SPC - CCIT	ellis.dawn@spc.edu	
4	Djuan Fox	SPC	fox.djuan@spcollege.edu	
5	Brian Frank	SPC		
6	John Long	SPC - CCIT	longsjohn@spcollege.edu	
7	Laura Malave	SPC - CCIT		
8	John Sands	CSSIA	sands.mac@gmail.com	
9	James Stewart	SPC-CCIT		
10	KEVIN THOMAS SPC		Thomas.Kevin@sp	
11	Ina Kehn			
12	Angela Ashe	SPC	ashe.angela@spcollege	
13	Susan Borzewski-Ehn	SPC		
14				

Appendix D

St. Petersburg College Board of Trustees (BOT) Agenda

AGENDA

ST. PETERSBURG COLLEGE BOARD OF TRUSTEES
March 19, 2019

EPICENTER MEETING ROOM (1-453)
13805 -58th STREET N. CLEARWATER,
FL
REGULAR MEETING: 9:00 A.M.

I. CALL TO ORDER
A. Invocation
B. Pledge of Allegiance

II. RECOGNITIONS

A. Presentation of Retirement Resolutions and Motion for Adoption
I. Vivian O'Dell *(Attending)*

B. Announcements
I. New Vice President, Institutional Advancement and Foundation Executive Director

III. COMMENTS
A. Board Chair
B. Board Members
C. President
D. Public Comment pursuant to §286.0105 FS

IV. REVIEW AND APPROVAL OF MINUTES
Board of Trustees' Meeting of February 19, 2019 *(Action)*

V. MONTHLY REPORTS
A. General Counsel
B. St. Petersburg College Foundation- Structure, Processes & Campaign Readiness Review- Ms. Susan Kubik, Principal, eAdvancement *(Presentation)*

VI. STRATEGIC FOCUS AND PLANNING
A. STUDENT SUCCESS AND ACADEMIC ACHIEVEMENT
I. Proposed 2019-2020 Academic Calendar-Mr. Djuan Fox, Director, Academic Services *(Presentation/Action)*

B. BUDGET AND FINANCE
1. Monthly Budget Report - Ms. Janette Hunt, Associate Vice President, Budget and Compliance *(Presentation)*

C. ADMINISTRATIVE MATTERS

1. Human Resources

a. Personnel Report *(Action)*

b. Annual Membership Assessment in Florida College System Risk Management *(Action)*

VII. CONSENT AGENDA

A. OLD BUSINESS **(items previously considered but not finalized)** - None

B. NEW BUSINESS

1. Workforce and Professional Development Curriculum Changes *(Action)*

2. Credit curriculum Changes *(Action)*

3. Notice of Intent to Initiate the Baccalaureate Approval Process *(Action)*

4. CAPITAL OUTLAY, MAINTENANCE, RENOVATION, AND CONSTRUCTION
   a. Downtown Parking Garage Renovation *(Action)*

VIII. INFORMATIONAL REPORTS - None

IX. PROPOSED CHANGES TO BOT RULES MANUAL - Public Hearing

6Hx23-2.22 Reappointment or non-reappointment of instructional and administrative personnel not under continuing contract *(Action)*

X. PRESIDENT'S REPORT

XI. NEXT MEETING DATE AND SITE:

April 16, 2019, EpiCenter (1-451, 1-453)

XII. ADJOURNMENT

If any person wishes to appeal a decision made with respect to any matter considered by the Board at its meeting March 19, 2019, he or she will need a record of the proceedings. It is the obligation of such person to ensure a verbatim record of the proceedings is made, §286.0105, Florida Statutes.

Items summarized on the Agenda may not contain full information regarding the matter being considered. Further information regarding these items may be obtained by calling the Board Clerk at (727) 341-3241.

***No packet enclosure**
Date Advertised: February 15, 2019

Appendix E

Notice of Letter of Intent to SPC BOT

March 19, 2019

MEMORANDUM

TO: Board of Trustees, St. Petersburg College
FROM: Dr. Tonjua Williams, President
SUBJECT: Notice of lntent to Initiate the Baccalaureate Approval Process

Approval is sought to initiate the State of Florida approval process to offer a new baccalaureate level education program.

The College seeks to submit the following Notice of lntent (NOI) {pursuant to 6A-14.095, Florida Administrative Code (F.A.C.)}. The NOI initiates the approval process to offer a Bachelors of Applied Science in Cybersecurity.

The Bachelor of Applied Science (BAS) in Cybersecurity is a professional workforce degree program covering technologies and practices designed to protect and safeguard the information resources of an organization including computers, networks, programs and data from threats such as unauthorized access, malicious or insecure programming, exfiltration, etc. In a computing framework the terms security and cybersecurity are used synonymously.

This proposed BAS degree in Cybersecurity would prepare students for a 'real world' experience as the curriculum would include multiple industry certifications covering specific security concepts and practices. Industry ce1tification validates a student's skills and knowledge in a specific area of study. Industry certificates are awarded by a professional group or a vendor and in many cases require periodic renewal. Aligning curriculum to industry certifications ensures that the curriculum is kept current with technical workforce skills that align with workforce practices. This BAS degree program would build upon students' core knowledge in key technology areas such as computers, computer networks, digital forensics, and computer security with an upper division curriculum focusing on defense and risk mitigation, software assurance, information assurance, and security management. Additional supportive information will be presented to the Board of Trustee in the formal approval application in June 2019.

Anne Cooper, Senior Vice President for Instruction and Academic Programs recommends approval.

Chancellor Kathy Hebda
Chancellor, Division of Florida Colleges 325 West Gaines Street, Room 1544
Tallahassee, FL 32399-0400

March 19, 2019

Dear Chancellor Hedba,

St. Petersburg College (SPC) respectfully submits the following as a Notice of Intent per 6A- 14.095, Florida Administrative Code to initiate the process of approval to offer baccalaureate level education.

SPC proposes to offer Pinellas County residents the opportunity to earn a Bachelor of Applied Science in Cybersecurity, a degree that compliments the traditional workforce emphasis of baccalaureate programs in state colleges by offering upward mobility into leadership roles and/or to further their education in cybersecurity master's degree programs and certificates throughout the state. The opportunity exists also to further the student's technical career skills by obtaining higher-level security industry certifications.

Program Description/Key Skills/Career Path and Employment

Title/Degree type: The Bachelor of Applied Science (BAS) in Cybersecurity is a professional workforce degree program covering technologies and practices designed to protect and safeguard the information resources of an organization including computers, networks, programs and data from threats such as unauthorized access, malicious or insecure programming, exfiltration, etc. In a computing framework the terms security and cybersecurity are used synonymously.

The proposed 120 credit hour program will consist of:
- 33 credit hours of general education courses
- 42 credit hours of lower division specialized courses
- 45 credit hours of upper division courses of 30 credits of a common core
  15 credits of courses in a chosen concentration

In the upper division all students would take a common core of security and information technology courses. Students would then have the flexibility to select one of several focused, technical sub plans for additional specialization. A key advantage of this structure is that it permits the introduction of additional sub plans in the future as the needs of the workplace change and new technologies emerge.

This proposed BAS degree in Cybersecurity would prepare students for a 'real world' experience as the curriculum would include multiple industry certifications covering specific security concepts and practices. Industry ce1tification validates a student's skills and knowledge in a specific area of study. Industry certificates are awarded by a professional group or a vendor and in many cases require periodic renewal. Aligning curriculum to industry certifications ensures that the curriculum is kept current with technical workforce skills that align with workforce practices. This BAS degree program would build upon students' core knowledge in key technology areas such as computers, computer networks, digital forensics, and computer security with an upper division curriculum focusing on defense and risk mitigation, software assurance, information assurance, and security management.

Key Skills of Graduates: The graduates of this proposed BAS program would gain essential workforce skills including the ability to secure and defend computer networks and resources, the ability to identify and adopt best practice in cybersecurity policy, the ability to identify cyber threats and vulnerabilities and the skills to mitigate the associated risks, the skills required to implement effective identify management and access methods, skill in assessing and building secure systems architecture, the ability to identify vulnerabilities in program code and to ensure secure programming practices, an understanding of the role and use of cryptographic algorithms in security, and the skills

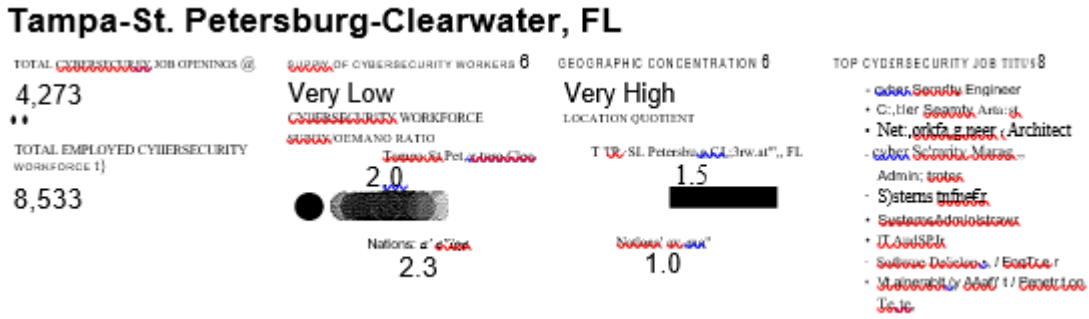
necessary to ensure that an organization's resources are secure when hosted on a cloud platform.

Career Path or Potential Employment: The Bachelors of Applied Science degree in Cybersecurity creates a seamless career path for students, including dual enrolled high school students, currently pursuing Associate in Science Degrees in career and technical programs at SPC. The A.S. degrees currently offered through the College of Computer and Information technology and Public Safety in the various Information technology and digital forensic disciplines that would articulate into this BAS program and in-and-of themselves, each qualify graduates for entry-level employment into fields such as Information Security Analysts, Programmers and Software Developers, Computer User Support, Computer Network Specialist, Network & Computer System Administrators, Computer Network Architects, and Computer System Analysts.

The curriculum in the computer technology and forensics A.S. programs at St Petersburg College are aligned with entry level industry certifications such as CompTIA A+, CompTIA Net+, CompTIA Security+ and EC-Council's Certified Ethical Hacking that provide students a pathway of milestone opportunities in the field of cybersecurity.

The proposed BAS program in Cybersecurity builds on this foundation and equips students with the skills and certifications required to be prepared for success in several of the jobs identified in the NICE Cybersecurity Workforce Framework including Systems Security Analysts, Security Control Assessors, Vulnerability Assessment Analysts, Cyber Defense Analysts, Security Architects, Information Security Analysts, Information Technology Specialists, Information Security Officers, Information Security Managers, Directors of Information Security, Chief Information Security Officers and principle cybersecurity practitioners who, as a result of this program, would better understand the evolving issues in the field of cybersecurity thereby providing opportunities for sustainable employment in the workplace.

As illustrated below, the workforce need is acute at all levels in SPC's region. (Source: https://www.cyberseek.org/heatmap.html



As industry certifications are an important component of Florida's public education system, the BAS curriculum would also align with industry certificates such as the CompTIA CySA+, PenTest+, ITIL Foundation, SSCP, CISSP, and Cloud+.

Summary of Discussions with state university and Florida College's service district

Cybersecurity is a rapidly emerging discipline. For many years security was almost an afterthought and was covered in at best one or two courses. This situation was not unique to academe as business, industry, and government were also slow to recognize the importance of investing in cyber security. This is no longer the case. Significant resources are being devoted to improving the security posture of organizations. The U.S. government has created numerous programs designed to promote and encourage the development of the nation's cyber security workforce. We now widely recognize that there are many dimensions to security and that it warrants focused study as a distinct and complex discipline.

This development, and subsequent growth in demand for cyber security professionals, has triggered the development of academic programs to attempt to address the growing need. Interestingly we see cyber security programs emerge as part of engineering programs, within business programs, and as standalone programs. This is evidence that this new discipline is complex and can be addressed from many perspectives.

The University of South Florida (USF) is the only state university in the SPC service area. St. Petersburg College enjoys a strong relationship with USF as well as the private colleges (primarily Eckerd College and The University of Tampa). SPC students have experienced seamless transitions into the upper division programs at these institutions; providing multiple upper-division options for our students.

USF offers a Bachelor of Science Degree in Cybersecurity (BSCyS). This program is offered through the College of Engineering at USF. The University of Tampa (UT) is a private institution that offers a Cybersecurity major within the College of Business. Both of these programs offer a prescribed set of courses that lead to a Bachelor of Science degree in Cybersecurity. The USF program requires 17 core courses at the 3000/4000 level while the UT program requires 24 hours of core courses. In both programs students may select several electives.

Meetings are being scheduled for further discussion with F. Frank Ghannadian the Dean of the College of Business at the University of Tampa and with Robert H. Bishop, the Dean of the College of Engineering and Sri Sridharan the Director of the Center for Cybersecurity at the University of South Florida.

Eckerd College offers a Bachelor of Science degree in Computer Science but does not offer a separate major or program of study in cybersecurity. The program proposal has been shared with USF and Eckerd College in recent months and both are supportive of SPC's decision to move forward with the application process.

The proposed SPC program is offered through the College of Computer and Information Technology. The program features a set of core courses but is distinct in that it also offers three separate sub plans within the degree program. These sub plans consisting of 15 credit hours each, enable students to focus on more specific, technical disciplines within cybersecurity.

St. Petersburg College had the privilege of being the first of the state's community colleges to begin offering Baccalaureate degrees. The college was accredited as a Level II institution by the Southern Association of Colleges and Schools to offer four-year degrees in December 2001.

Since that time, the ability to offer these higher-level degrees has been a critical part of the college's mission. It has been an on-going strategic priority to provide workforce programs at the baccalaureate level in order to meet the needs of the local community. The Baccalaureate program enrollment at the college has grown dramatically since its inception. While currently the largest of the 28 state colleges in terms of Baccalaureate enrollment and graduates, this new Baccalaureate proposal represents the college's first proposal in nearly 10 years.

Expected Term/Year of Enrollment

The college proposes to offer first term enrollment for the Bachelor of Applied Science Degree in Cybersecurity in Fall 2020.

Startup Costs

Development of the program is primarily funded by a grant from the Department of Education (DOE). St. Petersburg College submitted an application to expand cyber security programming in response to the DOE's Pilot Program for Cybersecurity Education Technology Upgrades for Community Colleges. The college was awarded a two year grant totaling $83,540. The grant will fund the development of nine new courses, faculty development, consultative services, printing, and other start-up expenses.

The current administrative structure and facilities can accommodate the new BAS program. The primary ongoing expense may be in new personnel although the college will continue to use its pool of subject matter experts who bring their rich, current experience to the classroom.

The focus areas are modeled to take advantage of existing programs, courses, facilities, and shared assets. It supports the "One College" model by unifying three distinct areas of study into one cooperative area of study utilizing every campus in the SPC network.

The information provided in this letter of intent to begin the approval process to offer baccalaureate level education at St. Petersburg College. Additional supportive information is available and will be presented in the formal approval proposal in July 2019.

Sincerely,

Tonjua Williams, Ph.D.
President
St. Petersburg College

Appendix F

Presentation Prepared for BOT Meeting

MEETING THE NEEDS OF THE CYBERSECURITY WORKFORCE

A PROPOSAL FOR A NEW BACHELORS OF APPLIED SCIENCE DEGREE IN CYBERSECURITY

CYBERSECURITY HAS EMERGED AS ITS OWN, DISTINCT DISCIPLINE

- Security has traditionally been an afterthought especially with respect to the Internet
- Slow to recognize the vulnerabilities of the Internet as business platform
- Security has, of necessity, become a priority
- Striving to catch up

THE WORKFORCE NEED IS ACUTE AT ALL LEVELS

National level

TOTAL CYBERSECURITY JOB OPENINGS
313,735

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
715,715

Florida

TOTAL CYBERSECURITY JOB OPENINGS
13,465

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
35,987

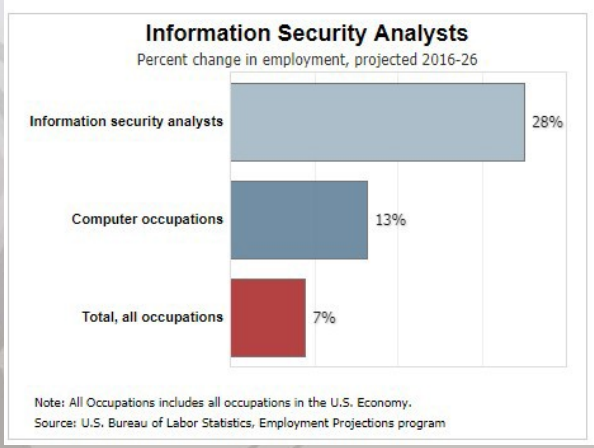
Tampa-St. Pete

TOTAL CYBERSECURITY JOB OPENINGS
4,273

TOTAL EMPLOYED CYBERSECURITY WORKFORCE
8,533

AND THE NEED IS GROWING

28%
GROWTH IS
PROJECTED
2016-2026



PROJECTED CYBERSECURITY WORKFORCE GAP

An (ISC)2 survey states that the cybersecurity workforce gap is on pace to hit **1.8 million by 2022**

SPC CURRENT OFFERINGS & ENROLLMENT

- 62 Certificate Program
- 331 Associates Degree
- 202 Information Assurance Sub Plan within BAS

THE PROPOSAL

Develop a Bachelor of Applied Science (BAS) in Cybersecurity as a professional workforce degree program covering technologies and practices designed to protect and safeguard the information resources of an organization

THE PURPOSE

- Equip cybersecurity students with advanced, real world skills needed to make an immediate impact in the workplace
- Help close the employment gap in the local, cybersecurity workforce

THE PROCESS

- Build on the existing foundation at SPC
- Create a more technically-focused BAS program
- Align the curriculum with industry certifications
- Align the curriculum with the NICE Cybersecurity Workforce Framework
- Align the curriculum with the needs of the local cybersecurity workforce

COMMUNITY SUPPORT

A group of senior, cybersecurity professionals participated in a Developing a Curriculum (DACUM) Event at the Collaborative Lab facility.

Companies represented included:

KnowBe4 Human error. Conquered.
citi
Honeywell THE POWER OF CONNECTED
CITY OF LARGO FL
st.petersburg
PSCU
JPMorgan Chase & Co.
AMGEN
ΣΟΦΙΑ SOFIA INFORMATION TECHNOLOGY CONSULTING MISSION CRITICAL SOLUTIONS
Delbridge Group

DACUM OUTCOMES

NICE Specialty Area	NICE Work Role	Aligned Certifications
Operate and Maintain	Security Systems Analyst (1)	Sec+, Server+, Cloud+, CySA+, CASP+, Pentest+, ECSA,
Securely Provision	Security Control Assessor (2)	Sec+, Cloud+, Pentest+,CySA+,CASP+
	Security Architect (5)	Cloud+, CASP+, ECND, ECSA,
Protect and Defend	Vulnerability Assessment Analyst (3)	Net+, Sec+, Project+, CySA+, CASP+, Pentest+, ECIH, ECSA, GCIH, GISP
	Cyber Defense Analyst (4)	Net+, Sec+, CySA+, Pentest+, CND, GCED,

DEVELOPMENT FUNDED BY DOE GRANT

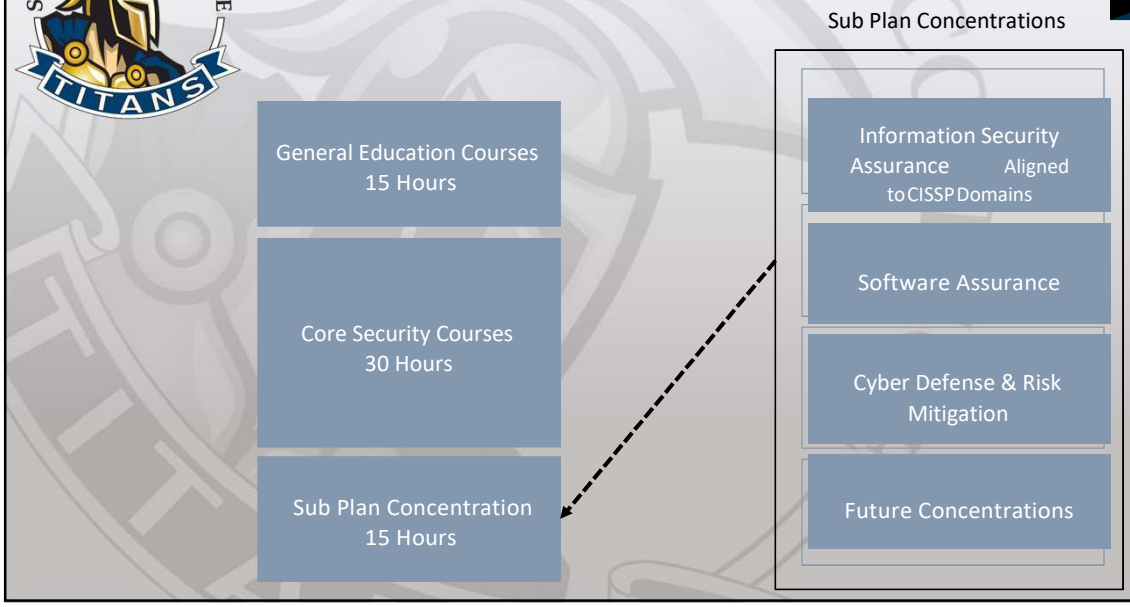
- Two year award for $83,540
- Year 1 – develop a new sub plan in the existing BAS program (4 courses)
- Year 2 – develop the new BAS degree program
- Includes faculty development and marketing
- Current staff can support delivery

YEAR 1 – NEW SUB PLAN

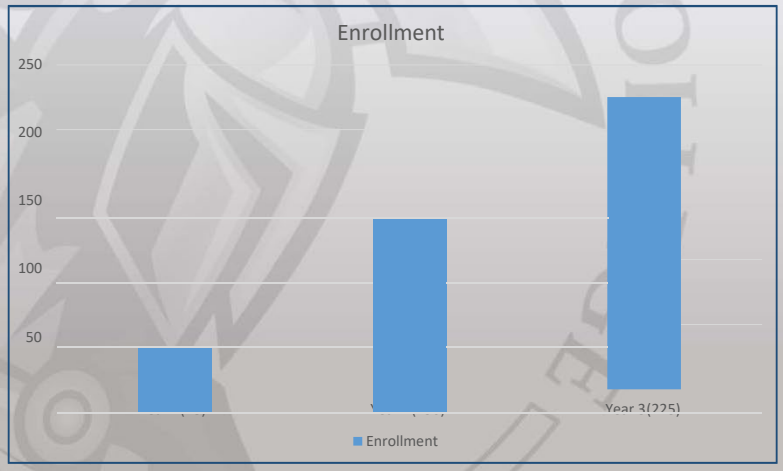
Cyber Security - Defense and Risk Mitigation

1. **Existing Course** - ISM4323 Security Essentials **[Security Analyst]**
2. **New Course** - Securing the Cloud (CNT 3421 – Cloud+) **[Security Control Assessor, Security Architect, Security Analyst]**
3. **New Course** - Vulnerability Assessment and Analysis (PenTest+) **[Vulnerability Assessment Analyst]**
4. **New Course** - Incident Detection and Response (CSA+) **[Cyber Defense Analyst]**
5. **New Course** - Secure System Architectures (CASP+) **[Security Architect, Security Analyst]**

YEAR 2 – NEW CYBERSECURITY BAS DEGREE PROGRAM



ENROLLMENT PROJECTIONS



KEY DATES AND MILESTONES

- January 2019 – DACUM Event
- March 2019
  - Board of Trustees Approval
  - Notice of Intent to Chancellor, Division of Florida Colleges
  - Minimum 100 day review period begins
- June 2019 – Baccalaureate Proposal Submitted to the State
- October 2019 – Approval from State
- August 2020 – New sub plan offered
- August 2020 – New Cybersecurity Degree Program offered

Appendix G

Program Comparison Worksheet

Program Comparison Worksheet

Pensacola State	Eastern State	West Florida	USF	Keiser University	University of Tampa
CORE	**CORE**	**NO CORE**	**CORE**	**NO CORE**	**NO CORE**
CGS 3812 Business Continuity and Disaster Recover	GEB 3213 Foundations of Managerial Communications	COT3100, COP3014, COP3530, CDA3101 taken in Soph Year	CEN 3722 Human Computer Interfaces		
CIS 3361 Security Testing & Auditing	ISM 3011 MIS		CGS 3303 IT Concepts		
CIS 3615C Secure Software Development	ISM 4300 Information Systems Operations Management		CGS 3853 Web Systems for IT		
CIS 4253 Ethics in I.T.			CIS 3213 Foundation of Cybersecurity		
CIS 4385 Computer Forensics & Investigations	MAN 4505 Operational Decision Making		CIS 3363 IT Systems Security		
CIS 4512 Information Security & Risk Management			CIS 3615 Secure Software Dev		
CIS 4596 Cybersecurity Capstone			CIS 4200 Penetration Testing		
			CIS XXXX Human Security		
Information Security Concentration	**Cybersecurity Specialization**	**Cybersecurity (Jr/Sr Years)**	CIS 4935 Senior Project for IT	**Cyber Forensics Information Security**	**Cybersecurity (College of Business)**
CIS 3367C Operating Systems Security	CEN 4341 Platform Technology	COP 4610 Theory & Fund OS	CNT 4104 Lab Comp Info Networks	Accouting for Non-Financial Majors	ITM 350 Info Sec Principles
CIS 4201 Laws & Legal Aspects of I.T.	CIS 3391C Computer Forensics	COP 3022 Int Comp Prog	CNT 4403 Network Security & Firewalls	Legal & Ethical Environments	ITM 380 Network Security
CIS 4357 Advanced Security Practitioner	CIS 3392C Windows Forensics	COP 4710 Database Systems	COP 3515 Advanced Program Design for IT	Ethics in Information Systems	ITM 480 Ethical Hacking
CNT 3411 Security Operations	CNT 3403 Network Defense Security	CNT 4007 Theory & Fund of Networking	COP 4538 Data Structures & Algorithms for IT	Security Polices & Disaster Preparedness	ITM 375 Info Sec Stds, Risk Mgt, and Compliance

Pensacola State	Eastern State	West Florida	USF	Keiser University	University of Tampa
CNT 3431 Securing the Cloud	CNT 4704 Network Planning & Design	CEN 4078 Secure Software Development	COP 4703 Advanced Database	Systems Analysis	ITM 415 Physical & Operational Security
CNT 3524 Mobile Security	COP 3330 OO Programming	CTS 4348 Linux Sys Admin	ENG 3000 Lab Foundations of Engineering	Criminal Evidence & Procedures	ITM 450 Cybersecurity Capstone
ISM 4314 Project & Change Management for I.T.	COP 3703 Database Design/ Architecture	CAP 4136 Malware Analysis	ISM 4323 Information Security & IT Risk Management	Systems Design	
	COP 3813 Internet Programming	CNT 4403 Computer and Network Security	LIS XXXX Cybersecurity Ethics	Cyber Crimes	
Cyber Forensics Concentration	COP 4849 Web Applications Programming	CIS 4385 Ethical Hacking		White Collar & Econo Crime	
ACG 3024 Accounting for Non-Financial Majors	ISM 3113 Information Systems Analysis & Design	CIS 4368 Database Security		Database Systems Mgt	
BUL 3130 Legal Environment	ISM 3321 Cybersecurity Fundamentals	CNT 4416 Cyber War Gaming		I.T. Planning	
CIS 4357 Advanced SecurityPractitioner	ISM 3324 Applications in Information Security	CIS 4595C Capstone		Digital Media Forensics	
CJE 4610 Crime Detection and Investigation	ISM 4041 Emerging Information Technologies	9 Hours of Electives		Network Forensics	
CJE 4694 Cybercrime	CEN 4949 Internship			Computer System Forensics Analysis	
CJE4696 Criminal Justice System Responses to Cyber Crimes				Network Defense & Countermeasures	
CNT 3524 Mobile Security				Org and Tech of Info Systems	

Appendix H

Internal DACUM Program Worksheet

Internal DACUM Workshop Worksheet

CORE	Status	Potential Industry Certification Alignment	Initial KU Mapping	Targeted NICE Framework Role
ISM 4330 Security Policy	Existing	CISSP	Policy, Legal, Ethics, Compliance Cyber Security Planning	Security Systems Analyst
ISM 4321 Strategic Cyber Security Enforcement	Existing	CISSP	Policy, Legal, Ethics, Compliance Cyber Threats Cyber Defense Cyber Security Planning	Security Systems Analyst Cyber Defense Analyst
CIS 4253 Ethics for Information Technology	New (grant funded 2020)	CISSP	Policy, Legal, Ethics, Compliance	Security Systems Analyst
CIS 4219 Human Aspects of Cyber Security	New (grant funded 2020)		Cyber Threats Cyber Defense	Security Systems Analyst
ISM 4338 Advanced Cyber Forensics	New (grant funded 2020)		Digital Forensics Device Forensics Host Forensics Network Forensics	Security Systems Analyst Security Control Assessor
CNT 4416 Cyber War Gaming	New (grant funded 2020)		Cyber Threats Cyber Defense	Cyber Defense Analyst Security Systems Analyst
ISM XXXX Compliance and Data Governance	New (grant funded 2020)	CISA, QSA	Policy, Legal, Ethics, Compliance	Security Control Assessor
CIS 3083 Cloud Computing Foundations	New (Internally funded)	EMC, CompTIA	Cloud Computing Networking Tech & Protocols	Security Architect Security Systems Analyst Security Control Assessor
ISM 4041 Emerging Security Technologies	New (Internally funded)		Independent/Directed Study /Research	Security Systems Analyst
ISM4915 Capstone	New (Internally funded)			

CORE	Status	Potential Industry Certification Alignment	Initial KU Mapping	Targeted NICE Framework Role
Defense and Risk Mitigation (Spring 2020)				
ISM4323 Security Essentials	Existing	CompTIA Sec+	Fundamental Security Design IA Fundamentals Intro to Cryptography	Security Systems Analyst Cyber Defense Analyst
CNT3421 Securing the Cloud	New (grant funded 2019)	(ISC)2 CCSP CompTIA Cloud+	Cloud Computing Cyber Defense Cyber Threats	Security Architect Security Systems Analyst Security Control Assessor
CTS4124 Threat Detection and Mitigation	New (grant funded 2019)	CompTIA CySA	Cyber Defense Cyber Threats	Vulnerability Assessment Analyst Cyber Defense Analyst
CIS3XXX Security Architectures	New (grant funded 2019)	CASP+	IT System Components System Administration Fundamental Security Design	Security Architect
CIS4200 Penetration Testing	New (grant funded 2019)	CompTIA Pentest+	Cyber Defense	Vulnerability Assessment Analyst
15 General Education Credits				

Appendix I

Detail of Consultations with CSSIA

Moraine Valley Community College

Invoice Detail:

Date	Description of Work	Hours
10-12-18	Review of grant award and discussion of next steps	2 hours
10-19-19	Discussion of resources available through CSSIA Center	2 hours
11-1-18	Consultative support - discussion of curriculum resources available	4 hours
12-3-18	Review/Discussion of DACUM structure and format	2 hours
12-4-18	Review and comment on DACUM invitee list	1 hour
12-5-18	Discussion of training resources available via CSSIA	2 hours
12-14 -18	DACUM discussion continued	1 hour
1-11-19	DACUM discussion continued	1 hour
1-16-19	CTF discussion regarding resources available at CSSIA (includes discussion with D. Durkee)	2 hours
1-17-19	Consultative support re: NICE resources available for curriculum and workforce mapping	2 hours
1-28-19	DACUM prep	4 hours
1-29-19	DACUM Session	8 hours
2-8-19	DACUM follow up discussion	2 hours
2-27-19	DACUM follow up, review of suggested curriculum, comment, and discussion	6 hours
3-4-19	Consultative support for curriculum development and programming	4 hours
4-8-19	Consultative Support	4 hours

4-24-19	Discussion with Dr. Stewart at CAE ELF conference in Pensacola	2 hours
4-25-19	Consultation re: CTF resources available at CSSIA	1 hour

Appendix J

Occupational Overview for Cybersecurity BAS Degree

Occupation Overview for Cybersecurity BAS Degree at St. Petersburg College

Federal CIP 11.1003

Bachelor or Associate Level Occupations

Computer and Information Systems Managers (11-3021)
Computer Network Support Specialists (15-1152)
Computer Systems Analysts (15-1121)
Database Administrators (15-1141)
Information Security Analysts (15-1122)

EMSI Q1 2019 Data Set

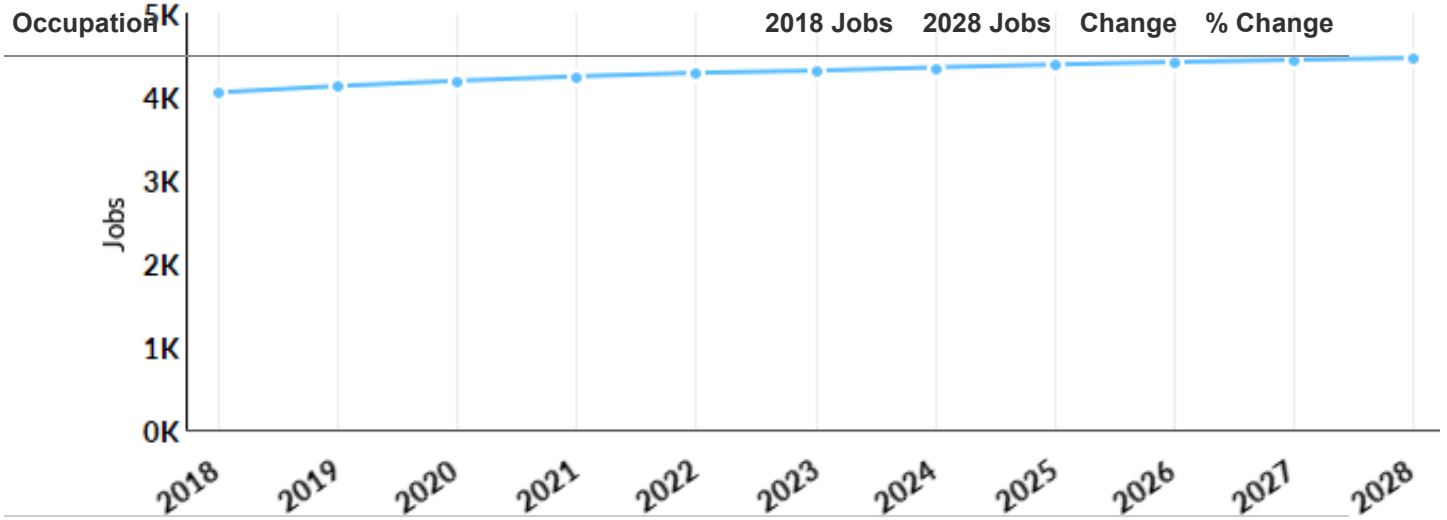
March 2019
Pinellas County, Florida

Occupation Summary for 5 Occupations

4,044	10.2%	$36.32/hr
Jobs (2018)	**% Change (2018-2028)**	**Median Hourly Earnings**
12% below National average	Nation: 13.4%	Nation: $43.33/hr

Growth

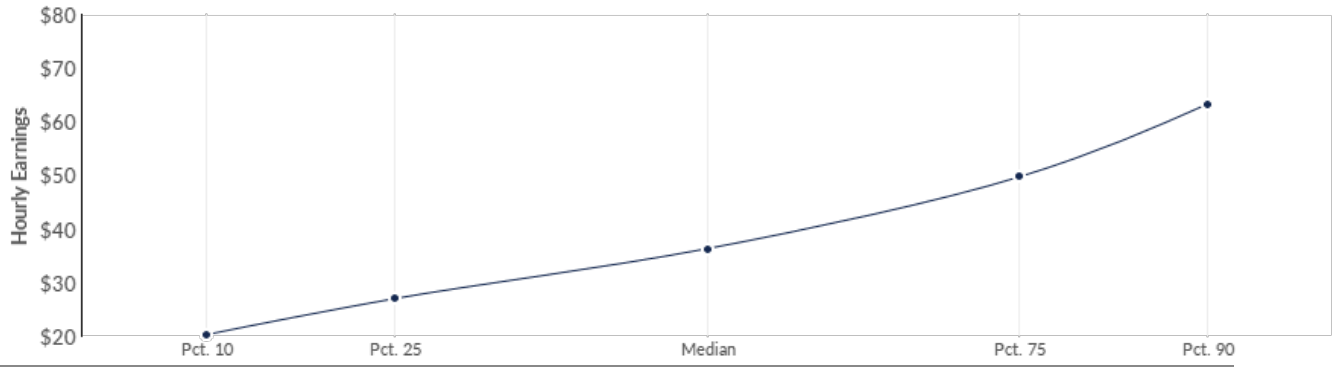
4,044	4,457	413	10.2%
2018 Jobs	**2028 Jobs**	**Change (2018-2028)**	**% Change (2018-2028)**



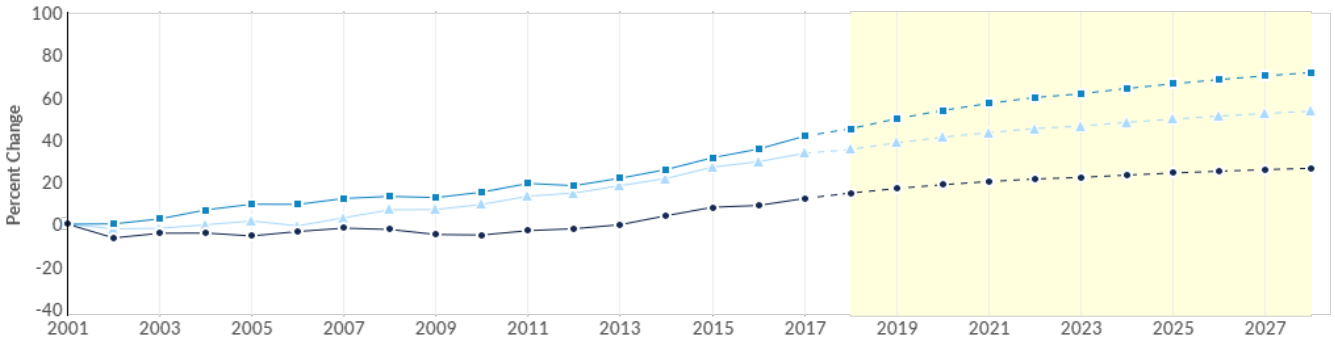
Computer and Information Systems Managers (11-3021)	1,024	1,175	151	15%
Computer Systems Analysts (15-1121)	1,484	1,609	125	8%
Information Security Analysts (15-1122)	359	428	69	19%
Computer Network Support Specialists (15-1152)	710	745	35	5%
Database Administrators (15-1141)	468	500	32	7%

Percentile Earnings

$27.00/hr	$36.32/hr	$49.73/hr
25th Percentile Earnings	Median Earnings	75th Percentile Earnings



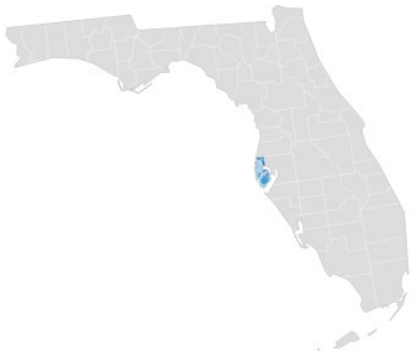
Occupation	25th Percentile Earnings	Median Earnings	75th Percentile Earnings
Computer and Information Systems Managers (11-3021)	$36.27	$53.27	$69.43
Computer Systems Analysts (15-1121)	$26.30	$33.75	$43.06
Information Security Analysts (15-1122)	$26.45	$37.28	$47.42
Database Administrators (15-1141)	$29.17	$39.39	$49.80
Computer Network Support Specialists (15-1152)	$18.47	$26.76	$35.42



Regional Growth Trends

	Region	2018 Jobs	2028 Jobs	Change	% Change
●	Region	4,044	4,457	413	10.2%
●	Florida	70,087	82,901	12,814	18.3%
●	United States	1,564,178	1,773,931	209,753	13.4%

Regional Breakdown



ZIP	2028 Jobs
Saint Petersburg, FL 33716 (in Pinellas county)	684
Clearwater, FL 33760 (in Pinellas county)	398
Saint Petersburg, FL 33701 (in Pinellas county)	286
Clearwater, FL 33759 (in Pinellas county)	252
Oldsmar, FL 34677 (in Pinellas county)	170

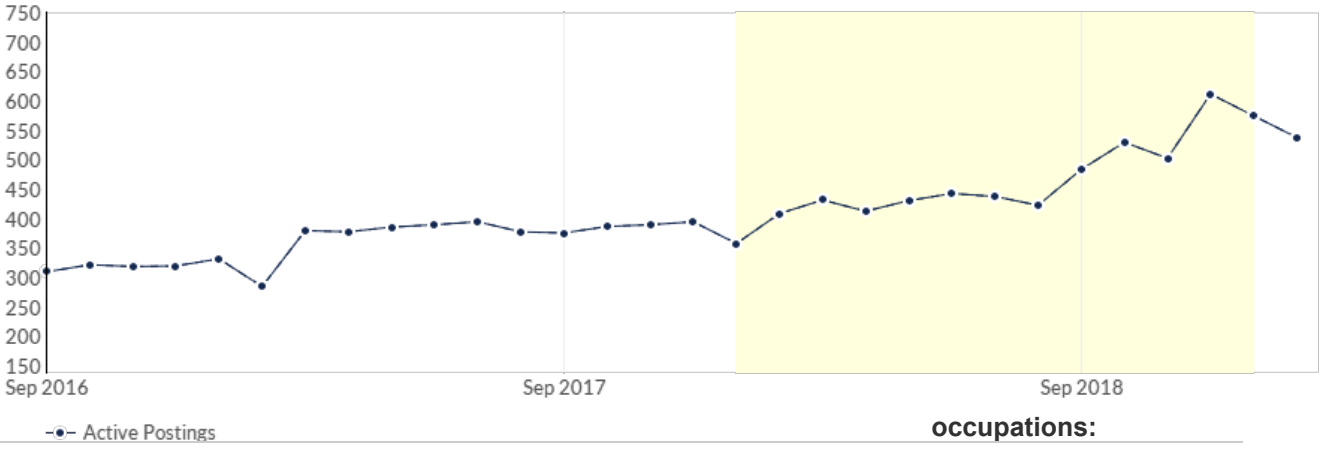
Job Postings Summary

2,749	5 : 1	33 days
Unique Postings	**Posting Intensity**	**Median Posting Duration**
19,567 Total Postings	Regional Average: 4 : 1	Regional Average: 31 days

There were **14,303** total job postings for your selection from January 2018 to February 2019, of which **2,749** were unique. These numbers give us a Posting Intensity of **5-to-1**, meaning that for every 5 postings there is 1 unique job posting.This is close to the Posting Intensity for all other occupations and companies in the region (4-to-1), indicating that they are putting average effort toward hiring for this position.

Monthly Active Postings

For these occupations:

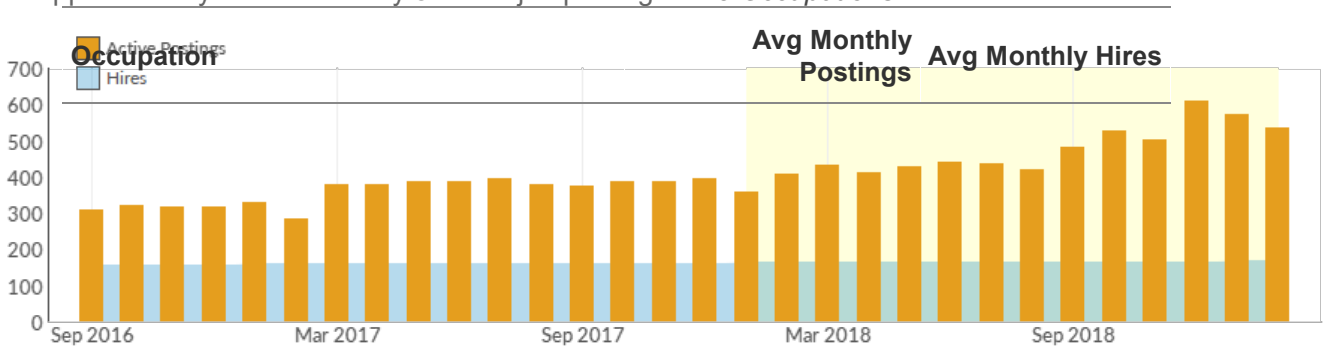


11-3021	Computer and Information Systems Managers
15-1152	Computer Network Support Specialists
15-1121	Computer Systems Analysts
15-1141	Database Administrators
15-1122	Information Security Analysts

Job Postings vs. Hires (Jan 2018 - Feb 2019)

470 **Avg. Monthly Postings** | **165** **Avg. Monthly Hires**

In an average month, there were **576** active job postings for *5 Occupations*, and **185** actually hired. This means there was approximately 1 hire for every 3 active job postings for *5 Occupations*.



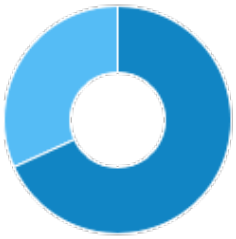
Occupation	Avg Monthly Postings	Avg Monthly Hires
Computer Systems Analysts	229	53
Information Security Analysts	100	17
Computer and Information Systems Managers	84	36
Database Administrators	53	23
Computer Network Support Specialists	5	37

Note: LMI projects 340 Average Annual Openings. EMSI Average Monthly Hires for the past year equate to 1,284 Average Annual Hires. This shows that currently there more hires than LMI is projecting.

Top Companies Posting (Jan 2018 - Jan 2019)

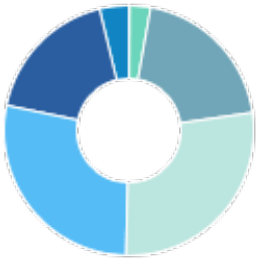
Company	Total/ Unique	Posting Intensity	Median Posting Duration
ACCENTURE, INC.	471 / 253	2 : 1	51 days
Robert Half International Inc.	2,780 / 225	12 : 1	25 days
Raymond James Financial, Inc.	946 / 135	7 : 1	15 days
Jabil Circuit, Inc.	860 / 104	8 : 1	66 days
Computer Task Group, Incorporated	158 / 75	2 : 1	30 days
Baycare Home Care, Inc.	302 / 68	4 : 1	46 days
Raytheon Company	520 / 66	8 : 1	51 days
Kforce Inc.	415 / 60	7 : 1	31 days
The Nielsen Company	601 / 57	11 : 1	52 days
Apex Systems, Inc.	424 / 40	11 : 1	44 days

Occupation Gender Breakdown



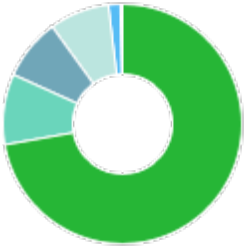
Gender	2018 Jobs	2018 Percent
Males	2,759	68.2%
Females	1,285	31.8%

Occupation Age Breakdown



Age	2018 Jobs	2018 Percent
14-18	4	0.1%
19-24	110	2.7%
25-34	805	19.9%
35-44	1,118	27.6%
45-54	1,127	27.9%
55-64	728	18.0%
65+	153	3.8%

Occupation Race/Ethnicity Breakdown



Race/Ethnicity	2018 Jobs	2018 Percent
White	2,921	72.2%
Hispanic or Latino	385	9.5%
Asian	335	8.3%
Black or African American	327	8.1%
Two or More Races	65	1.6%
American Indian or Alaska Native	9	0.2%
Native Hawaiian or Other Pacific Islander	3	0.1%

Occupational Programs

10	542	356
Programs (2017)	Completions (2017)	Openings (2017)

CIP Code	Program	Completions (2017)
11.1001	Network and System Administration/Administrator	145
52.1201	Management Information Systems, General	109
11.1003	Computer and Information Systems Security/Information Assurance	97
11.0201	Computer Programming/Programmer, General	93
11.0103	Information Technology	47

Industries Employing 3 Computer and Mathematical Occupations(2018)

	Within the Industry		
Industry	Occupation Group Jobs	Percent of Occupation Group	Percent of Total Jobs
Corporate, Subsidiary, and Regional Managing Offices	632	15.6%	3.0%
Custom Computer Programming Services	361	8.9%	13.6%
Computer Systems Design Services	345	8.5%	13.6%
Wired Telecommunications Carriers	120	3.0%	5.0%
Data Processing, Hosting, and Related Services	107	2.6%	8.5%

Parameters

Occupations

Code	Description
15-1122	Information Security Analysts
11-3021	Computer and Information Systems Managers
15-1121	Computer Systems Analysts
15-1152	Computer Network Support Specialists
15-1141	Database Administrators

Regions

Code	Description
12103	Pinellas County, FL

Timeframe
2018 - 2028

Datarun
2019.1 – QCEW Employees, Non-QCEW Employees, Self-Employed, and Extended Proprietors

****

Appendix A - Data Sources and Calculations

Location Quotient
Location quotient (LQ) is a way of quantifying how concentrated a particular industry, cluster, occupation, or demographic group is in a region as compared to the nation. It can reveal what makes a particular region unique in comparison to the national average.

Occupation Data
Emsi occupation employment data are based on final Emsi industry data and final Emsi staffing patterns. Wage estimates are based on Occupational Employment Statistics (QCEW and Non-QCEW Employees classes of worker) and the American Community Survey (Self-Employed and Extended Proprietors). Occupational wage estimates also affected by county-level Emsi earnings by industry.

Emsi Job Postings
Job postings are collected from various sources and processed/enriched to provide information such as standardized company name, occupation, skills, and geography.

Institution Data
The institution data in this report is taken directly from the national IPEDS database published by the U.S. Department of Education's National Center for Education Statistics.

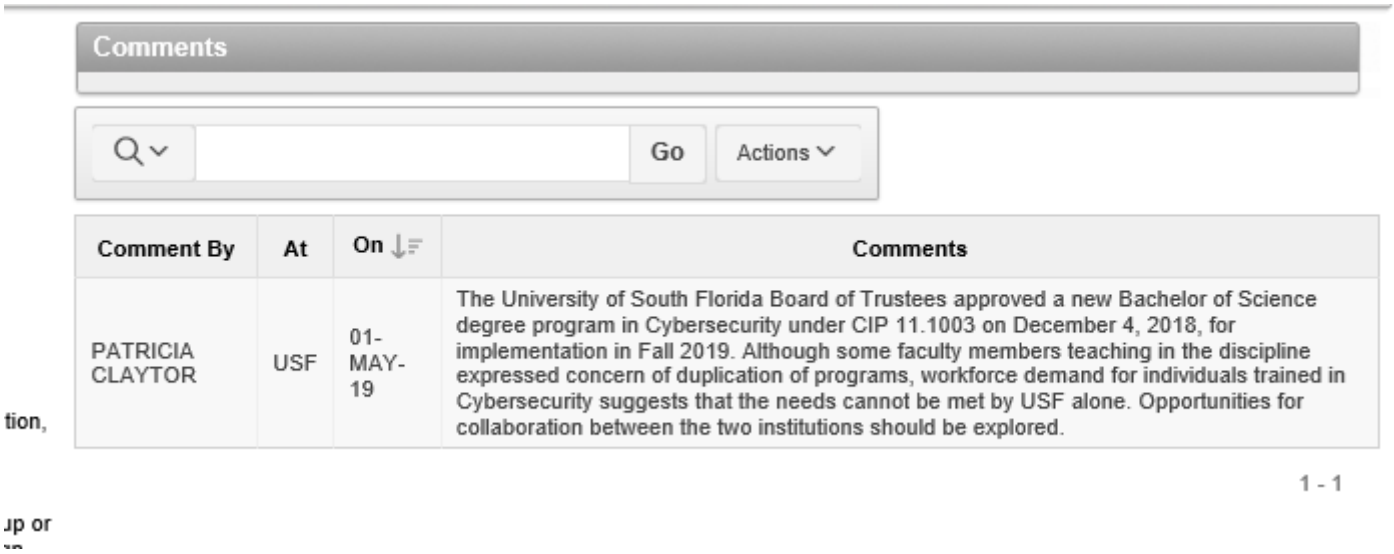
State Data Sources
This report uses state data from the following agencies: Florida Department of Economic Opportunity

Appendix K

Feedback from State Institutions Regarding NOI

From: Djuan Fox
Sent: Monday, May 6, 2019 10:12 AM
To: Tom Furlong <Furlong.Tom@spcollege.edu>; James Stewart <Stewart.James@SPCollege.edu>
Subject: RE: Academic Program Pre-proposal Recognition System

Please see the comment submitted by USF below.



Comments

Go Actions

Comment By	At	On	Comments
PATRICIA CLAYTOR	USF	01-MAY-19	The University of South Florida Board of Trustees approved a new Bachelor of Science degree program in Cybersecurity under CIP 11.1003 on December 4, 2018, for implementation in Fall 2019. Although some faculty members teaching in the discipline expressed concern of duplication of programs, workforce demand for individuals trained in Cybersecurity suggests that the needs cannot be met by USF alone. Opportunities for collaboration between the two institutions should be explored.

1 - 1

tion,

up or

Djuan Fox
Director of Academic Services
Instruction and Academic Programs
St. Petersburg College | EpiCenter
727.341.3334 | fox.djuan@spcollege.edu

From: Tom Furlong <Furlong.Tom@spcollege.edu>
Sent: Sunday, May 5, 2019 12:15 PM
To: Djuan Fox <Fox.Djuan@spcollege.edu>; James Stewart <Stewart.James@SPCollege.edu>
Subject: Fwd: Academic Program Pre-proposal Recognition System

Please review and get back to me. Thanks

Sent from my iPhone

Begin forwarded message:

From: <web_do_not_reply@flbog.net>
Date: May 5, 2019 at 5:00:05 AM EDT
To: <furlong.tom@spcollege.edu>
Subject: Academic Program Pre-proposal Recognition System

CAUTION: This email originated from outside of SPC.

Dear TOM FURLONG,

SAINT PETERSBURG COLLEGE entered information for a potential bachelor's degree program in APPRiSe.
The prospective program was titled Cybersecurity in CIP code family: 11 COMPUTER AND INFORMATION SCIENCES AND SUPPORT SERVICES.
The comment period for this prospective program has closed. The prospective program, and all comments, will remain available in APPRiSe. We appreciate your continued participation in the system and the benefit your knowledge contributes to the development of bachelor's degree programs in Florida.

Sincerely,

Karinda Barrett
Florida College System

Traki Taylor
Board of Governors, State University System

Thank You
Automatic Notification
Do Not Reply

Appendix L

SPC Press Release – SPC Designated as a National Center of Excellence in Cyber Defense Education – NSA CAE-CDE

Marketing and Strategic Communications
District Office

St. Petersburg College
SPC

This is a press release from St. Petersburg College. For more information, contact Rita Farlow, Executive Director, Marketing and Strategic Communications, 727-302-6526 or Marilyn Shaw, PR/Communications Coordinator, 727-341-4712.

SPC Named Center of Excellence in Cyber Defense Education

October is National Cybersecurity Awareness Month, which makes St. Petersburg College's latest accolade even sweeter. The National Security Agency (NSA) and the Department of Homeland Security have designated St. Petersburg College as a National Center of Academic Excellence in Cyber Defense Education (CAE-CDE) through the academic year 2024. This designation recognizes the college's contribution to meet the demands to provide a highly skilled cybersecurity workforce.

SPC is the fourth state college in Florida to receive the two-year designation for the Cybersecurity Associate in Science degree.

"This designation reflects SPC's mission to provide academic excellence for our students. We're proud to support the local growing workforce with skilled professionals to protect the cybersecurity infrastructure," SPC President Tonjua Williams said.

The goal of the CAE-CD, sponsored by the National Security Agency and Department of Homeland Security, is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cybersecurity defense and producing professionals with cybersecurity defense expertise throughout the nation.

SPC's Cybersecurity Associate in Science degree addresses the critical shortage of professionals with cybersecurity skills.

"The CAE recognition by the National Security Agency and the Department of Homeland Security validates the strength of SPC's AS Cybersecurity program," said Laura Malave, SPC Cybersecurity Academic Chair for the College of Computer and Information Technology. "SPC is preparing students for careers in Cybersecurity through practical, hands-on learning on the real-world tools used by industry professionals."

The CAE designation recognizes excellence in the institutional approach to cybersecurity, excellence of the academic program, broad inculcation of cybersecurity in all facets of the institution (including academic programs, information technology policies and broad awareness of cybersecurity issues across the campus), faculty and staff development and the institution's outreach to the community.

For information about SPC's College of Computer and Information Technology Center for Cybersecurity, visit here and for information about SPC's A.S. degree in Cybersecurity, visit here.

Appendix M

Letter of Support for St. Petersburg College Cybersecurity BAS Proposal from the University of South Florida

University of South Florida

A Preeminent Research University

February 6, 2019

Dr. Tonjua Williams
President, St Petersburg College
PO Box 13489
St. Petersburg, FL 33733-3489

Dear President Williams,

Thank you for your letter dated January 25, 2019 regarding additional areas of workforce needs in Pinellas County and how SPC and USF can work together to support the educational opportunities of the Tampa Bay region. At USF, we are thrilled to have SPC as our partner as we work with local business and industry to improve the lives of those we serve.

I am pleased give you USF's approval and continued support, as SPC begins the State of Florida's process for baccalaureate program development in the areas of:

- Cybersecurity
- Human Services
- Respiratory Care
- Digital Media Technology

I look forward to continuing our strong relationship, and thank you, President Williams, for your continued leadership.

Regards,

Judy Genshaft

Judy Genshaft
USF System President

OFFICE OF THE USF SYSTEM
University of South Florida • 4202 East Fowler Avenue • Tampa, FL 33620
www.system.usf.edu