
Florida Center for Cybersecurity



Making Florida the Cyber State

A Board of Governors Report
Submitted to the Florida Legislature and Governor
December 2013



Florida Center for Cybersecurity

Right now, Florida faces a narrow window of opportunity to capitalize on one of the most in-demand, high-paying, and rapidly growing fields of our time—cybersecurity. With six-figure starting salaries, this specialized STEM field can keep thousands of Florida graduates working in the state by creating new high-skilled jobs, attracting high-tech companies to open their doors here, and serving as a vital resource to businesses and national defense.

Within the next 12 months, one of a handful of states will emerge as the leader in cybersecurity and become the magnet that attracts the billions of dollars of private-sector and military spending that will be invested in this emerging field. Florida can become this leader.

Recognizing this need and opportunity, the 2013 Florida Legislature requested this report to provide a plan and budget to create the Florida Center for Cybersecurity, to be housed under the leadership of the University of South Florida. The charge: Secure Florida's place as the national leader in this burgeoning field. USF, through collaboration with its sister institutions across the State University System and private partners, can meet the challenge. The plan and proposed investments laid out in this report provide the blueprint for Florida to develop cybersecurity as a central pillar of its economic future.

The demand is huge. Even when compared with other high-demand IT jobs, demand for cybersecurity jobs is growing more than three times faster. Business leaders say they can't hire skilled cybersecurity workers fast enough, and our nation's military and homeland security agencies are looking for help in navigating the constantly changing world of cybersecurity research.

The question now becomes: how many of the hundreds of billions of dollars of public- and private-sector investment to be targeted at cybersecurity does Florida want to attract?

Across the State University System and at the state's independent colleges and universities, pockets of good work are now being done in this field. These include the first-of-its-kind cybersecurity master's degree approved by USF's Board of Trustees, a recent local cybersecurity outreach effort by the University of West Florida, a cybersecurity program being promoted by the Florida Institute of Technology, and a cybersecurity-emphasized bachelor's degree at Embry Riddle University, to name a few. These efforts are valuable, and there is plenty of work to go around. But if Florida wants to claim a place of national prominence in this field, it needs a center that draws these disparate pockets into a unified statewide partnership.

The Florida Center for Cybersecurity (FCC) will provide focus, organization, a cohesive workforce development strategy, faculty skills and expertise, and avenues for collaboration among many currently independent state experts.

"The diverse threats we face are increasingly cyber-based... We are losing data, money, and ideas through cyber intrusions. This threatens innovation and, as citizens, we are also increasingly vulnerable to losing our personal information... in the future, resources devoted to cyber-based threats will equal or even eclipse the resources devoted to non-cyber based terrorist threats."

— James B. Comey, FBI Director, in a statement before the Senate Committee on Homeland Security and Governmental Affairs, November 14, 2013

The mission:

- Position Florida as the national leader in cybersecurity and its related workforce through education, community engagement and innovative, interdisciplinary research;
- Create thousands of new high-paying jobs in the state's cybersecurity industry;
- Serve as a statewide facilitator for cybersecurity education—providing degrees, certificates and training while contributing to Board of Governors priorities and encouraging students in non-IT majors to obtain industry-recognized cybersecurity specializations to enhance employability and wages upon earning their desired degrees;
- Enhance Florida's cybersecurity workforce, including reintegrating military veterans by utilizing their specialized skills and training;
- Act as a cybersecurity clearinghouse for statewide business and higher education communities—sharing knowledge, resources and training opportunities to help mitigate cybersecurity threats, and optimizing investment to eliminate unnecessary duplication;
- Attract new financial, healthcare, transportation, utility and defense companies to Florida.

It is a bold, long-term vision with a high-impact, short-term return on investment.

The FCC's budget request for \$16.1 million in operating funds, coupled with millions more in repurposed existing university funds and private support, will facilitate the awarding of thousands of new high-tech, in-demand degrees, certificates and industry certifications, beginning in the spring of 2014. Annual estimates at USF alone are an additional 550 cybersecurity certificates awarded, 475 undergraduate certificates or concentrations, 270 graduate certificates or concentrations, nearly 900 more bachelor's degrees, 215 master's degrees and 50 more doctoral degrees.

These graduates will enter the workforce prepared for the six-figure-salary jobs that are waiting for them. In the last five years, the number of cybersecurity-related job postings nationwide grew by more than 70 percent, compared to postings for more general technology jobs that grew by 20 percent and postings for all jobs that grew by 6 percent.

Meanwhile, employers and the state economy will benefit from an infusion of new skills and knowledge, as well as the "multiplier-effect" that a cybersecurity workforce provides. It has been estimated that for every IT job created, an additional 1.58 jobs will be gained in a particular region.

A new state-of-the-art cybersecurity facility, built with a phased-in investment of \$30 million, will provide a central resource for the entire state, particularly with the inclusion of a sensitive compartmented information facility (SCIF) used to analyze and help protect classified information. With one such facility available for research among institutions and public and private partners, Florida can maximize efficiencies—in much the same way as the Magnet Lab at Florida State University and the research vessels assigned to the Florida Institute of Oceanography.

The demand for cybersecurity professionals over the past five years grew 3.5 times faster than the demand for other IT jobs and about 12 times faster than for all jobs.

– *Computerworld magazine*

In short, a presence in the cybersecurity industry will quickly bring Florida's economy new revenue, new jobs and an unparalleled cybersecurity knowledge base. It will drive the State University System further toward national prominence as a coordinated unit, preparing graduates for the practical, high-paying jobs of today and tomorrow.

This report has been prepared in response to a mandate by the 2013 Florida Legislature, whose vision for the creation of the Florida Center for Cybersecurity was enacted into law via proviso language in the General Appropriations Act for Fiscal Year 2013-2014 and signed by Gov. Rick Scott. Full text of the Legislature's charge to the Board of Governors is provided below:

The Board of Governors shall submit a report no later than December 1, 2013, to the Legislature and the Governor that provides a plan for the creation of a Florida Center for Cybersecurity to be principally located at, and under the leadership of, the University of South Florida. The goals of the Florida Center for Cybersecurity shall be: to position Florida as the leading state in cybersecurity and its related workforce; to create new jobs in the cybersecurity industry in the state; to educate students to excel in cybersecurity professions in the state; to enhance the capabilities of the existing cybersecurity workforce in the state; to work with the business community statewide to identify and remedy any cybersecurity vulnerabilities; and to attract financial services, healthcare, defense industry and other companies to relocate to, or startup within, the state. The report shall include any proposed capital and operational startup costs as well as a budget to support the ongoing operations of the proposed Florida Center for Cybersecurity.

Chapter 2013-40, Laws of Florida, Page 46.

Table of Contents

| | |
|---|-----|
| EXECUTIVE SUMMARY | i |
| THE LEGISLATURE'S AND GOVERNOR'S CHARGE | iii |
| NEED AND PURPOSE | 1 |
| Risks and threats | 1 |
| The national picture | 2 |
| Workforce development | 3 |
| Military veterans | 4 |
| USF and Tampa Bay | 4 |
| MAP: A STATEWIDE NETWORK | 7 |
| VISION | 9 |
| MISSION | 9 |
| Board of Governors' Strategic Priorities | 11 |
| Proposed budget summary | 13 |
| ORGANIZATION | 15 |
| Higher Education Advisory Council | 15 |
| Community Advisory Board | 15 |
| CONCLUSION | 17 |
| FOOTNOTES | 19 |
| REFERENCES | 21 |
| APPENDIX | 23 |
| Appendix A: Curriculum plan | 24 |
| Appendix B: Workforce output projections | 27 |
| Appendix C: Existing cybersecurity education programs | 30 |
| Appendix D: Common definitions in cybersecurity | 36 |
| Appendix E: Selected faculty biographies | 40 |
| Appendix F: Higher Education Advisory Council Meeting Minutes | 52 |
| Appendix G: Support for the Florida Center for Cybersecurity | 56 |

Risks and threats

Cybersecurity is increasingly vital as more and more people are connected by the Internet, businesses rely more heavily on cloud-based and big data services, and government officials face more web-based attacks related to terrorism, espionage or other areas of national security. The danger is growing exponentially as the world becomes more web-dependent. According to one research group, cyberattack incidents reported by federal agencies have grown nearly 800 percent in just the past six years.¹

Leon Panetta, then U.S. Secretary of Defense, warned in a 2012 speech that the United States could face a “cyber-Pearl Harbor . . . An aggressor nation or extremist group could use these kinds of cyber tools to gain control of critical switches. They could derail passenger trains, or even more dangerous, derail passenger trains loaded with lethal chemicals. They could contaminate the water supply in major cities, or shut down the power grid across large parts of the country.”²

Cybercrime costs the United States \$338 billion a year.

- *Robin (Montana) Williams, branch chief of cybersecurity-education awareness at the Department of Homeland Security, as quoted in the Chronicle of Higher Education September 2013*

In the private sector, PricewaterhouseCoopers has found that 93 percent of organizations experienced some form of cybersecurity breach in the previous year.

Industry analysts have estimated that cybercrime “costs more than \$10 trillion to society, with billions of dollars being stolen from small, medium, and large-sized enterprises and identities of millions compromised.”³ It’s also estimated that cyber-crime is worth \$400 billion annually.⁴

Still, it’s difficult to understand the full cost of cybercrime due to its ripple effects. Stolen intellectual property, theft of technology data, costs in cybertheft prevention, lost productivity—these cyber-crime side

effects compound the impact of directly measurable dollar losses. Estimates of annual losses range from “a few billion dollars to hundreds of billions.” U.S. Rep. Mike Rogers (R-Alabama), a member of both the House Armed Services and Homeland Security committees, claims that hackers from China alone may cost the U.S. as much as \$2 trillion.⁵

The complexity is increasing not only because more people are connected to the Internet, but also because hackers have developed “backdoor” ways to attack more complex systems. “Attackers deterred by a large company’s defenses often choose to breach the lesser defenses of a small business that has a business relationship with the attacker’s ultimate target, using the smaller company to leapfrog into the larger one,” according to a 2013 Symantec report.⁶

Like a game of Whac-A-Mole, the ingenuity of cyber hackers and the lucrative temptations that drive their creativity cannot be defeated by one-time tech solutions. The game evolves with every new device, program or app. There is even now a black market for attack toolkits, some starting at just \$15.⁷

Meanwhile, not all security threats are intentional, nor do all data breaches come from outside. Employee carelessness poses cybersecurity problems of its own.⁸ Clearly, education and behavioral changes are crucial in our efforts to keep data safe.

However, as ominous as this world of cyber-threats is, it opens up a huge workforce and research opportunity for the state that takes the lead in creating solutions. Florida should be that leading state.

The National picture

Across the country, elected officials on both sides of the aisle have taken note of the significance of cybersecurity. Following the 9/11 attacks, the administration of former President George W. Bush was among the first to recognize the importance of cybersecurity as an issue of national security, and the emphasis has continued and investment strengthened under the current administration and Congress. The federal Comprehensive National Cybersecurity Initiative (CNCI) called cybersecurity “one of the most serious economic and security challenges we face as a nation.”⁹

In much the same way that Florida has greatly benefited from being a hub of 20th and early 21st century military activity and spending, the state must adapt to ensure it remains the center of 21st century cyber- and high-tech-warfare and federal defense investment. Our nation will inevitably invest trillions in its national cyber-defense over the next 25 years. Should that investment be made in Florida, or should those trillions of dollars in investment and human capital be ceded to other states who choose to invest their limited state funds in becoming America’s leader in cybersecurity? Two of the CNCI’s initiatives directly acknowledge the need to expand the effort beyond the federal government, paving the way for Florida to stake its claim in this growing field through an investment like the FCC:

Initiative #8: Expand cyber education

While billions of dollars are being spent on new technologies to secure the U.S. Government in cyberspace, it is the people with the right knowledge, skills and abilities to implement those technologies who will determine success. However there are not enough cybersecurity experts within the Federal Government or private sector to implement the CNCI, nor is there an adequately established Federal cybersecurity career field. Existing cybersecurity training and personnel development programs, while good, are limited in focus and lack unity of effort. In order to effectively ensure our continued technical advantage and future cybersecurity, we must develop a technologically-skilled and cyber-savvy workforce and an effective pipeline of future employees. It will take a national strategy, similar to the effort to upgrade science and mathematics education in the 1950’s, to meet this challenge.

Initiative #9: Define and develop enduring “leap-ahead” technology, strategies, and programs

*One goal of the CNCI is to develop technologies that provide increases in cybersecurity by orders of magnitude above current systems and which can be deployed within 5 to 10 years. This initiative seeks to develop strategies and programs to enhance the component of the government R&D portfolio that pursues high-risk/high-payoff solutions to critical cybersecurity problems. The Federal Government has begun to outline Grand Challenges for the research community to help solve these difficult problems that require ‘out of the box’ thinking. In dealing with the private sector, the government is identifying and communicating common needs that should drive mutual investment in key research areas.*¹⁰

The Cybersecurity Enhancement Act of 2010 (HR 4061), which passed with unusually strong bipartisan support, authorized “hundreds of millions of dollars for cybersecurity research and education.” This appropriation included funding for the National Science Foundation “to increase the size and skills of the cybersecurity workforce” and aimed to increase “research and development, standards development and coordination, and public outreach” in cybersecurity.

U.S. Chief Information Officer Steven VanRoekel said more than \$13 billion has been recommended for cybersecurity. The Pentagon said in its spending plan that “Defense initiatives include creating teams of cybersecurity specialists to carry out defensive and offensive operations and constructing a new joint programs center for U.S. Cyber Command.” Moreover, Pentagon spending on cybersecurity is forecasted to jump from \$3.9 billion to \$4.7 billion in fiscal year 2014.¹²

The importance of establishing the FCC is summed up by Symantec's Francis deSouza: "We should see a building of the education foundation that will support the U.S. as a world leader in information security. . . . And we should see more focused research in a collaborative effort between the public and private sectors."

Workforce development

As Floridians and statewide organizations conduct more of their day-to-day business online, transmitting or storing confidential or sensitive information electronically, the need for network and information security has increased exponentially. Today, professionals with experience in cybersecurity are among the most sought after employees in the state.

Over the past two years, the number of jobs requiring a Certified Information Systems Security Professional (CISSP) certification has jumped from 19,000 to more than 29,000.

– *Computerworld magazine March 2013*

How sought after? In the last five years, the number of job postings for all jobs grew by 6 percent. Postings for technology jobs grew by almost 20 percent. Postings for cybersecurity-related jobs grew by more than 70 percent, according to a Computerworld report.¹⁴ According to the federal CNCI, "There are 30,000 specialists needed today, but only about 2,000 have necessary skills." Industry analysts estimate the market for cybersecurity services could exceed \$120 billion globally by 2017.

According to the U.S. Department of Labor (Career One Stop, www.careerinfonet.org) demand for Information Security Analysts in Florida will increase 19 percent between 2010 and 2020, serving the fourth-largest statewide market need behind only California, Virginia, and Texas.

Simply look to local help-wanted ads. In just one year, according to one workforce analysis in Tampa Bay, job postings from IT companies like IBM, Lockheed Martin and JPMorgan Chase increased from 734 positions to 1,230 (a 68 percent annual increase).¹⁵ The report noted that Hillsborough and Pinellas counties expect an average growth rate for IT jobs of 15.8 percent through 2019, higher than the expected 13.6 percent rise of all employment in the same period. The report singles out cybersecurity as a rapidly expanding field.¹⁶

Moreover, growth in high-expertise jobs has a "multiplier" effect that benefits local economies. That same report notes that IT jobs as a whole accounted for nearly 56,000 jobs in Hillsborough/Pinellas in 2012, with a "labor income" contribution to the area's economy of \$4.7 billion annually and a multiplier effect of an additional 88,000 jobs. "Expressed in terms of a multiplier, for every job in IT, another 1.58 jobs will be gained in the region," the report indicates.

Not only are cybersecurity jobs in incredibly high demand, they are also very high paying. The 2012 median salary for Information Security Analysts in Florida was \$74,200 (rising to \$117,800 at the 90th percentile). High demand and high salaries are replicated for those in related occupations in Florida: Network and Computer Systems Administrators (\$72,600/\$113,800); Computer Systems Analysts (\$83,800/\$128,200); Computer and Information Systems Managers (\$120,500/\$187,200); Computer Network Support Specialists (\$50,500/\$90,700); and, Computer Occupations, All Other (\$73,900/\$103,700).

Specifically, Payscale.com lists the annual salary range for graduates with a bachelor's degree in cybersecurity at \$54,000 to \$82,000, depending on occupation, while a master's degree in cybersecurity yields an annual salary range of \$53,249 to \$98,477. Perhaps more importantly, Payscale.com reports that graduates with selected professional certifications in cybersecurity—one of the immediate and most prioritized return-on-investment strategies of the FCC—realize significant supplements to annual salary:

| | |
|---|--------------------------------------|
| Certified Information Systems Security Professional (CISSP) | \$109,464 to \$154,178 ¹⁷ |
| Certified Ethical Hacker (CEH) | \$100,000 |
| SANS/CIAC Certified Forensic Analyst | \$85,000 |
| Microsoft Certified Professional | \$70,000 |
| CompTIA Security+ | \$69,919 |
| Cisco Certified Network Associate (CCNA) | \$67,407 |

Military veterans

According to a 2013 report by online job-search engine Monster.com, the number of U.S. military veterans rejoining the civilian population in each of the next four years will be substantial: 300,000. The hardest hit veterans in the current unemployment figures belong to the age range of 20-24, at 19.1 percent as of April 2013, compared to a national average of non-veterans in that age group of 6.9 percent.¹⁸

Military veterans are uniquely qualified for the cybersecurity field because of their training, and often, their security clearances.¹⁹ The FCC's programs will provide skills that will not only capitalize on veterans' strengths but will also provide nearly immediate access to the kinds of jobs that will enable them to remain in the state and contribute toward its economic growth.

The FCC will conduct an extensive outreach and support program aimed specifically at recruiting and training military veterans for these cyber jobs.

USF and Tampa Bay

The University of South Florida is a top-tier global research university dedicated to student success. It is home to the USF Institute for Secure and Innovative Computing (40.1540), which has been preparing graduates to meet cybersecurity workforce needs for many years—with still booming demand. The institution is located in Tampa Bay, one of the largest and fastest-growing metropolitan areas in the U.S, with a population of more than 4.3 million people. It's at the western end of the I-4 High-Tech Corridor and near MacDill Air Force Base. Home to both U.S. Central Command (CENTCOM) and U.S. Special Operations Command (SOCOM), the region is a hotbed for national defense operations as well as for healthcare, technology and financial services.

USF has been designated as one of the top four veteran-friendly universities in the nation. With the number of enrolled veterans growing each year, 10,000 active duty service men and women working at MacDill Air Force Base (excluding CENTCOM and SOCOM), and 1,200 retiring from the base annually and seeking to reintegrate into the civilian workforce, the supply of prospective cybersecurity students and employees with the requisite security clearance represents a significant pool of talent that will be attractive to new businesses looking to relocate to Florida.

USF also has a highly successful track record in drawing research funding (\$413 million in FY 2013) and is ranked 10th in the world among universities granted U.S. patents.²⁰ In addition, USF—the founder of, and home to, the National Academy of Inventors—is enhancing its researchers' impact and visibility.

USF has demonstrated a commitment to interdisciplinary collaboration. Because cybersecurity touches nearly every area of information use and every facet of life—from national security and politics to business and personal privacy—this field is among the most interdisciplinary of any. There are substantial and useful intersections in cyber-research with policy, law, compliance, psychology, criminology and forensics. Locating the FCC at USF will enable the center to tap into an existing, robust group of well-credentialed research and teaching faculty in a wide range of disciplines.

“Not a day goes by that you don’t hear about the latest data breach, identity theft or other malicious cyber-attacks. It’s becoming more prevalent, impacting individuals, as well as businesses of all sizes. . . USF has a proven track-record of working on classified cybersecurity projects, and engaging with the Department of Defense, as well as an outstanding faculty with the knowledge base and research background to offer bachelor’s and master’s degrees in cybersecurity along with certificates and certifications.”

– Bob Dutkowsky, CEO of Tech Data Corporation, Florida’s second- largest Fortune 500 headquartered company

With an appropriate level of investment by the state and repurposing of some existing USF resources, USF could undertake a bold expansion of existing degree and certificate programs (in business, engineering and the iSchool) along with the design and delivery of new marketable tracks/certificates to enhance career opportunities for high-enrollment degree programs, including criminology (cybercrime) and psychology (cyberbehavior). In addition, USF could radically increase the number of professional certifications awarded to both USF graduates and current employees in partnership with the private sector.

USF also has strong private-sector support. The Tampa Bay Partnership, an eight-county²¹ coalition led by local CEOs to promote regional economic development, is among many active professional groups nurturing the financial and industrial base of the area around USF. The region is home to 26,000 retail establishments; 27,000 finance, insurance, and real estate offices; 110,000 service providers; 16,000 construction companies; 5,600 manufacturing concerns; 7,000 wholesale trade offices; and 3,000 government establishments—with a

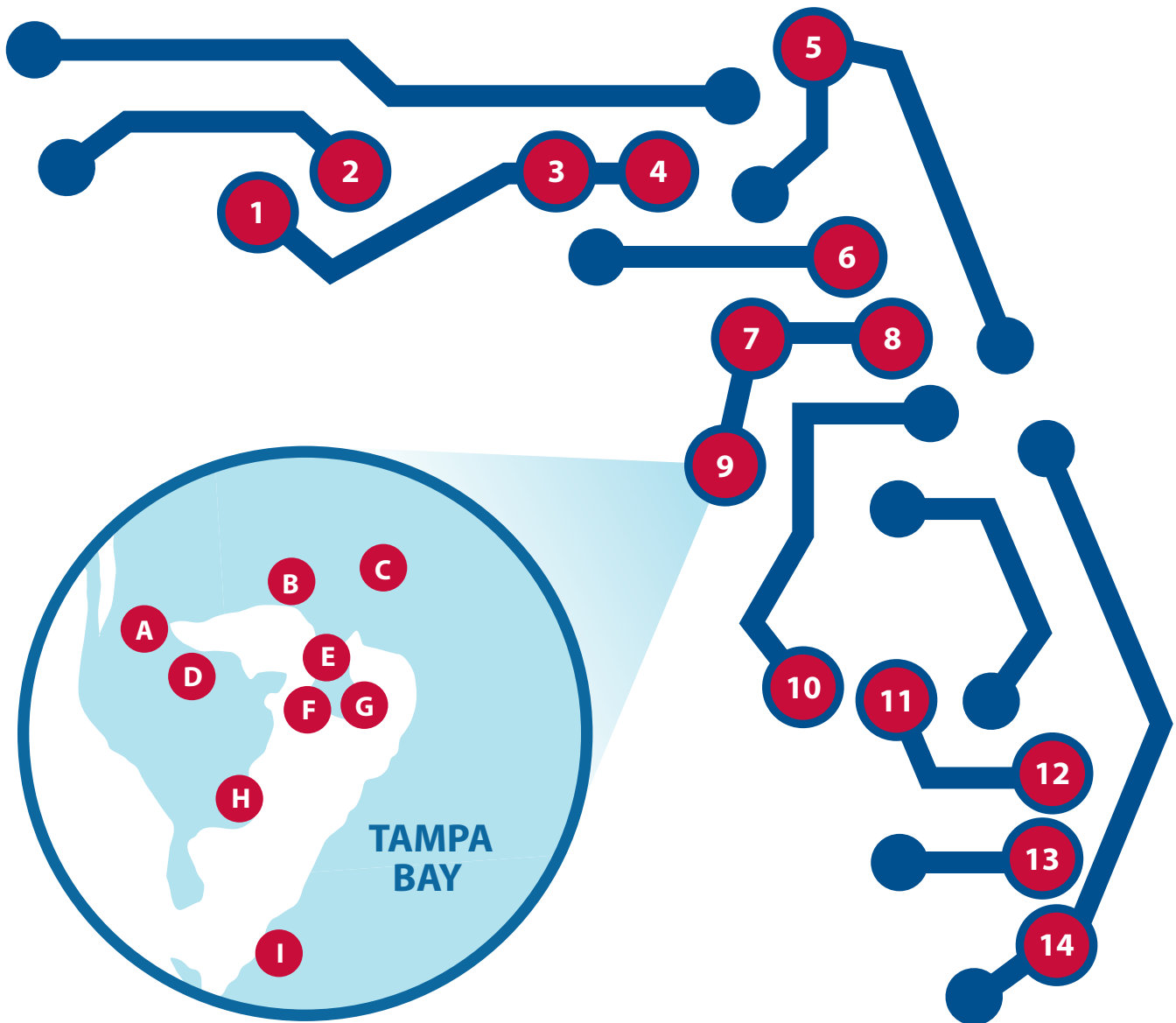
combined industry workforce of just under two million people.²² The Partnership estimates that 45 percent of the current population is in the prime employment years of 18 to 54;²³ a strong workforce pipeline in need of the high-paying jobs that IT positions provide.

Tampa Bay is home to several major health care employers, such as the James A. Haley Veterans’ Administration Hospital, All Children’s Hospital, Tampa General Hospital, and Moffitt Cancer Center, and has four top employers on the Fortune 500 list²⁴: World Fuel Services, Publix Supermarkets, Tech Data and Jabil Circuit. Many of these businesses and employers will increasingly need help keeping data and financial records secure as potential cyberattacks become more complex and difficult to fend off.

USF has a history of collaboration not only with the business community, but across the State University System. For example, the Florida Institute of Oceanography (FIO), which is housed at USF, has been continually lauded as one of Florida's best examples of partnership and cooperation. FIO's mission—to provide a diverse and collaborative statewide research and education forum, to leverage intellectual resources within the State University System, to strengthen networks and work together to benefit the general public and policymakers—closely mirrors the FCC's goals. It is USF's hope that its sister institutions in the State University System will see great benefit from the resources, knowledge and connections the FCC will provide and opt into the collaboration provided by the FCC, much like the shared experiences and successes of the FIO.

This is a prime time for collaboration in the State University System, as further evidenced by another system initiative, the Sunshine State Education and Research Computing Alliance (SSERCA). This joint effort among USF, the University of Florida, Florida State University, the University of Central Florida, Florida International University and the private University of Miami, aims to build a statewide infrastructure to support collaborative research in the world of big data—another technological world that would benefit from a strong cybersecurity knowledge base. These kinds of partnerships are good uses of state resources.

A Statewide Network



TAMPA BAY

- A Tech Data
- B Tampa International Airport
- C University of South Florida
- D Jabil Circuits
- E MacDill Air Force Base
- F U.S. Special Operations Command
- G U.S. Central Command
- H USF St. Petersburg
- I USF Sarasota-Manatee

AROUND THE STATE

- | | |
|----------------------------------|---|
| 1 University of West Florida | 8 University of Central Florida |
| 2 Eglin Air Force Base | 9 University of South Florida/Tampa Bay |
| 3 Florida A&M University | 10 New College of Florida |
| 4 Florida State University | 11 Florida Gulf Coast University |
| 5 University of North Florida | 12 Florida Atlantic University |
| 6 University of Florida | 13 Florida International University |
| 7 Florida Polytechnic University | 14 United States Southern Command |

Vision

The Florida Center for Cybersecurity at USF will be a national model in cybersecurity, cyber-intelligence and digital forensics to create a safe and secure information infrastructure for business and national security.

Mission

Guided by the goals the Legislature and Governor enumerated in the proviso language that commissioned this report, the FCC will pursue a bold vision and university-led mission to establish Florida as the nation's leader in cybersecurity in the following ways:

- Position Florida as the national leader in cybersecurity and its related workforce through education, community engagement and innovative, interdisciplinary research;
- Create thousands of new high-paying jobs in the state's cybersecurity industry;
- Serve as a statewide facilitator for cybersecurity education—providing degrees, certificates and training while contributing to Board of Governors priorities and encouraging students in non-IT majors to obtain industry-recognized cybersecurity specializations to enhance employability and wages upon earning their desired degrees;
- Enhance Florida's cybersecurity workforce, including reintegrating military veterans by utilizing their specialized skills and training;
- Act as a cybersecurity clearinghouse for statewide business and higher education communities—sharing knowledge, resources and training opportunities to help mitigate cybersecurity threats, and optimizing investment to eliminate unnecessary duplication;
- Attract new financial, healthcare, transportation, utility, and defense entities to Florida.

Position Florida as the national leader in cybersecurity and its related workforce

Florida can become the leading state in education, research and job production in cybersecurity. To do so, the FCC must dramatically increase the number of cybersecurity degree and certificate graduates and become nationally known for cutting-edge research and global connections. It will also achieve this goal by pursuing an aggressive agenda to encourage non-IT students to seek industry-recognized certifications in cyber professions and specialties that increase employability and wage earning potential within their desired fields of study.

The FCC will provide Floridians with a central location and e-portal to coordinate cybersecurity education and training, research and statewide outreach. It will serve students, parents and employers through an online cybersecurity platform by identifying career pathways; existing programs offered in K-12, state colleges, state and private universities; and available professional certifications. It will also offer employers a cyber-marketplace to post vacancies, identify qualified employees and provide curriculum feedback to ensure Florida's institutions are teaching the skills they need in future employees.

In addition, the FCC will work with external partners to obtain data or research sponsorships, foster interdisciplinary collaboration among researchers, and recruit postdoctoral students to enhance research productivity. It will serve as a valued resource for the entire State University System and for the state's independent higher education institutions, leveraging, promoting and branding Florida's many strengths to claim a place of national prominence.

Create new jobs in Florida's cybersecurity industry

Education and outreach to Florida businesses and citizens will support job creation for thousands of highly paid cybersecurity specialists—particularly as awareness of threats increases and as a well-trained workforce grows to meet needs. In addition, the center itself, along with employment generated by increased research funding, will boost the state's workforce.

USF awards more than 10,000 degrees each year, a quarter of which are in STEM fields. The projected addition to workforce development in cybersecurity, as estimated by USF, includes increasing the number of new professional cybersecurity certifications to be awarded annually (550, each with earning potentials of approximately \$100,000) by USF Innovative Education through online and face-to-face courses, beginning in spring of 2014. (See Appendix A for curriculum details.)

Educate students to excel in Florida's cybersecurity professions

The FCC will ensure students have a speedy and productive pathway to a high-paying career through high-quality education, shaped around the rapidly changing needs of business and industry. Beginning in fall 2014, USF will offer a multidisciplinary master's degree in Cybersecurity with four degree concentrations: Cyber Fundamentals (CF), Cyber Intelligence (CI), Cybercrime (CC), and Information Assurance (IA). (For more specifics and courses, see Appendix A.)

USF's program will be interdisciplinary at its core, making it easy to conduct advanced cybersecurity research. Additionally, students enrolled in programs across the university can benefit from a cybersecurity specialization through certificates offered through the FCC. For example, a criminology student may pursue a specialization in cyber-crime; a psychology student may delve into the behavioral aspect of cyber-criminal profiling—thus graduating with the FCC's assistance with an industry-recognized, highly-employable certification as a cyber-professional within their major of choice.

A nationally recognized website that ranks education programs found that while the number of students graduating with degrees in cybersecurity-related programs tripled nationally between 2006 and 2010 (from about 1,200 in 2006 to close to 3,600 in 2010), the number of Florida graduates from similar programs remained stagnant—at the same very low level of just over 60 in 2010.²⁵ The initial rates of degree completion goals in the FCC's plans would increase Florida's figure by 17 percent in the first year, and by 33 percent including certificate completions.

Enhance the capabilities of Florida's existing cybersecurity workforce

Continuing education for retooling and retraining the cybersecurity workforce will be essential given the rapidly changing nature of the field. The FCC will offer specialized training and certifications to existing cybersecurity workers, ensuring that Florida's workforce remains on the cutting-edge. Reintegrating military veterans into this field will be mutually beneficial, as the state's cybersecurity workforce will benefit from their unique skills, training and clearance.

Work with the business community statewide to identify and remedy cybersecurity vulnerabilities

The FCC will act as a collaborative cybersecurity repository for statewide business and higher education communities—coordinating existing resources, sharing knowledge, offering professional compliance and risk-assessment services and helping to mitigate cybersecurity threats. The FCC will also offer consumer and corporate education programs. As one example, the FCC plans to offer "Cybersecurity for CEOs" training sessions, providing the business community with a clearer understanding of cybersecurity threats and defenses—an idea generated directly from state business leaders who provided feedback for the FCC's direction.

Attract financial services, healthcare, defense industry and other companies to relocate to or start up within the state

The FCC will work closely with Enterprise Florida/Workforce Florida to respond to the needs of existing companies, those that are new to Florida and those that are considering locating to Florida. Having a ready supply of highly trained security specialists will attract cybersecurity companies to Florida, in addition to retaining companies who may be thinking of leaving the state due to insufficient talent. Additionally, the research performed at the center and resulting commercialization will entice industries to take advantage of Florida's expertise. The patents, licenses, software and hardware that will inevitably be discovered and developed through this research will lead to "home-grown" Florida start-up companies that can lead the industry.

Board of Governors' Priorities

The FCC's mission is grounded in education and workforce development, applied research and innovation and statewide engagement. They are guided by the Board of Governors' goals for the State University System, identified in the System's 2012-2025 Strategic Plan:²⁶

| STATE UNIVERSITY SYSTEM GOALS | EXCELLENCE | PRODUCTIVITY | STRATEGIC PRIORITIES FOR A KNOWLEDGE ECONOMY |
|------------------------------------|---|--|--|
| TEACHING & LEARNING | STRENGTHEN QUALITY & REPUTATION OF ACADEMIC PROGRAMS AND UNIVERSITIES | INCREASE DEGREE PRODUCTIVITY AND PROGRAM EFFICIENCY | INCREASE THE NUMBER OF DEGREES AWARDED IN STEM AND OTHER AREAS OF STRATEGIC EMPHASIS |
| SCHOLARSHIP, RESEARCH & INNOVATION | STRENGTHEN QUALITY & REPUTATION OF SCHOLARSHIP, RESEARCH AND INNOVATION | INCREASE RESEARCH AND COMMERCIALIZATION ACTIVITY | INCREASE COLLABORATION AND EXTERNAL SUPPORT FOR RESEARCH ACTIVITY |
| COMMUNITY & BUSINESS ENGAGEMENT | STRENGTHEN QUALITY & RECOGNITION OF COMMITMENT TO COMMUNITY AND BUSINESS ENGAGEMENT | INCREASE LEVELS OF COMMUNITY AND BUSINESS ENGAGEMENT | INCREASE COMMUNITY AND BUSINESS WORKFORCE |

(p. 13 of the Board of Governors Strategic Plan)

Teaching and Learning

In its 2012-2025 Strategic Plan, one of the three pressing needs identified by the Board of Governors is "high skilled, high demand graduates for the state's workforce." The FCC will produce thousands of degrees in a particularly high-demand STEM area, a Board of Governors Area of Strategic Emphasis, and through collaboration with other universities and external partners, will maximize productivity and efficiency.

Importantly, the FCC will also help align higher education with the state's critical workforce needs. According to the Board of Governors' Access and Attainment Commission's gap analysis, the top occupations in which there is a projected annual under-supply, exceeding 2,000 projected positions, are in the STEM field. Specifically, this critical gap exists in computer occupations, including computer systems analysts, computer programmers and computer network architects—all clearly aligned with cybersecurity.

Scholarship, Research and Innovation

USF has a long and successful record of securing federal and industry funding to support university-based applied and basic research on behalf of the defense, health and business sectors. With the requisite clearances in place, top secret and classified research continues at USF. As host to the FCC, USF will track and, to the extent necessary, coordinate statewide research activities related to cybersecurity by bringing the combined assets of the state's research community (including

universities and groups like Draper and SRI) together to strengthen Florida's competitive position and perhaps more importantly brand Florida as a state cohesively attaining national cybersecurity preeminence.

Federal and private levels of investment in Cybersecurity R&D are expected to continue to grow for years to come. The FCC effort will include building statewide collaborations around any Florida organization – public or private – that is willing to partner. Some prime candidates to begin the statewide collaborative effort include the Institute of Secure and Innovative Computing (USF), the Center for Security and Assurance in Information Technology (FSU), and the Center for Cryptology and Information Technology (FAU).

Future FCC facilities, including a sensitive compartmented information facility (SCIF) used to analyze and help protect classified information, can serve as a shared resource for the State University System. This facility is essential when performing sensitive, high-security-clearance research, as with many projects now funded via federal grants through the National Security Administration, National Science Foundation, National Institutes of Health, and Department of Defense. Such a facility built at USF, which already has the highest level of clearance, represents the first phase of capital needs envisioned to provide for shared-use by Florida's research community in much the same way as the Magnet Lab at FSU and the research vessels assigned to the Florida Institute of Oceanography.

Community and Business Engagement

Conferences will bring together researchers and students from a range of institutions and think-tanks to counter threats of cybercrime. Internships through the center will provide students with real-world, hands-on experiences and help students begin shaping their professional networks. The FCC will work with school boards and teachers in grades 5-12 to raise students' understanding of security risks in social media and online activities.

USF is already developing strong ties to statewide and national organizations to advance Florida's cybersecurity reputation, including Workforce Florida, the Florida Department of Law Enforcement, Enterprise Florida, the Florida I-4 High-Tech Corridor Council, local and state chambers of commerce and economic development councils, research firms such as Draper and SRI International, Department of Defense commands, the Maryland Cybersecurity Center, the National Cyber Partnership, and NSA Centers of Academic Excellence.

The National Cyber Partnership (NCP), based in Tampa Bay with USF as a founding partner, is a not-for-profit organization with the following objectives:

- Provide information and various resources to cyber-related industries, educational institutions and government, including the military, and the general public,
- Develop a deep understanding of issues involving both public and private sector benefits from cybersecurity enterprises, R&D, education, training and other related activities, and
- Obtain bi-partisan federal, state and local support for the purposes and goals of NCP.

USF has signed a Memorandum of Understanding with NCP with the intent to enter into a strategic partnership. The partnership is expected to help the FCC achieve national recognition and extend its reach to the entire nation.

USF has also entered into agreements with other private cybersecurity service providers based in Florida, including Crystal Clear Technologies, a company specializing in the development of cyber-secure facilities like the SCIF described above; and the International Information Systems Security Certification Consortium, Inc. (or ISC²), the provider of the gold-standard in cybersecurity industry certifications, the Certified Information Systems Security Professional certification (CISSP). In the past two years alone, the number of jobs requiring the CISSP jumped from about 19,000 to more than 29,000, according to Computerworld.

Proposed budget summary

Meaningful and robust achievement of the FCC's goals, as identified by the 2013 Legislature and supported by Gov. Rick Scott, and branding Florida as "the Cyber State," ready and willing to partner with defense and private sector organizations, will require investment in both operating and capital resources.

Trillions of dollars in private sector and national defense funds will be spent on cybersecurity initiatives in the next quarter-century. A small investment of Florida taxpayer funds will help draw those investment dollars to Florida, making for a good state investment, much the same way that this state's economic future was shaped tremendously by the investments locating MacDill AFB, Eglin AFB, NAS Pensacola, NAS Jacksonville, and other major military installations in Florida in the last half-century.

The proposed budget positions Florida as a national leader in the cybersecurity field. Given the high stakes, the fierce competition from other states, and limited state resources, this conservative budget is intended to provide the largest return on investment, brand Florida long-term as the state for cyber business, and make concrete and immediate job gains in the field.

Operating

Recurring operations of the FCC and associated programs will be funded in the following ways:

- (1)** Reinvestment of recurring USF resources resulting from termination and/or suspension of low-demand, non-strategic degree programs. During 2013, USF terminated 17 degree programs and placed a further 10 programs on inactive status. Further terminations/suspensions are expected in 2014. The (re)allocation of faculty and staff resources to cybersecurity-related programs in business, engineering, information technology and the iSchool is expected to amount to approximately \$2.5 million in repurposed resources following multi-year teachout and program closures.
- (2)** As host university, USF will provide institutional operating support for the FCC, including, but not limited to: Auditing and Compliance, Business & Finance, Facility Planning & Design, Human Resources, Information Technology, Legal Services, Patents and Licensing, Payroll, Purchasing, Safety and Security, and Sponsored Programs/IRB. The value of cost-sharing to the FCC is to be determined.
- (3)** A state investment in the Florida Center for Cybersecurity could be most efficiently accomplished in three targeted phases.
 - Phase I: \$7.1 million to establish the FCC at USF, which includes recruiting a nationally-recognized leader and technical support team with the requisite clearance. Attracting world-class talent to Florida (including national and international award winners and members of the National Academy of Sciences and National Academy of Engineering) will be essential for: (a) expanding existing and delivering new online degree, certificate, and professional certification programs, in partnership with Florida businesses to rapidly accelerate workforce development; (b) building a coordinated statewide cybersecurity network; (c) coordinating and capitalizing on university-based talent pool to successfully compete for federal and industry funding for cybersecurity research; and (d) promoting cybersecurity education and consumer protection programs for Floridians and Florida companies through public information and workshops.
 - Phase II: \$5 million to expand and accelerate capacity for education and training of the high-skilled, high-paid cybersecurity workforce through increasing access to affordable degree, certificate, and professional certification programs; extend the seed/matching-grant program for Florida's universities and research entities to yield strategic returns on investment through growing federal and industry R&D expenditures, patents and licensing revenues, startup companies, etc.

■ Phase III: \$4 million to create satellite nodes of the Florida Cybersecurity Network in selected markets—similar to Florida’s Small Business Development Network—in partnership with State University System institutions to ensure that the growing needs of cybersecurity education and training, research, and consulting outreach for Florida companies are met. This investment would also support state-wide initiatives and not-for-profit organizations that will foster cybersecurity initiatives in Florida and expand Florida’s cyber brand across the nation and the world.

(4) Business memberships and contracts associated with corporate access to cybersecurity information, workforce development, consulting, risk assessment and mitigation, business continuity and disaster recovery will reach \$2 million or more annually.

Total USF and corporate contribution to operating funding: \$4.5 million-plus

Total recurring operating funding request from the state: \$16.1 million

Capital

Capital needs will be phased-in over time. The highest and most immediate priority is the construction of a sensitive compartmented information facility, or SCIF, that will support classified/top secret research work for the defense, business and industry sectors. Most importantly, it will provide access for faculty and students, with clearance, from across the state to secure research and training facilities, a prerequisite for competitive federal research funding. The first phase, projected (by Crystal Clear Technologies, Inc., based in St. Petersburg, Florida) at 10,000 GSF and \$10 million, will be essential to assuring Florida’s research competitiveness with other states.

While existing classroom and office space can be re-purposed in the short-term to support significantly increased instructional/learning needs, and while recognizing that a growing portion of the curriculum will be delivered online, the eventual need for secure active learning laboratories/classrooms, auditorium and office space, along with secure data storage, increase the new space needs to approximately 40,000 GSF (including the SCIF) of State University System-shared space at a total cost of \$30.3 million.

Total non-recurring capital funding request from the state: \$30.3 M (phased-in) +PO&M

Much like the Florida Institute of Oceanography, USF will serve as the host institution of the Florida Center for Cybersecurity. The USF Board of Trustees will provide fiscal and management oversight. The specific purpose, bylaws, membership (full, partners, affiliates, associates etc.), goals, performance metrics and operating procedures will be established at the point of creation with input from all FCC partners.

The FCC will be most closely guided by its Higher Education Advisory Council and Community Advisory Board.

Higher Education Advisory Council

The FCC Higher Education Advisory Council includes representatives nominated by each institution of the State University System to help shape the FCC's work plan. The Advisory Council includes representatives of the Independent Colleges and Universities of Florida (ICUF), the Florida College System, and independent research groups in Florida (e.g. Draper, SRI).

| | |
|------------|--|
| Chair | TBD, Executive Director, FCC |
| FAMU | Deidre W. Evans, Associate Professor Computer and Information Sciences |
| FAU | Spyros Magliveras, Professor, Mathematical Sciences |
| FGCU | Robert Totterdale, Professor, Information Systems |
| FIU | Geoff Smith, Associate Professor, Computing and Information Sciences |
| FPU | Rick Maxey, Director, Government Relations |
| FSU | Mike Russo, Director, Information Security and Privacy |
| NCF | Ryan Noble, Chief Information Officer |
| UCF | Ross Hinkle, Vice Provost |
| UF | Elias Eldayrie, Vice President and Chief Information Officer |
| UNF | O. Patrick Kreidl, Associate Professor, Electrical Engineering |
| USF | Randy Borum, Professor, School of Information |
| UWF | Pam Northrup, Associate Vice Provost for Academic Innovation |
| ICUF | TBD |
| FCS | TBD |
| Research | TBD |
| Ex Officio | Sri Sridharan, Managing Director, USF Cybersecurity Initiative |

Minutes of the organization's first meeting are included in Appendix F of this report.

Community Advisory Board

Representing a balance of counsel from senior leadership in business and industry, and the academy, the FCC Community Advisory Board will provide strategic direction for the Center.

| | |
|------------|--|
| Chair | Provost & Executive Vice President, USF (host university), or designee |
| Community | Banking & Finance (Florida) |
| Community | Business/Technology (Florida) |
| Community | Defense (Florida-based) |
| Community | Healthcare (Florida) |
| Community | Transportation & Utilities (Florida) |
| Community | (National) |
| Academic | (Florida) |
| Academic | (National) |
| Academic | (National) |
| Ex-Officio | Executive Director, FCC |

Florida can and should seize the opportunity to become the nation's cyber state. It is an endeavor that will enhance the state's workforce and economy, spur community and business engagement, prepare students and returning veterans for high-demand and high-paying jobs, and attract new companies to Florida.

An investment in the Florida Center for Cybersecurity will produce wide-reaching benefits, both in the short-term and for generations to come.

- ¹ Goldgaber, Arthur, "Cyber Security Industry Report," Goldgaber Research Group, 2013. http://www.staffing360solutions.com/content/staf_wp_cyber.pdf
- ² Bumiller, Elisabeth, and Tom Shanker, "Panetta Warns of Dire Threat if Cyberattack on U.S.," *The New York Times*, October 11, 2102. <http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&r=0>
- ³ "Global Cyber Security Market to Reach \$80.02 Billion by 2017, According to New Report by Global Industry Analysts, Inc.," PRWeb, April 5, 2011. http://www.prweb.com/releases/cyber_security/_application_content_data/prweb8262390.htm
- ⁴ Ellyatt, Holly, "The threat from cybercrime? 'You ain't seen nothing yet,'" *CNBC*, August 13, 2013.
- ⁵ Corrin, Amber, "Tracking the Cost of Cyber Crime," *FCW: The Business of Federal Technology*, July 23, 2013.
- ⁶ *Internet Security Threat Report*, p. 4.
- ⁷ Schwartz, Matthew, "Malware Toolkits Generate Majority of Online Attacks," *SMB Information Week: Technology for Small and Midsize Businesses*, January 19, 2011. <http://www.informationweek.com/smb/security/malware-toolkits-generate-majority-of-on/229000835>
- ⁸ "Northrop Grumman on Cybersecurity," p. 4. www.northropgrumman.com/cybersecurity
- ⁹ "The Comprehensive National Cybersecurity Initiative," National Security Council, The White House (n.d.), p. 1. <http://www.whitehouse.gov/cybersecurity/comprehensive-national-cybersecurity-initiative>
- ¹⁰ "The Comprehensive National Cybersecurity Initiative," p. 4.
- ¹¹ Heckert, Brian, "Defining the Cybersecurity Enhancement Act: Vulnerabilities of IT and Communications Infrastructure," *CIO Digest*, July 2010, p. 7.
- ¹² Strohm, Chris, and Todd Shields, "Obama Boosts Pentagon Cyber Budget Amid Rising Attacks," *Bloomberg Business Week*, April 11, 2013. <http://www.businessweek.com/news/2013-04-10/lockheed-to-general-dynamics-target-shift-to-cyber-spend>
- ¹³ Heckert, p. 8.
- ¹⁴ Vijayan, Jaikumar, "Demand for IT Security Experts Outstrips Supply," *Computerworld*, March 7, 2013. http://www.computerworld.com/s/article/print/9237394/Demand_for_IT_security_experts
- ¹⁵ *Tampa Bay Information Technology Workforce Analysis: Hillsborough & Pinellas Findings*, October 2012. <http://workforcetampa.com/files/public/Tampa%20Bay%20IT%20Workforce%20Analysis/FINALREPORTwithAppendix.pdf>
- ¹⁶ "Hillsborough-Pinellas job Growth rates by Year," *Tampa Bay Information Technology Workforce Analysis: Hillsborough & Pinellas Findings*, October 2012, p. 70.
- ¹⁷ Salary depends on job title: Information Security Analyst/Manager/Officer, Security Consultant, and IT Director.
- ¹⁸ *Veterans Employment: New Insights, Innovations, and Programs That are Making a Difference*. Proceedings of the NAWDP Annual Conference, May 21, 2013. *Monster.com*. <http://www.nawdp.org/Content/NavigationMenu/WorkforceDevelopment/AnnualConference2/VetEmp.pdf>. The *Monster.com* report shows a different figure for nonveteran overall US employment in April 2013 (6.9%) than the BLS's general US figure of 7.5%; regardless, the bottom line is that veterans could use some means of boosting their chances of successfully transitioning to the civilian employment world.
- ¹⁹ *Tampa Bay Information Technology Workforce Analysis: Hillsborough & Pinellas Findings*, October 2012, p. 22. <http://workforcetampa.com/files/public/Tampa%20Bay%20IT%20Workforce%20Analysis/FINALREPORTwithAppendix.pdf>

²⁰ "Points of Pride," USF. <http://www.usf.edu/about-usf/points-of-pride.aspx>

²¹ The eight counties in the TBP are Hillsborough, Pinellas, Manatee, Pasco, Citrus, Hernando, Polk, and Sarasota; the area includes major metropolitan areas of Tampa and St. Petersburg, along with Clearwater, Bradenton, Sarasota, Venice, Winter Haven, and Lakeland.

²² Nielsen 2013 estimates, from Tampa Bay Partnership. <http://www.tampabay.us/demographics.aspx>

²³ "Demographics," Tampa Bay Partnership. <http://www.tampabay.us/demographics.aspx>

²⁴ "Fortune 500." http://money.cnn.com/magazines/fortune/fortune500/2013/full_list/

²⁵ "Florida Cyber Security Program Graduates," in *PhD's Education Index*, "Best Cyber Security Programs in Florida." <http://graduate-school.phds.org/education-index/cyber-security-schools-in-florida>

²⁶ Strategic Plan 2012-2025, State University System of Florida Board of Governors. http://www.flbog.edu/pressroom/_doc/2011-11-28_Strategic_Plan_2012-2025_FINAL.PDF

The 2013 (ISC)2 Global Information Security Workforce Study, Frost & Sullivan. www.frost.com

"Best for Vets: Colleges 2013," Military Times (n.d.)
<http://projects.militarytimes.com/jobs/best-for-vets/2013/colleges/4-year/>

Bureau of Labor Statistics.
http://www.bls.gov/news.release/archives/laus_05172013.pdf.

Bumiller, Elisabeth, and Tom Shanker, "Panetta Warns of Dire Threat if Cyberattack on U.S.," The New York Times, Oct. 11, 2012.
http://www.nytimes.com/2012/10/12/world/panetta-warns-of-dire-threat-of-cyberattack.html?pagewanted=all&_r=0

Caruson, Kiki, Susan MacManus, and Brian McPhee, "Cyber Policy-Making at the Local Governmental Level: An Analysis of Threats, Preparedness, and Bureaucratic Roadblocks to Success," Homeland Security and Emergency Management, 2012 9(2), pp. 1-22.

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

Corrin, Amber, "Tracking the Cost of Cyber Crime," FCW: The Business of Federal Technology, July 23, 2013.

"The Current State of Cybercrime 2013: A Look Inside the Changing Threat Landscape," RSA/EMC2.
<http://www.emc.com/collateral/fraud-report/current-state-cybercrime-2013.pdf>

Cyber Security Jobs Report, Abell Foundation and Cyberpoint International, January 8, 2013.

"Demographics," Tampa Bay Partnership. <http://www.tampabay.us/demographics.aspx>

"Florida Cyber Security Program Graduates," in PhD's Education Index, "Best Cyber Security Programs in Florida."
<http://graduate-school.phds.org/education-index/cyber-security-schools-in-florida>

"Fortune 500." http://money.cnn.com/magazines/fortune/fortune500/2013/full_list/

"Global Cyber Security Market to Reach \$80.02 Billion by 2017, According to New Report by Global Industry Analysts, Inc.," PRWeb, April 5, 2011. http://www.prweb.com/releases/cyber_security/_application_content_data/prweb8262390.htm

"Global Security Market Worth \$120.1 Billion by 2017," MarketsandMarkets, 2013.
<http://www.marketsandmarkets.com/PressReleases/cyber-security.asp>

Heckert, Brian, "Defining the Cybersecurity Enhancement Act: Vulnerabilities of IT and Communications Infrastructure," CIO Digest, July 2010.

Information Security Breaches Survey, Executive Summary, PricewaterhouseCoopers, April 2012.
http://www.pwc.co.uk/en_UK/uk/assets/pdf/olpapp/uk-information-security-breaches-survey-executive-summary.pdf

Internet Security Threat Report, Symantec Corporation, 2013.
http://www.symantec.com/security_response/publications/threatreport.jsp

"MacDill Air Force Base, located in Tampa By the Numbers," MacDill Air Force Base, located in Tampa Air Force Base.
<http://www.MacDillAirForceBase.af.mil/questions/topic.asp?id=570>

Melendez, Barbara, "Globalization Focus of Diversity Summit," USF News, May 5, 2011,
<http://news.usf.edu/article/templates/?a=3400>

Mile2. <http://mile2.com/>

"National & Competitive Intelligence—USF College of Business," USF. <http://business.usf.edu/programs/intelligence-analysis/>

"Centers of Academic Excellence Institutions," National Security Agency, Feb. 2013.
http://www.nsa.gov/ia/academic_outreach/nat_cae/institutions.shtml

"Northrop Grumman on Cybersecurity," www.northropgrumman.com/cybersecurity

"Points of Pride," USF. <http://www.usf.edu/about-usf/points-of-pride.aspx>

Progress Report 2010-2012, USF World, University of South Florida.
http://global.usf.edu/wordpress/wp-content/uploads/USF-World-Progress-Report_FINAL_May-13-2013.pdf

"The Risk vs. Cost of Enterprise DDoS Protection," Arbor Networks, 2012.
<http://www.arbornetworks.com/index.php?lang=en>

Schwartz, Matthew, "Malware Toolkits Generate Majority of Online Attacks," SMB Information Week: Technology for Small and Midsize Businesses, January 19, 2011.
<http://www.informationweek.com/smb/security/malware-toolkits-generate-majority-of-on/229000835>

Strategic Plan 2012-2025, State University System of Florida Board of Governors.
http://www.flbog.edu/pressroom/_doc/2011-11-28_Strategic_Plan_2012-2025_FINAL.PDF

Tampa Bay Information Technology Workforce Analysis: Hillsborough & Pinellas Findings, October 2012.
<http://workforcetampa.com/files/public/Tampa%20Bay%20IT%20Workforce%20Analysis/FINALREPORTwithAppendix.pdf>

Tampa Bay Partnership. <http://www.tampabay.us/ demographics.aspx>

Tampa Bay Technology Forum. <http://www.tbtf.org/?page=Veterans>

Veterans Employment: New Insights, Innovations, and Programs That are Making a Difference. Proceedings of the NAWDP Annual Conference, May 21, 2013. Monster.com.
<http://www.nawdp.org/Content/NavigationMenu?WorkforceDevelopment/AnnualConference2/VetEmp.pdf>

"Veterans Reintegration and Resilience," USF Research & Innovation. <http://www.research.usf.edu/vri/>

"Veterans Services," USF. <http://www.veterans.usf.edu/>

Vijayan, Jaikumar, "Demand for IT Security Experts Outstrips Supply," Computerworld, March 7, 2013.
http://www.computerworld.com/s/article/print/9237394/Demand_for_IT_security_experts

"What is INTO?" <http://www.intohigher.com/us/en-us/what-is-into.aspx>

Appendix Table of Contents

| | |
|--|----|
| APPENDIX | 23 |
| Appendix A: Curriculum plan | 24 |
| Appendix B: Workforce output projections..... | 27 |
| Appendix C: Existing cybersecurity education programs..... | 30 |
| Appendix D: Common definitions in cybersecurity | 36 |
| Appendix E: Selected faculty biographies | 40 |
| Appendix F: Higher Education Advisory Council Meeting Minutes..... | 52 |
| Appendix G: Support for the Florida Center for Cybersecurity..... | 56 |

Appendix A: Curriculum plan

The interdisciplinary master's degree and certificate programs offer four degree concentrations: Cyber Fundamentals (CF), Cyber Intelligence (CI), Cybercrime (CC), and Information Assurance (IA). The 30-credit program for the master's degree includes four core courses required for all concentrations, plus individualized courses per concentration:

Core courses

CNT 5004 Data Communications /Network

This course describes the components of IT infrastructures and their interactions. Specific topics include Physical layer & data link layer/ Ethernet, Network layer/ IP & Transport layer/ TCP, Application layer & support services, Routing & subnetting, WAN technologies, Wireless & phone networks, and Network security and managerial issues. The exchange of information between computer applications is called Business Data Communications (DataComm). Datacomm technologies provide the underlying plumbing that enables computer applications to access resources on remote computers. The primary goal of this course is to answer the question "How does the IT infrastructure work?" A big part of it is, "How do computers talk to each other?"

Specific topics include:

Physical layer & data link layer/ Ethernet
Network layer/ IP & Transport layer/ TCP
Application layer & support services
Routing & subnetting
WAN technologies
Wireless & phone networks
Network security & managerial issues

CIS 5362 Cryptography

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

For this class, the syllabus is likely to be built around the following content (based on the TOC in the Schneier Cryptography Engineering book):
Cryptography context (design criteria, generic attacks)

- Block ciphers
- Hash functions
- Message authentication codes
- Secure channel
- Key negotiation
- Prime numbers
- Diffie-Hellman
- RSA
- Key negotiation
- Key management (Kerberos)
- PKI
- Storing secrets

ISM 6328 Basics of Information Security and Risk Management

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

A good class combines teaching a trade and thinking about the trade. This class has an approximately 40-60 balance between skills acquisition and conceptual understanding.

Specifically, the course objectives are to:

- introduce the importance of information security and related business concerns
- make students aware of the major categories of information security threats
- make students aware of the common information security controls

- enable students to implement the basic information security controls
- introduce students to the important legal provisions regarding information security
- make students aware of the methodological implications for information security arising from these legal provisions
- provide students with an understanding of the standard methodologies for complying with legal requirements for IT general controls
- provide a basic understanding of IT risk management in organizations

ISM 6930 Decision Processes for Business Continuity and Disaster Recovery

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

Course contents will include:

- NIST incident handling process
- Incident response team
- Communication management with stakeholders during incidents
- Compliance with legal requirements

CF concentration

EEL 6764 Computer Architecture

CIS 6930 (special topics) Computer Networks, Fundamental principles and analysis

CIS 6930 (special topics) Security & Privacy

CI concentration

LIS 5937 Visual Information Analytics

ENC 6261 Analytic Communication

CCJ 6074 Advanced Intelligence Analytic Methods

INR 5365 Core Concepts in Intelligence

DSC 6600 Cyber intelligence

LIS 6758 Information Strategy & Decision Making

CC concentration

CJE 6688 Cybercrime and Criminal Justice

CJE 6623 Digital Evidence Recognition

CJE 6624 Introduction to Digital Evidence

CJE 6625 Network Forensic Criminal

CJE 6626 Digital Forensic Criminal Investigations

IA concentration

ISM 6145 Seminar on Software Testing

ISM 6125 Software Architecture

ISM 6124 Advanced Systems Analysis and Design

ISM 6316 Project Management

ISM 6218 Advanced Database Administration

The FCC will draw from several of USF's colleges and centers, as well as area experts:

Arts and Sciences

Relational Communication
Organizational Communication
Economics
Geosciences
Psychology
iSchool

Behavioral and Community Sciences

Communication Sciences and Disorders
Criminology
Louis de la Parte Florida Mental Health Inst.

Business

Information Systems / Decision Sciences
National and Competitive Intelligence

Education

Educational Leadership and Policy Studies
Educational Measurement and Research
Psychological and Social Foundations

Engineering

Chemical and Biomedical Engineering
Civil and Environmental Engineering
Computer Science and Engineering
Industrial and Management Systems
Information Technology

Global Sustainability

Public Health

Environmental and Occupational Health
Epidemiology and Biostatistics
Global Health
Health Policy and Management

Office of Research and Innovation

Center for Urban Transportation

Appendix B: Workforce output projections

USF's projected addition to workforce development in cybersecurity, based upon full funding, includes increasing the number of new professional cybersecurity certifications to be awarded annually (550, each with earning potentials of approximately \$100,000) by USF Innovative Education through online and face-to-face courses, beginning in spring of 2014.

■ Increasing the number of new professional cybersecurity certifications to be awarded annually (550, each with earning potentials of approximately \$100,000) by USF Innovative Education through online and face-to-face courses, beginning in spring of 2014:

- +100 Certified Information Systems Security Professional (CISSP)
- +50 Systems Security Certification Practitioner (SSCP)
- +50 Certified Authorization Professional (CAP)
- +50 Certified Secure Software Lifecycle Professional (CSSLP)
- +50 Information Systems Security Architecture Professional (CISSP-ISSAP)
- +50 Information Systems Security Engineering Professional (CISSP-ISSEP)
- +50 Information Systems Security Management Professional (CISSP-ISSMP)
- +50 CompTIA Security
- +50 CompTIA Offering – CASP
- +50 Cisco Certified Network Associate (CCNA) Security

■ Increasing the number of new academic certificates/concentrations to be delivered online and face-to-face and to be awarded by USF annually in cybersecurity-related fields, beginning in 2014-15:

- +475 undergraduate certificates/concentrations
- +270 graduate certificates/concentrations

USF's proposed new certificate programs:

Computer Security, Cyberbehavior, Cyberbullying, Cybercrime, Cybersecurity, Cybersecurity Compliance and Risk Management, Cybersecurity in Counseling & Higher Education, Electronic Medical Records Security, Encryption & Information Security, Information Assurance for Healthcare, Information Assurance for Financial Services, Information Assurance for Energy & Utilities, Medical Device Security.

■ Increasing the number of projected additional degrees to be awarded by USF (by 2017-18) in cybersecurity-related fields over the number of degrees awarded in 2011-12:

- +867 baccalaureate degrees
- +215 graduate degrees
- +50 doctoral degrees

Appendix B: Workforce Output Projections

USF Interdisciplinary

Master of Science degree in *Cybersecurity* (a new, state-of-the-art program to be implemented in fall of 2014)

| | | | |
|--------------------|----------|----------------|-------------|
| Master's (online): | CIP Code | 2014-15 (proj) | 2017-18 |
| | 43.0303 | 120 | 300 (+100%) |

New :

Graduate Certificate in *Cybersecurity* with concentrations in *Cyber Fundamentals*, *Cyber Intelligence*, *Cybercrime* and *Information Assurance*:

50 annually

College of Engineering

(accredited by ABET)

Computer Science & Engineering, Engineering Management, Industrial & Manufacturing Engineering, and Information Technology.

| | | | |
|----------------|---|---------|------------|
| Baccalaureate: | CIP Codes | 2011-12 | 2017-18 |
| | 11.0101/11.1013/11.0401/14.0901/ 14.3501 | 292 | 336 (+15%) |
| Master's: | CIP Codes | 2011-12 | 2017-18 |
| | 11.0501/14.0901/14.3501/14.0501/ 13.3502 | 155 | 194 (+25%) |
| Doctoral: | CIP Codes | 2011-12 | 2017-18 |
| | 14.0901/14.3051/14.0501 | 16 | 24 (+50%) |

New:

Baccalaureate Certificate/Concentration in *Computer Security*:

50 annually

Graduate Certificate/Concentration in *Computer Security*:

25 annually

College of Business

(accredited by AACSB)

Accounting, Business Economics, Entrepreneurship in Applied Technologies, Finance, Management Information Systems, Management, and Marketing.

| | | | |
|----------------|---|---------|--------------|
| Baccalaureate: | CIP Codes | 2011-12 | 2017-18 |
| | 52.0101/52.0201/52.0301/52.0601/ 52.0801/52.1201/52.1401 | 1,787 | 2,055 (+15%) |
| Master's: | CIP Codes | 2011-12 | 2017-18 |
| | 52.0101/52.0201/52.0301/52.0701/ 52.0801/52.1201/52.1401 | 339 | 424 (+25%) |
| Doctoral: | CIP Codes | 2011-12 | 2017-18 |
| | 52.0201 | 6 | 12 (+100%) |

New:

Baccalaureate Certificate/Concentrations in *Information Assurance for Healthcare*; *Information Assurance for Financial Services*; and *Information Assurance for Energy & Utilities* :

150 annually

Graduate Certificate/Concentration in *Cybersecurity Compliance and Risk Management*:

50 annually

Appendix B: Workforce Output Projections

USF Health

Bioinformatics, Biotechnology, Health Informatics, and Medical Technology.

| | | | |
|----------------|-------------------------------|---------|------------|
| Baccalaureate: | CIP Codes | 2011-12 | 2017-18 |
| | 51.1005 | 10 | 50 (+400%) |
| Master's: | CIP Codes | 2011-12 | 2017-18 |
| | 51.2706 (new)/26.1103/26.1201 | 17 | 51 (+200%) |

New:

| | |
|--|-------------|
| Graduate Certificate in <i>Medical Device Security</i> : | 10 annually |
| Graduate Certificate in <i>Electronic Medical Records Security</i> : | 10 annually |

College of Arts & Sciences

Library/Information Studies (Cyberintelligence, Strategic Intelligence, Visual Analytics & Communication), Health Information Technology, Mathematics, and Psychology.

| | | | |
|----------------|---------------------------------------|---------|--------------|
| Baccalaureate: | CIP Codes | 2011-12 | 2017-18 |
| | 27.0101/42.0101/11.0103 (new) | 1,125 | 1,294 (+15%) |
| Master's: | CIP Codes | 2011-12 | 2017-18 |
| | 25.0101/27.0101/42.0101/11.0403 (new) | 146 | 183 (+25%) |
| Doctoral: | CIP Codes | 2011-12 | 2017-18 |
| | 27.0101/42.0101 | 23 | 46 (+100%) |

New:

| | |
|--|--------------|
| Baccalaureate Certificate/Concentration in <i>Cyberbehavior</i> (Industrial & Organizational Psychology): | 100 annually |
| Baccalaureate Certificate/Concentration in <i>Encryption and Information Security</i> (Mathematics & Statistics) | 50 annually |
| Graduate Certificate/Concentration in <i>Cyberbehavior</i> (Industrial & Organizational Psychology): | 25 annually |
| Graduate Certificate/Concentration in <i>Encryption and Information Security</i> (Mathematics & Statistics) | 25 annually |

College of Behavioral & Community Sciences

Criminology, and Criminal Justice Administration.

| | | | |
|----------------|-----------------|---------|------------|
| Baccalaureate: | CIP Codes | 2011-12 | 2017-18 |
| | 45.0401 | 461 | 507 (+10%) |
| Master's: | CIP Codes | 2011-12 | 2017-18 |
| | 45.0401/43.0103 | 40 | 60 (+50%) |
| Doctoral: | CIP Codes | 2011-12 | 2017-18 |
| | 45.0401 | 5 | 10 (+100%) |

New:

| | |
|--|--------------|
| Baccalaureate Certificate/Concentration in <i>Cybercrime</i> : | 100 annually |
| Graduate Certificate/Concentration in <i>Cybercrime</i> : | 25 annually |

College of Education

(Accredited by NCATE)

New:

| | |
|---|-------------|
| Baccalaureate Certificate/Concentration in <i>Cyberbullying</i> : | 25 annually |
| Graduate Certificate/Concentration in <i>Cyberbullying</i> : | 25 annually |
| Graduate Certificate/Concentration in <i>Cybersecurity in</i> | |

Appendix C: Existing Cybersecurity Education Efforts

Existing Cybersecurity Education Efforts: Florida Universities

| School | Bachelor's | Master's | CS Center/Institute |
|----------------------------------|--|--|--|
| Embry Riddle University | Cyber Intelligence and Security, Software Engineering with Cybersecurity Emphasis, Bachelor of Science in Technical Management Information Security, | - | Department of Global Security and Intelligence Studies (Daytona, FL) |
| Florida Atlantic University | - | Information Technology & Management | Center for Cryptology and Information Security |
| Florida Institute of Technology | - | Information Technology--Cybersecurity | - |
| Florida International University | - | Management Information Systems, Information Technology, Telecommunications and Networking, Computer Science | - |
| Florida State University | - | Computer Criminology, Computer Network and System Administration, Computer Science | Center for Security & Assurance in Information Technology |
| Keiser University | Cyber Forensics/Information Security | Information Security | - |
| Nova Southeastern University | Computer Information Systems, Computer Science, Information Technology | Information Security, Computer Information Systems, Computer Science, Information Technology, Management Information Systems | Secure and Robust Distributed Systems Laboratory |
| Rasmussen College | Cyber Security | - | - |
| University of Central Florida | - | Digital Forensics | - |
| University of Florida | Computer Science/Engineering | Computer Science/Engineering | - |

Appendix C: Existing Cybersecurity Education Efforts

| Research Areas | Scholarships/Grants | Certifications/Minors | NSA Designation | Corporate/Governmental Partnerships |
|---|--|--|-----------------|--|
| Emphasis is placed on effective communications, quantitative skills, global awareness, social responsibility, ethical and legal grounding, information technology, critical thinking skills, teamwork, computer and network functional skills, broad cyber industry familiarity, and a commitment to lifelong learning. | - | Security and Intelligence Minor, The Security and Intelligence Certificate of Completion, Undergraduate Certificate in Information Assurance | - | FAA, NASA, NIKSUN, IEEE |
| Cryptology, Cyber Crime, Quantum and Post-quantum Cryptology, Secure Systems, Social Perspectives of Information Security | Funding provided by the National Security Agency and the Department of Homeland Security | Information Security Minor and Certificate (offered in the College of Business) | CAE/R | National Security Agency, Department of Homeland Security |
| Computer and information security, cryptography, application and operating system security | - | Graduate Certificate in Information Assurance and Cybersecurity (online) | - | - |
| Cybersecurity test technology program, developing technology to prevent cyberattacks | DoD recently provided funding for cyberspace research | - | - | Department of Defense's Test Resource Management Center |
| Secure Software, Locking, Intrusion Detection Systems, Honeynets, Computer Forensics, RFID, Securing Cyber-Physical Systems, Security and Privacy in Database and Data Management, Network Security | Scholarship funding offered to graduate students through the National Science Foundation and the Department of Homeland Security | NSTISSI-4011, National Training Standard for Information Systems Security (INFOSEC) Professionals, and CNSSI-4014, Information Assurance Training Standard for Information Systems Security Officers (ISSO) | CAE/IAE, CAE/R | National Security Agency, Department of Homeland Security, National Science Foundation |
| - | - | - | - | - |
| Information assurance research, support of security, reliability, availability, and performance of computer and information systems in distributed environments, study of enterprise, grid, wireless, ad-hoc and ubiquitous systems | - | Information Assurance/Security Minor, Graduate Certificate in Information Security Management, Graduate Certificate in Information System Security | CAE/IAE | National Security Agency, Department of Homeland Security |
| - | - | CompTIA® A+ Essentials, CompTIA® A+ Practical Application, CompTIA® Linux+, Powered by LPI, CompTIA® Network+, CompTIA® Security+, Microsoft® Exchange Server, Microsoft® Windows Workstation, Windows® Applications Development with Microsoft® .NET Framework, Windows® Server Active Directory, Windows® Server Network Infrastructure, CIW® Javascript Specialist, Interconnecting Cisco® Networking Devices | - | - |
| - | - | Graduate Certificate in Computer Forensics | - | - |
| - | - | - | - | - |

Appendix C: Existing Cybersecurity Education Efforts

Existing Cybersecurity Education Efforts: National Universities

| School | Bachelor's | Master's | CS Center/Institute |
|---|--|--|---|
| Carnegie Mellon University (They have a four-pronged Cybersecurity Strategic Initiative focusing on Research, Outreach, Speakers, and Partnership. Education offered through their CyLab) | - | Information Security Technology and Management, Information Technology, Information Networking, Information Technology-Privacy Engineering, Information Security Policy and Management, Information Technology and Information Security, Executive Masters in Information Assurance, Information Technology and Mobility, Information Technology and Software Management | CyLab, Software Engineering Institute, CERT Program (workshops and training focused on improving network security, responding to and analyzing security incidents, and creating and managing computer security incident response teams) |
| Embry Riddle University | Cyber Intelligence and Security, Software Engineering with Cybersecurity Emphasis, Bachelor of Science in Technical Management Information Security, | - | Department of Global Security and Intelligence Studies (Daytona, FL) |
| George Mason University | Information Technology with concentration in Information Security and Network Administration | Information Security, Information Security and Assurance, Computer Engineering with concentration in Network and Systems Security, Management of Secure Information Systems | Center for Secure Information Systems |
| George Washington University | Computer Science | Cybersecurity, Computer Science, Professional Studies in Security and Safety Leadership (with a focus in Strategic Cybersecurity Enforcement), Cybersecurity in Computer Science, Executive MBA in Cybersecurity, Master of Laws in National Security Law | Cyber Security Policy and Research Institute |
| Iowa State University | Computer Engineering with specialization in Information Assurance | Information Assurance, Engineering in Information Assurance | Information Assurance Center, Power Infrastructure Cybersecurity Laboratory |
| Massachusetts Institute of Technology | Electrical Engineering and Computer Science | Electrical Engineering and Computer Science | Lincoln Laboratory |
| Mississippi State University | Computer Science, Software Engineering, Computer Engineering | Computer Science | Center for Computer Security and Research |

Appendix C: Existing Cybersecurity Education Efforts

| Research Areas | Scholarships/Grants | Certifications/Minors | NSA Designation | Corporate/Governmental Partnerships |
|---|---|--|-----------------|--|
| Trustworthy computing platforms and devices, next-generation secure and available networks, mobility, security of cyber-physical systems, secure home computing, survivable distributed systems and outsourced services, privacy protection, threat analysis and modeling, software security, cryptography, usable privacy and security, threat prediction and response, business risk analysis and economic implications | Scholarship funding offered to graduate students through the National Science Foundation and the Department of Homeland Security. US Department of Defense funds the Software Engineering Institute and the CERT Program. | - | CAE/IAE, CAE/R | Raytheon, Honeywell, Facebook, General Motors, Lockheed Martin, Northrop Grumman, InterDigital, Alcatel-Lucent, Core Security Technologies |
| Emphasis is placed on effective communications, quantitative skills, global awareness, social responsibility, ethical and legal grounding, information technology, critical thinking skills, teamwork, computer and network functional skills, broad cyber industry familiarity, and a commitment to lifelong learning. | - | Security and Intelligence Minor, The Security and Intelligence Certificate of Completion, Undergraduate Certificate in Information Assurance | - | FAA, NASA, NIKSUN, IEEE |
| Network attack modeling, analysis, and visualization, virtualization for security, protection against malicious code, cyber situational awareness, secure composable systems, privacy in location-based applications, automated intrusion recovery, secure data centers | Information Assurance Scholarship Program funded by the US Department of Defense | Applied Cyber Security Graduate Certificates | CAE/IAE, CAE/R | NSA, National Science Foundation, Air Force Research Laboratory, Air Force Office of Scientific Research, National Institute of Standards and Technology, DCS Corp, Intelligence Advanced Research Projects Activity |
| Computer network security and information assurance, computer system and network privacy, electronic commerce security, security mechanisms related to intellectual property, e-government security, internet regulatory issues, computer ethics and social impact of technology, information assurance and computer security education and workforce development | Scholarships and grants are funded by the Defense Department, the Department of Homeland Security, and the National Science Foundation (administered over \$8 million in grants since 2002) | Computer Security and Information Assurance Graduate Certificate | CAE/IAE, CAE/R | National Security Agency, Department of Homeland Security, Department of Defense, National Science Foundation |
| Forensics, intrusion detection, network modeling, wireless communications, information/cyber warfare, artificial intelligence and data mining, foreign policy, identity theft, cryptography. Cyber-physical systems framework for risk modeling and mitigation of cyber-attacks on the power grid that accounts for dynamics of the physical system, as well as the operational aspects of the cyber-based control network. | National Science Foundation funds Iowa State's Scholarship for Service program | Graduate Certificate in Information Assurance | CAE/IAE, CAE/R | National Security Agency, National Science Foundation |
| Development of prototype components and systems for computer network security | Federally funded (it is a Department of Defense Research and Development Laboratory) | Short Programs Professional Education on Applied Cyber Security, Short Programs Professional Education on Cryptography and Computer Security | - | Maryland Cybersecurity Center, Department of Defense |
| Artificial Intelligence, Computer Crime and Forensics, Cryptography and Information Security | Scholarships funded through the Department of Defense and the National Science Foundation | Information Assurance Professional Certificate (INFOSEC Professional) | CAE/IAE, CAE/R | National Science Foundation, Army Research Laboratory, Cisco, Dexisive Inc |

Appendix C: Existing Cybersecurity Education Efforts

| School | Bachelor's | Master's | CS Center/Institute |
|---|---|---|--|
| Pennsylvania State University | Security and Risk Analysis-Information and Cyber Security (online) | Information Sciences and Technology | Penn State Cyber Security Lab |
| Syracuse University | - | Cybersecurity Law and Policy Course | Institute for National Security and Counterterrorism |
| University of Maryland-College Park | Computer Science with a Cybersecurity specialization | Computer Science/Electrical and Computer Engineering, Engineering in Cybersecurity | Maryland Cybersecurity Center |
| University of Maryland-University College | Cybersecurity, Computer Networks and Security | Cybersecurity, Cybersecurity Policy, Digital Forensics and Cyber Investigation, Information Technology and Information Assurance | - |
| University of Southern California | - | Computer Science with Specialization in Computer Security, Cyber Security | Center for Computer Systems Security |
| University of Texas-San Antonio | Infrastructure Assurance, Computer Science with Computer and Information Security concentration | Information Technology (also available with Information Assurance Concentration), MBA Information Assurance concentration, MBA Information Systems concentration, Computer Science with Computer and Information Security concentration | Center for Infrastructure Assurance and Security (which offers cyber security events, training classes, exercises, and competitions), Institute for Cyber Security (conducts basic and applied research in partnership with academia, government and industry), Center for Education and Research in Information and Infrastructure Security (conducts high impact research in information assurance and security and educates the cybersecurity workforce needed now and in the future. The center's research objective is to offer leading edge solutions that will help to solve cybersecurity problems of national scope and importance) |
| University of Washington | - | Cybersecurity and Leadership (Online), Cyber Security Engineering, Information Management, Information Assurance | Center for Information Assurance and Cybersecurity |

Appendix C: Existing Cybersecurity Education Efforts

| Research Areas | Scholarships/Grants | Certifications/Minors | NSA Designation | Corporate/Governmental Partnerships |
|---|--|--|-----------------|--|
| Malware analysis, systems security in cloud computing, holistic security of smartphone systems, secure lean software, self-protecting data centers, computer-aided human centric cyber situation awareness, resilient and self-healing software systems and networks, malware and software security, wireless network security, understanding and assuring information privacy; identity management, access control, trust computing, enterprise “health care” models, on-the-fly “surgery” techniques, cyber security situational awareness information security economics, policies and security management, and social implications of security. | Professors have been awarded grants by the National Science Foundation to continue their research | Post-baccalaureate Certificate in Information Systems Security (online) | CAE/IAE, CAE/R | National Security Agency, National Science Foundation, Cisco, HP, Department of Homeland Security, Air Force Research Laboratory, Department of Defense |
| Law, National Security & Counterterrorism, Security Governance, New Frontiers in Science, Cyber, & Technology, Homeland Security | - | Certificate of Advanced Studies in Systems Assurance, Certificate of Advanced Studies in Security Studies | CAE/IAE, CAE/R | US Department of Homeland Security, Department of Defense, Booz Allen Hamilton, RAND Corporation, Dyn-Corp International, National Science Foundation |
| Wireless and network security, secure software, cyber supply chain security, privacy in social networks, cybersecurity policy, cryptography, attacker behavioral analysis, health care IT, multimedia forensics, the economics of cybersecurity | Grants funded by the National Science Foundation | Graduate Certificate in Engineering in Cybersecurity, Graduate Certificate in Professional Studies in Cybersecurity Leadership | CAE/R | Booz Allen Hamilton, Northrop Grumman, Sourcefire, Lockheed Martin, SAIC, Lincoln Laboratory, Google |
| - | UMUC hosts an annual gala to raise funds for Cybersecurity student scholarships. Attendants include a broad range of industry leaders and members of the Maryland Commission on Cybersecurity Innovation and Excellence. | Cybersecurity Policy, Cybersecurity Technology, Foundations of Cybersecurity, Homeland Security Management, Information Assurance, Minor in Cybersecurity | CAE/IAE | NSA, Department of Homeland Security, Booz Allen Hamilton, AT&T, Cisco, Dell, Northrop Grumman, Microsoft, Lockheed Martin, Google, SAIC, & more. |
| Technologies supporting confidentiality, integrity, resiliency, privacy, intrusion detection and response, and survivability of critical infrastructure | - | Minor in Applied Computer Security, Specialization in Cyber Security, Specialization in Digital Forensics | CAE/R | US Department of Homeland Security, National Security Agency |
| Digital forensics, information security management and strategy, applied network and information systems security, and the economics and psychology of information security, botnet analysis and defense, trustworthy cloud computing, secure information sharing, social computing security, infrastructure assurance, assured data provenance, privacy policies and enforcement. | The ICS was established through a grant provided by the Texas Emerging Technology Fund. Research is also funded by the NSF and the Department of Homeland Security. | Minor in Digital Forensics, Minor in Infrastructure Assurance and Forensics | CAE/IAE | National Security Agency, National Science Foundation, Department of Homeland Security, Texas Emerging Technology Fund, Cisco, The University of Texas System, Symantec, Dell, BAE Systems |
| Wireless network infrastructure, Internet security, and commercial/industrial applications, systems engineering in information assurance, developing strategies to recruit, hire and retain cybersecurity employees, next generation honeypots | Part of the Scholarship for Service funded by the National Science Foundation | Information Systems Security Certificate, Information Security and Risk Management Certificate, Network Engineering Certificate, Digital Forensics Certificate | CAE/IAE, CAE/R | Microsoft, Boeing, Accuvant, Department of Homeland Security, NSA |

Appendix C: Existing cybersecurity education efforts

Appendix D: Common Definitions in Cybersecurity

Account Harvesting – collecting or “harvesting” of all the authentic account names on a system

Accessibility – the degree to which a computer or information system is available

Advanced Windows Security – system Administration practices that ensure security of Windows operating systems, including permissions, networking, file sharing, and more

Anonymous – a loosely affiliated collective of “hacktivists,” typically motivated socially and politically, who engage in cyberattacks against corporate and government targets through web site disruptions and defacements, often resulting in the theft and release of sensitive or secured documents or personal information

Application – software that performs programmed functions for a user. Applications can support word processing, spreadsheet development, graphic creation, presentation creation and database tasks

Backbone – the backbone is the “skeleton” of the Internet; it is a high-speed fiber optic network of main lines that interconnect around the world at various places or Network Access Points (NAPs)

Backdoor – a backdoor can be created by the exploitation of a vulnerability, such as a programming error or malware, and allows access into a device without proper authentication

Bandwidth – the capacity of a communication channel to pass data during a certain period of time

Biometrics – access controlled by physical characteristics

Bit – the smallest unit measure of information storage, a term derived from “binary digit”

Black Hat (Hacker) – A hacker with malicious intent who accesses computer networks without proper authority, legally or otherwise; slang for computer criminal

Blacklisting – blocking of harmful websites, often done by parents or employees with the aid of software programs that block with specified or selected criteria

Blended Threat – combined cyberattack methods that are used to increase damage during a computer network attack

Botnet – a controlled network of a large number of computers infected with Trojan horse viruses by cybercriminals often used to implement a denial of service attack

Botmaster(s) – a person or group of people in control of a botnet and whose location is usually difficult to determine

Browser – used to view online content, a browser is a software program that can retrieve and display information and

store cookies

Buffer Overflow – overloading of a temporary data storage area so data overflows into adjacent buffers and corrupts them

BYOD (Bring Your Own Device) – acronym used to describe a policy that allows personal mobile devices within range of a wireless network, usually a corporate or private network, and that allows those users access

Cache – high-speed storage mechanism for memory or disks; pronounced “cash”

Cryptography – science and practice of securing with algorithms, particularly for third-party communications

Ciphertext – encrypted form of a message being transferred

Client – a machine that uses and requests service from another system machine such as a “server”

Computer Emergency Response Team (CERT) – organization that provides incident response services to cyberattack victims and provides information about known vulnerabilities and threats as well as ways to stay safe online

Confidentiality – ensuring that information or data on a system is not accessed by unauthorized users

Cookie – data exchanged between an HTTP server and browser that is then stored on a client for later server retrieval

Denial of Service (DoS) – prevention of authorized access or halting of system operations or system functions

Digital Forensics – branch of forensic science including the recovery and investigation of digital media, often legal evidence, found in digital devices and digital records

Distributed denial of service (DDoS) – multiple systems, such as a botnet, for which operation and system functions have been halted

Domain Hijacking – an attacker blocks access to the DNS server and replaces information to gain access and take over that domain

Domain Name System (DNS) – the way domain names on the Internet are translated into Internet Protocol addresses; the named form of an Internet address

Doxing – an urban term used to describe searching for personally identifiable information by using online documents

Firewall – a software or hardware component that prevents unauthorized access to or modification of a system

Flooding – providing more information than a system can handle to ultimately cause failure of that system

Grey Hat (Hacker) – hacker operating without malicious intent but is prepared to operate against legal or ethical boundaries

Hacking – accessing computer networks, legally or otherwise; heavily modify the software or hardware of one's own computer system; slang for computer crime

Hackivism – hacking in the name of social or political protest or to facilitate change for a cause

Hardening – identifying and fixing system vulnerabilities

Honey Pot – a “trap” to detect and thwart a potential cyberattack on a system before exploitation occurs

Identity Management – practices involving the management of identification of individuals and verifying data to grant access with proper permissions

Integrity – assuring that information is accurate and complete

Internet Protocol – method used to send data from one computer to another over the Internet

Intrusion Detection System (IDS) – security management system that gathers and analyzes information on computers or on a network

MAC Address – numerical address that identifies each network device

Malware – software containing malicious code that is usually intended to gain unauthorized access to a computer or system

Man-in-the-Browser – Trojan horse that intercepts and manipulates electronic information over a supposedly secure link

Man-in-the-Middle Attack – similar to the Man-in-the-Browser, but the hacker creates a diversion on the legitimate page that enables him/her to make changes in real time to the information entered by the unsuspecting user

Mobile and Wireless Security – system administration practices that ensure security of mobile and wireless devices, including the cloud, WLAN, and WIFI, and includes encryption methods, authentication, access permissions, and protection

Open source – free licensing and distribution of certain software and applications to promote universal access

Password Cracking – attempt to guess passwords, sometimes with the aid of a cracking program

Password Sniffing – passive wiretapping to gain access to a password on a network

Patch – software update by a vendor intended to fix a known vulnerability

Penetration Testing and Vulnerability Assessment – testing of the external perimeter of a network to determine

cyberattacks that could be caused by threats and the exploitation of vulnerabilities

Phishing – attempt to trick an e-mail recipient into disclosing sensitive information by posing as a trusted source

Root – the name of the administrator account on a Linux system

Session Hijacking (Sidejacking) – taking over or duplicating an established session

Sniffing – another name for passive wiretapping

Social Engineering – using social techniques, such as lying, blackmailing or impersonating, to trick another person with the ultimate goal of gaining otherwise unauthorized access to an information system

Spoofing –pretending to be an authorized user to gain access to a system

Steganography –hiding a message or data within a file or program

Threat – potential for violation of security, often by exploitation of a vulnerability

Trojan horse – non-self-replicating malware that gains privileged access to the operating system then exploits the computer and allows unauthorized access to the target computer through a backdoor – all while appearing to perform a non-malicious function

Virus – a hidden, self-replicating program usually containing malicious code that cannot run by itself

Vulnerability – part of a system, device, computer, or network that could be exploited by a threat to execute a cyberattack

White Hat (Hacker) – penetration tester responsible for the security of a system

Worm – a program containing malicious code that can replicate over a network and run by itself

Zombie – a compromised computer that will be later used, unbeknown to the owner, to execute an attack

Appendix E: Selected faculty biographies

College of Business



Manish Agrawal, Ph. D.

Associate Professor

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

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



Walter Andrusyszyn

Adjunct Professor

Research Interests: Law and diplomacy, intelligence analysis

Walter Andrusyszyn, an adjunct professor, teaches international business courses at the undergraduate level in the College of Business. Andrusyszyn, who began teaching at the University of South Florida in 2007, has an extensive background in both business and government. Temporarily returning to government in 2009, he served as the deputy permanent representative to the North Atlantic Treaty Organization or NATO and shared responsibility in preparing U.S. President Barack Obama's first visit to Europe. He has also served on the White House's National Security Council and held various positions with the Department of State. Andrusyszyn has private sector experience as a manager for a large American company that began operations in Europe in 2003.



Kaushal Chari, MBA, Ph. D.

Associate Dean and Professor

Professor Kaushal Chari serves as chair of the Information Systems & Decision Sciences Department of the College of Business. He currently teaches a course in distributed systems and participates in numerous university committees and research efforts. Chari's research program covers three broad areas: software engineering, business intelligence and distributed systems. He is interested in applying quantitative as well as intelligent techniques to address problems related to IT systems, software development and business process management. Chari's work has been published in a variety of academic journals, including Management Science, Information Systems Research, INFORMS Journal on Computing, and IEEE Transactions on Software Engineering. Chari served as the associate editor of MIS for Interfaces journal from 2002-2010, and as the vice chair of the INFORMS

Appendix E: Selected faculty biographies

Information Systems Society from 2007 – 2009.



Michael Fountain, MBA, Ph. D.

Director

Michael Fountain holds three faculty appointments at USF, serving as the John & Beverley Grant Endowed Chair in Entrepreneurship, a professor in the College of Engineering, and a professor in the Department of Psychiatry & Behavioral Medicine. He currently serves as founding director of USF's Center for Entrepreneurship and the director for university-wide interdisciplinary entrepreneurship educational programs. Fountain is an expert in creating, financing, and growing biotechnological, medical device, and life science companies. He has founded or cofounded seven new ventures (three later publicly traded companies) and patented and commercialized numerous innovative medical and diagnostic products (including sustained release anti-cancer drugs, genetically engineered diagnostic products for autoimmune diseases, microencapsulated dermatologic products and

vaccine products for prevention of human and animal infectious disease). He was a pioneer in the development and application of the use of phospholipids in micro- and nano-particle technologies for drug encapsulation. Fountain has been instrumental in the development and deploying of entrepreneurial programs on an international level. He has served as an Entrepreneur-in-Residence with the Ewing Marion Kauffman Foundation overseeing strategy, venture capital and private equity, and life sciences entrepreneurship.



Balaji Padmanabhan, Ph. D.

Chair, Information Systems Decision Sciences

Associate Professor

Balaji Padmanabhan is the Anderson Professor of Global Management and an associate professor in the Information Systems Decision Sciences Department. He has created and taught undergraduate, MBA/MS, and doctoral courses in areas related to business/data analytics, computational thinking, and electronic commerce. Padmanabhan's research addresses data analytics for business applications, algorithms for online news recommender systems, management of data analytics in firms, fraud detection in healthcare, analytics in examining service quality and customer churn, behavioral profiling, and pattern discovery. His work has been published in both computer science and information systems journals and conferences including Management Science, Information Systems

Research, MIS Quarterly, and INFORMS Journal on Computing. Padmanabhan's professional service includes work as associate editor and program committee member of several academic journals and conferences. He has published his research in leading outlets in business and computer science. He also works with several firms on technical, strategic and educational issues related to business and data analytics.

College of Engineering



David Armitage

Former Director, Division of Information Technology, College of Engineering, Lakeland, FL

David Armitage is the former Director, Division of Information Technology, College of Engineering, Lakeland, FL, where he was responsible for overall coordination of activities of division, including course scheduling, credentialing faculty for courses, faculty evaluation and program development. Responsible for coordinating the integration of the unit and its academic programs, current and proposed, into the College of Engineering. His research interests include the use of technology and advanced pedagogies to improve computing knowledge transfer to undergraduates, experimental application of electroencephalography to computing education, and

Appendix E: Selected faculty biographies



Robotics applications.

José L. Zayas-Castro, MBA, Ph. D.

Professor and Associate Dean for Research

Dr. José L. Zayas-Castro is Professor and Associate Dean for Research, College of Engineering at the University of South Florida (USF) in Tampa. For nine and half years he was Chairperson of the Department of Industrial & Management Systems Engineering at the USF. Dr. Zayas-Castro has a B.S. in IE from UPRM and M.S. in Management & Industrial Engineering, MBA, and Ph.D. from Rensselaer Polytechnic Institute. His interests relate to statistical process control, applied modeling, systems integration, business and R & D strategy, innovation and entrepreneurship, cost analysis, technology transfer, assessment, healthcare systems and healthcare delivery, and innovation in engineering education. Dr. Zayas-Castro recent research has emphasized the re- design of processes and products, re-engineering the service sector, particularly healthcare, and the integration of research and engineering education. Examples are: reengineering and modeling healthcare operational systems in healthcare systems, e.g., hospitals and clinics, healthcare decision making in outpatient and inpatient processes, re-engineering of Graduate Medical Education, decision tools for the classification and diagnostic of prostate cancer, product and process developments in medical devices and bio-medical businesses, and the extension and adaptation of the Learning Factory using small scale technology. Dr. Zayas-Castro participates in various advisory and review committees in the National Science Foundation, and has been associated to more than \$9 million in external funding. Dr. Zayas-Castro has more than 40 publications and over 60 presentations.



Lawrence Hall, Ph. D.

Professor and Department Chair

Research Interests: Distributed machine learning, data mining, pattern recognition and integrating AI into image processing, fuzzy logic in pattern recognition, AI and learning

Lawrence Hall is a Professor and Chair of Computer Science and Engineering at University of South Florida. He received his Ph.D. in Computer Science from the Florida State University in 1986 and a B.S. in Applied Mathematics from the Florida Institute of Technology in 1980. He has received funding from the National Science Foundation. He co-edited the 2001 Joint North American Fuzzy Information Processing Society (NAFIPS), IFSA conference proceedings. He was the co-program chair of NAFIPS 2004. He received the IEEE SMC Society Outstanding Contribution Award in 2000. He received an Outstanding Research Achievement Award from the University of South Florida in 2004 and is a past president of NAFIPS. He is currently the president-elect of the SMC Society and the editor-in-chief of the IEEE Transactions on Systems, Man and Cybernetics, Part B. Also, he is associate editor for IEEE Transactions on Fuzzy Systems, International Journal of Intelligent Data Analysis, and International Journal of Approximate Reasoning, and is a Fellow of IEEE.

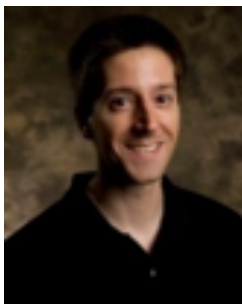


Rangachar Kasturi, Ph. D.

Douglas W. Hood Professor

Research Interests: Computer Vision, Pattern Recognition, Biometrics, Video Information Processing
Dr. Kasturi is the Douglas W. Hood Professor of Computer Science and Engineering at the University of South Florida. He received his Ph.D. degree from Texas Tech University in 1982. He was a Professor of Computer Science and Engineering and Electrical Engineering at the Pennsylvania State University during 1982-2003. Dr. Kasturi served as the President of the International Association for Pattern Recognition (IAPR) during 2002-04 and as the President of the IEEE Computer Society during 2008. He is a Fellow of the IEEE and a Fellow of IAPR. He was a Fulbright scholar during 1999.

Appendix E: Selected faculty biographies



Jay Ligatti, Ph. D.

Associate Professor

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

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

College of Arts and Sciences



Jim Andrews, Ph. D.

Director

Research Interests: Interdisciplinary health informatics

Jim Andrews is the Director of the University of South Florida, School of Information, as well as Interim Director of the School of Mass Communications. He works with the faculty from both schools to develop new synergies that will lead to innovative research and education in a dynamic and shifting media and information landscape. His research falls broadly within the interdisciplinary field of health informatics. Specifically, he has interests in clinical research informatics, as well as health-related information behaviors, particularly in the context of cancer genetics. He works collaboratively with researchers from USF Health, within SI and SMC, and also across the county and internationally.



Randy Borum, Ph. D.

Professor

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

Dr. Randy Borum is a Professor and Coordinator of Strategy and Information Analysis in the School of Information at the University of South Florida. He holds a joint appointment to the College of Public Health and has previously served on the faculty of the College of Behavioral and Community Sciences. He regularly teaches and consults with law enforcement agencies, the Intelligence Community, and DoD, and has authored/ co-authored more than 140 professional publications. Dr. Borum has been an instructor with the BJA State & Local Anti-Terrorism Training (SLATT) Program since 1999, and worked as a Senior Consultant to the U.S. Secret Service for more than

a decade helping to develop, refine and study behavior-based protocols for threat assessment and protective intelligence. He has previously served as a sworn police officer, Forensic Coordinator for a regional state psychiatric facility, and as full-time faculty at He has taught at the FBI Academy, FLETC, JFK Special Warfare Center and School (Ft. Bragg); Joint Special Operations University; CIA; and the US Army Intelligence Center and School (Ft. Huachuca). He was Principal Investigator on the "Psychology of Terrorism" initiative for an agency in the US Intelligence Community. He serves as an advisor to the FBI's Behavioral Analysis Unit-1 (Threat Assessment & National Security), the National Center for the Analysis of Violent Crime (NCAVC), the FLETC Behavioral Science Division, and is listed on the United Nations' Roster of Experts in Terrorism. Dr. Borum is a Past-President of the American Academy of Forensic Psychology, and currently serves as Senior Editor of the Journal of Strategic Security, and on the editorial boards of the American Intelligence Journal; Behavioral Sciences & the Law and Red Team Journal (online).

Appendix E: Selected faculty biographies



Chuck Connor, Ph. D.

Associate Dean for Research and Professor

Research Interests: Volcanic risk models, high resolution magnetic survey techniques and mapping

In volcanology, Connor's research has focused on development of volcanic hazard and risk models. Research involves high resolution magnetic surveys and techniques, inversion of magnetic data. Recent geophysics projects have been in Armenia, Nicaragua, the western US, and Japan. To support this research Connor has various geophysical instruments (TEM, slingram EM, Cs-vapor magnetometer, differential GPS, carbon dioxide flux meter), data loggers, and a beowulf cluster for parallel programming involved in heavy lifting numerical problems and stochastic simulations. Funding comes from the US National Science Foundation, the US Geological Survey, and WorldBank.



Eric Eisenberg, Ph. D.

Professor and Dean

Research Interests: Organizational and health communication, strategic uses of communication

Eisenberg leads the largest college at USF, home to 24 academic departments, 22 centers and institutes, more than 15,000 students, 600 faculty and 180 staff. Eisenberg is a nationally recognized scholar in the strategic use of communication to promote positive organizational change. He has published extensively in national and international scholarly journals and is a widely sought-after consultant. Eisenberg was appointed to a five-year term as dean of the USF College of Arts and Sciences in March 2010. As interim dean from 2008-2010, he guided the college through a complex process of restructuring that led to the establishment of the School of Humanities, School of Social Sciences, and School of Natural Sciences and Mathematics, as well as steering the efforts to integrate new academic units into the college. He supported the recruitment of outstanding new faculty from the United States and abroad, strengthened the college's leadership and cultivated a greater sense of scholarly community across the college.



David Jacobson, Ph. D.

Professor

Research Interests: Immigration and citizenship, human rights, women's status in global conflict, sustainability

Jacobson's research focuses on areas related to immigration and citizenship, international institutions and law, human rights, and women's status in global conflict. His work concerns sustainability in two areas: the sustainability of communities in the context of social change and the implications of climate change for human institutions.

Appendix E: Selected faculty biographies



Michael Brannick, Ph.D.

Professor, Psychology

Research Interests: Industrial and organizational psychology

Michael Brannick is a professor and former chair of the department of Psychology. He received his Ph.D. from Bowling Green State University in 1986. His research interests include Industrial and organizational psychology, Research Methods and Statistics, and Team Performance (effectiveness and measurement). He teaches undergraduate as well as graduate level courses. His undergraduate courses include: Industrial psychology, applied psychology, Fairness in selecting employees, research methods, and tests and measures. His graduate courses include: Correlation & regression, Decision making, Job analysis, Meta-analysis, Psychometrics, Teams & teamwork, and Univariate statistics (ANOVA & Regression). He is a Member of the American Psychological Association, the American Psychological Society, and the Society for Research Synthesis Methodology, as well as a fellow of the Society for Industrial and Organizational Psychology.



Toru Shimizu, Ph.D.

Chair and Professor, Psychology

Research Interests: Visual information processing, comparative neuroscience, cognitive neuroscience

Shimizu received his M.S. and Ph. D. degrees in psychology from the University of Maryland and was a post-doctoral neuroscientist at the University of California, San Diego. He has been a visiting professor at Keio University in Japan and helped to facilitate a collaborative research agreement between the psychology departments of Keio and USF. Shimizu's research is focused on visual information processing, animal cognition, comparative neuroscience, and evolution of the brain. He leads the Comparative Cognition and Neuroscience laboratory at USF. Shimizu teaches Comparative Psychology, Psychology of Learning, Physiological Psychology, Methods in Neurosciences, and Neuroscience Seminar.



Paul Spector, Ph.D.

Area Director, Industrial/Organizational Program

Paul E. Spector is a distinguished university professor of industrial/organizational (I/O) psychology and I/O doctoral program director at the University of South Florida. He is also director of the NIOSH funded Sunshine Education and Research Center's Occupational Health Psychology program. He is the Associate Editor for Point/Counterpoint for Journal of Organizational Behavior, and Associate Editor for Work & Stress, and is on the editorial board of Journal of Applied Psychology. His research is in the areas of occupational stress and workplace violence. Spector received his Ph.D. in Industrial/Organizational Psychology at the University of South Florida in 1975. He is interested in how organizational factors, work-nonwork interface, and personal characteristics interact to affect employee health, safety, and well-being. All of this fits into the newly emerging interdisciplinary field of occupational health psychology. He studies counterproductive work behavior, interpersonal conflict, job attitudes, job stress, work-family conflict, and workplace violence. He also studies how personality affects each of these areas.



Stephen Stark, Ph.D.

Associate Professor and Graduate Program Director

Research Interests: Psychometrics, computer adaptive testing, multivariate statistics

Dr. Stark's research focuses on the development and application of psychometric methods to practical problems in industrial organizational and educational settings. He has worked with university faculty and practitioners to develop and improve tests measuring constructs, such as job performance, personality, and cognitive ability. He has published papers on computer adaptive testing, differential item and test functioning (measurement bias), and issues related to faking in personality assessment. He teaches psychometrics, multivariate statistics, industrial organizational psychology, and introduction to social psychology.

Office of Research and Innovation



Sudeep Sarkar, Ph. D.

Associate Vice President for Research and Innovation
Professor, Computer Science and Engineering

Research Interests: Perceptual organization using pattern theory, cloud computing, image analysis

Sarkar received the B.Tech. degree in Electrical Engineering from the Indian Institute of Technology, Kanpur, in 1988. He received the M.S. and Ph.D. degrees in Electrical Engineering, on a University Presidential Fellowship, from The Ohio State University, Columbus, in 1990 and 1993, respectively. He has co-authored one book and co-edited another book on perceptual organization. He is the recipient of the National Science Foundation CAREER award in 1994, the USF Teaching Incentive Program Award for Undergraduate Teaching Excellence in 1997, the Outstanding Undergraduate Teaching Award in 1998, and the Theodore and Venette Askounes-Ashford Distinguished Scholar Award in 2004. He served on the editorial boards for the IEEE Transactions on Pattern Analysis and Machine Intelligence (1999-2003) and Pattern Analysis and Applications Journal during (2000-2001). He is currently serving on the editorial board of the Pattern Recognition Journal and the IEEE Transactions on Systems, Man, and Cybernetics.



Paul R. Sanberg, Ph.D., D.Sc.

Senior Vice President for Research & Innovation
President, USF Research Foundation
Distinguished University Professor

Research Interests: Technology and innovation, cell therapeutics for degenerative diseases

Sanberg is a member of the Board of Scientific Counselors for the National Institute of Drug Abuse at the National Institutes of Health, and has served on numerous scientific advisory boards for health-related foundations and companies. He has significant industry experience with biotech companies involved in cell therapy for degenerative disorders and biopharmaceutical development. He is the Editor-in-chief of Technology and Innovation, and serves on editorial boards for more than 30 scientific journals. Dr. Sanberg is the President of the National Academy of Inventors and has also served as president of a number of professional societies including the American Society for Neural Transplantation and Repair, the Cell Transplant Society, and the International Behavioral Neuroscience Society. He is the author of more than 600 scientific articles, including thirteen books, with over 20,000 scientific citations (Google scholar). As an inventor on approximately 100 health-related U.S. and foreign patents, his early work was pioneering in understanding why brain cells die in neurological disorders and in drug abuse research. Sanberg's work has been instrumental in translating new pharmaceutical and cellular therapeutics to clinical trials for Tourette syndrome, depression, stroke, Huntington's disease and Parkinson's disease. He is a Fellow of the AAAS, a Charter Fellow of the National Academy of Inventors, and serves on the evaluation committee of the National Medal of Technology and Innovation.



Lt. General Martin Steele

Director of Office of Military Partnerships
Associate Vice President for Veterans Research

Lieutenant General Martin R. Steele, US Marine Corps (retired), is the associate vice president for veterans research. General Steele, who joined USF in 2009, has been executive director of Military Partnerships and co-chair of USF's Veterans Reintegration & Resilience Initiative, a major goal of which is the formation of a nationally recognized research center aimed at the rehabilitation and successful reintegration of veterans. General Steele enlisted in the Marine Corps in 1965 and rose from private to three-star general with a tenure as the longest serving chief operating officer in the history of the Marine Corps. He culminated his military career as the deputy chief of staff for plans, policies, and operations at Headquarters, US Marine Corps in Washington, DC. Upon his retirement from

Appendix E: Selected faculty biographies

active duty, General Steele served as president and CEO of the Intrepid Sea-Air-Space Museum, the largest naval museum in the world. A decorated combat veteran with over 34 years of service, he is a recognized expert in the integration of all elements of national power (diplomatic, economic, informational, and military) with strategic military war plans and has served as an executive strategic planner/policy director in multiple theaters across Asia. His extraordinary career was chronicled as one of three principals in the award winning military biography *Boys of '67* by Charles Jones. As founder and chairman of Steele Partners, Inc., a strategic advisory and leadership consulting company, General Steele has led a philanthropic transition program assisting exiting Marines into private sector jobs throughout the country, at no cost to the Marine participants, the Marine Corps or to the companies that provide employment opportunities. He serves on several boards across the country, including Fisher House Foundation, Veterans Advantage, and the Marine Corps Scholarship Foundation. General Steele holds a bachelor's degree in history from the University of Arkansas, where he was recognized as a distinguished graduate of the Fulbright College of Arts and Sciences, and master's degrees from Central Michigan University, Salve Regina College, and the Naval War College.

College of Behavioral and Community Sciences



Max Bromley, Ed. D.

Associate Professor

Research Interests: Law enforcement accreditation standards

Dr. Bromley is Associate Professor Emeritus in the Department of Criminology and Director of the Master of Arts in Criminal Justice Administration Program (designed specifically for criminal justice practitioners) at the University of South Florida. Prior to becoming a fulltime faculty member he served as the Associate Director of Public Safety at USF and worked in the criminal justice field for almost 25 years. He served on the statewide task force that established the first set of law enforcement accreditation standards for Florida. Dr. Bromley was also the Chairperson for USF's taskforce on campus security following the terrorist attack on September 11th. Bromley co-authored the textbook *Crime and Justice in America*, 6th edition. He also co-edited *Hospital and College Security Liability* and was

the senior co-author of *College Crime Prevention and Personal Safety Awareness*. In addition, he has written dozens of scholarly articles, book chapters and technical documents on a variety of campus crimes and campus policing issues. Dr. Bromley assisted the U.S. Bureau of Justice statistics in developing and implementing the first national survey of campus law enforcement agencies. More recently Dr. Bromley has also been involved in research on community policing. His articles have appeared in *Policing*, *Police Quarterly*, *Criminal Justice Policy Review*, and *Journal of Contemporary Criminal Justice*. Dr. Bromley also wrote *Department Self-Study: A Guide for Campus Law Enforcement Administrators*, which is used at over 1,000 institutions of higher education.



Charles Dion, MA

Director, Policy and Services Research Data Center

Research Interests: Statistical analysis of large administrative databases

Charles Dion, M.A. is the Director of the Policy and Services Research Data Center (PSRDC) in the Department of Mental Health Law and Policy at the Louis de la Parte Florida Mental Health Institute (FMHI), University of South Florida. He received both his Bachelor's and Master's degrees from the University of South Florida in Mathematics. His Master's degree has a concentration in Statistics. Following the completion of his Master's degree he went to work for Florida Medical Quality Assurance, Inc. (FMQAI), the Florida Medicare Quality Improvement Organization as a Data Analyst where he worked for fourteen years developing expertise in data mining and the statistical analysis of large administrative data bases, primarily Medicare claims data, and steadily increasing his level of responsibility. The positions he held were Data Analyst, Statistician, Lead Statistician, Director of Analytic Services, and Chief Analytic Officer.

Appendix E: Selected faculty biographies



LeGrande Gardner , Ph. D.

Instructor

Research Interests: Criminal intelligence, computer and digital media crime, digital forensics, antiterrorism, surveillance and counter-surveillance

LeGrande Gardner, Ph.D. is an Instructor in Criminology at the University of South Florida. He earned his doctorate in sociology with a criminology specialization from Virginia Polytechnic Institute and State University (1984). He received his B.S. (1979) and M.A. (1981) from Georgia Southern University. Prior to becoming a full time faculty member he served as a sworn law enforcement officer for over 25 years with experience in both federal and local agencies, including an appointment as a Special Agent with the Federal Bureau of Investigation (FBI). Dr. Gardner's law enforcement career included 17 years in managerial, administrative, and supervisory assignments to include criminal intelligence, computer crime and crimes involving digital media, Digital Forensics Laboratory, computer forensics, anti-terrorism, Homeland Security, organized crime, criminal gang interdiction and suppression, and surveillance and counter-surveillance operations. Additional experiences as a police supervisor included patrol operations, specialized street-level tactical operations, career criminals, surveillance operations, and an assignment on the Special Weapons And Tactics (S.W.A.T.) Team. In his last three years of active duty he was concurrently assigned as a Task Force Agent to the FBI's Cyber Crimes Unit. Dr. Gardner has over 28 years experience as an adjunct instructor and police trainer for numerous law enforcement agencies, government organizations, colleges and universities, and private contractors. In addition to his academic credentials, he received certification by the State of Florida Criminal Justice and Standards Training Commission as a police instructor, firearms instructor, defensive tactics instructor, and police/emergency vehicle driving instructor. He regularly taught in the regional police academy and served as an Instructor for police in-service training programs. Dr. Gardner's teaching interest and specialization is in the areas of cyber-crimes, technology-related crimes, digital forensics, and e-discovery. As an extension of his prior background in criminal intelligence investigations, his research interest is in the area of subcultural deviance and criminal behavior, more specifically 1%er bikers and organized criminal hacking groups.



Michael J. Leiber, Ph. D.

Professor and Chair

Research Interests: Racial and ethnic issues in criminology

Michael J. Leiber, Ph.D., is a Professor in Criminology at the University of South Florida. He earned his doctorate in criminal justice from the State University of New York at Albany. His main research interests and publications lie in juvenile delinquency, juvenile justice, and race/ethnicity. Over the last twenty years, he has also worked with the Office of Juvenile Justice & Delinquency Prevention (OJJDP) as a consultant dealing with the overrepresentation of minority youth in the juvenile justice system. In 2008, he received the W.E.B. Du Bois award for significant contributions to the field of racial and ethnic issues in criminology from the Western Society of Criminology.



Paul Stiles, J.D., Ph.D.

Associate Professor and Associate Chair

Paul G. Stiles, J.D., Ph.D., is an Associate Professor and Associate Chair in the Department of Mental Health Law & Policy at the Louis de la Parte Florida Mental Health Institute, University of South Florida (USF). He received his Ph.D. in Clinical Psychology from Hahnemann University and J.D. in Law from Villanova University Law School. Dr. Stiles' clinical experience includes providing psychological and neuropsychological services in both private and public psychiatric facilities as well as nursing homes. In addition to a substantive focus on geriatric mental health services and policy, his research has involved the compilation, integration, analysis and dissemination of relatively large administrative data sets (e.g. Medicaid/Medicare eligibility and claims files, national hospital surveys, state mental health service regulatory databases) and the application of findings to public mental health systems and the mental health of older persons. Dr. Stiles has also focused on research integrity and ethics and was principal investigator for an NIMH-funded project examining whether enhancements made to the form and process of information disclosure during informed consent procedures improve comprehension and understanding of the disclosures by mentally ill persons. Most recently he is involved in examining the impact of actual and perceived coercion on prisoners in research. He teaches courses on legal and ethical issues in aging, provides intensive workshops on research ethics, and formerly chaired the social-behavioral IRB for USF (which he still serves on) and currently chairs the USF Conflict of Interest Committee. Dr. Stiles was also the principal investigator on two NIH grants to develop and conduct an intense course on research ethics as well as a series of instructional modules on the ethical conduct of research. Finally, he currently is PI on an NIMH grant to implement an intense summer program to train undergraduates in research processes/ethics as well as facilitator for the MHLP post-doctoral fellowship program.

Appendix E: Selected faculty biographies



Julianne Serovich, Ph.D.

Dean and Professor

Research Interests: Disclosure of HIV status, treatment for homeless youths

Serovich's research focuses on the relationship between HIV disclosure to family, friends, and sex partners and the effects of sharing such information both on reducing HIV transmission and building social support structures for those coping with the illness. She is the principal investigator (PI) of the Kiss & Tell Project for Men and the Kiss & Tell Project for Women as well as other major studies that have resulted in more than 60 book chapters and peer reviewed publications. Her work began more than two decades ago at Texas Tech University, where, after receiving her doctorate from the University of Georgia, she was named an assistant professor of marriage and family therapy in 1991. Also a graduate of Loyola College, Baltimore, she joined the OSU faculty in 1995 and was named the inaugural director of the CFT program. Since 1997, she has received grant funding in excess of \$9 million, mostly from the National Institutes of Mental Health (NIMH).

Office of Information Technology



Alex Campoe, B.S.

Director of Information Security

Research Interests: Identity and access management, IT audits, risk management, security policies

Alex Campoe is USF's director of Information Security. He is a CISSP-certified Security professional with more than 15 years of experience dealing with a broad range of issues involving data security, from policy and governance, to detailed data forensics. Campoe's professional experience includes responsibilities for Identity and Access Management, IT audits, Risk Management, writing and implementation of security policies and awareness program. His technical hands on experience includes working with UNIX administration (Solaris, Linux), MySQL, PHP, Perl and

data forensics tools. Alex earned a BS in Electrical Engineering from the University of Texas at Arlington.



Michael Pearce, CIO

Vice President, Information Technology

Michael Pearce currently serves as the System Vice President, CIO for the University of South Florida System. Until recently, Mike served as the Chief Information Officer for Suffolk University in Boston Massachusetts. Prior to that he served as the Deputy Chief Information Officer for the University of Southern California, located in Los Angeles, and headed the technical component of the Information Services Division for the University. He has held numerous other managerial positions in Accounting, Finance, and Information Systems for a variety of organizations ranging in size from small venture capital start-up firms to large multi-billion dollar conglomerates. In previous roles, Mike has held both technical and administrative roles of increasing responsibility such as the Vice President of Information Technology for Bausch & Lomb, Vice President and Chief Information Officer for Chiron Vision, and as Corporate Controller of Beckman Instruments. During his 25 year history, Mike has led a number of global projects, system implementations, and reengineering initiatives for a variety of companies. He spearheaded the worldwide-shared services initiatives that resulted in a Shared Service Data Center in Geneva, Switzerland, and Fullerton, California. Mike currently holds a master's degree in Finance and a bachelor's degree in accounting with significant experience in Information Systems Management. He serves on numerous customer, industry, and technology advisory boards throughout the nation.

College of Education



Ilene R. Berson, Ph. D., NCSP

Professor

Ilene R. Berson, Ph.D., NCSP is a Professor of Early Childhood in the Department of Childhood Education and Literacy Studies at the University of South Florida. She also serves as the coordinator of the USF Early Childhood doctoral program with an emphasis on social justice and child advocacy. Dr. Berson has extensive experience working with children ages birth to eight, and she is a nationally certified and state licensed school psychologist. Her research focuses on prevention and intervention services for young children at imminent risk for behavioral and mental health challenges associated with child maltreatment and other traumatic events. She leads collaborative reform initiatives, forging linkages between early childhood, child welfare, and health care systems, as well as international studies on the engagement of young children with digital technologies. Dr. Berson has extensively published books, chapters, and journal articles and has presented her research worldwide.

She has been the principal investigator on funded grants totaling over \$2.5 million. Dr. Berson embodies the characteristics of an engaged scholar who works closely in reciprocal relationships with practitioners and policymakers to develop innovative solutions for emerging and long term issues to promote young children's well being.



Dr. Michael J. Berson

Professor

Research Interests: Integration of technology into education

Dr. Michael J. Berson is a Professor of Social Science Education at the University of South Florida and a Senior Fellow in The Florida Joint Center for Citizenship. Within the USF College of Education, he has served as founding director of the iteach technology and teacher education program. Dr. Berson instructs courses in Social Science Methodology, receiving international recognition for integrating emerging technologies into instruction and modeling dynamic and fluid pedagogy. He has received the USF Outstanding Undergraduate Teaching Award and was twice chosen as the USF nominee for the United States Professor of the Year Program sponsored by CASE and The Carnegie Foundation for the Advancement of Teaching. He also was honored with the National Council for the Social Studies President's Award for outstanding contribution to the field and was selected for the Florida

Council for the Social Studies International Relations Award for his research in global child advocacy. Dr. Berson has served as an advisor on the integration of technology into education to numerous companies and organizations. He was elected Chair of the College and University Faculty Assembly of the National Council for the Social Studies, Vice President of the Society for Information Technology & Teacher Education, a Member of the Board of Directors for the Social Science Education Consortium, and a Member of the Advisory Board for the International Society for the Social Studies. Dr. Berson has extensively published books, chapters, and journal articles and presented his research worldwide. He was named the Association of Educational Publishers Distinguished Achievement Award Winner in the Learned Article category. He has been the principal investigator, co-principal investigator, or primary partner on funded grants totaling over \$6 million. Dr. Berson conducts research in the areas of global child advocacy and technology in social studies education.

Center for Urban Transportation Research



Jason Bittner, MPA

Director

Research Interests: Freight and intermodal transportation, infrastructure asset management

Jason Bittner was appointed in January 2012 as the 3rd Director of the Center for Urban Transportation Research (CUTR) at the University of South Florida. Mr. Bittner previously was Deputy Director of the National Center for Freight and Infrastructure Research and Education (CFIRE) at the University of Wisconsin–Madison. He had served as Principal Investigator or Co-Principal Investigator on over \$1.8 million in sponsored research in maintenance quality assurance, freight transportation and mobility concerns since 2008 and has published numerous articles

Appendix E: Selected faculty biographies

in the Transportation Research Record and other journals. He helped establish the Mid-America Freight Coalition, a ten-state partnership advancing freight planning and operations in the Midwest region and has over 14 years of experience working with multistate coalitions and regional entities on transportation topics. Mr. Bittner is a member of the TRB Committee on Transportation Asset Management and co-chair of the TRB Committee on Conduct of Research. He is also a member of the Executive Committee for the American Society for Public Administration, Section on Transportation Policy Analysis. Previous to his work at CFIRE, Mr. Bittner was an Assistant Municipal Manager in Ohio, where he was responsible for public works and economic development. He also interned on the staff of US Senator Howard Metzenbaum. Bittner taught Political Science at Edgewood College and held a Lecturer's appointment in Transportation Management and Policy at the University of Wisconsin. He holds a Master's degree from the La Follette School of Public Affairs at the University of Wisconsin and a Bachelor's degree in Political Science and Public Administration from the American University in Washington, D.C.

Operations and additional research



Michael Hill

Colonel, 92nd Mission Support Group Commander at Fairchild Air Force Base

Colonel Michael S. Hill is the 92nd Mission Support Group Commander at Fairchild Air Force Base, Washington. He leads the installation and mission support activities including security, civil engineering, force support contracting, communications, and logistics readiness. Additionally, he is responsible to support the 92nd Air Refueling Wing's Air Expeditionary Force contribution through personnel and equipment readiness. A native of Illinois, Colonel Hill received his Bachelor of Science degree in Computer Science from Northern Illinois University. He received his commission from the Air Force Reserve Officer Training Corps program at the Illinois Institute of Technology in Chicago. He has served as Director of Communications (J6), Joint Special Operations Task Force Two, C4 Requirements Manager, Executive officer, Aide-de-Camp to the AFSOC Commander, and as a Presidential Communications Officer at the White House Communications Agency. He also served as Commander of the 42nd Communications Squadron, Chief, Intelligence Systems Branch, Directorate of Intelligence, Headquarters Air Combat Command, and as the Commander, 1st Joint Communications Squadron, Joint Communications Support Element (JCSE) a joint airborne communications unit that provided communications support for Operations IRAQI and ENDURING FREEDOM.



John W. Long

Senior Vice President and Chief Operating Officer,
University of South Florida

John W. Long is a veteran U.S. Air Force officer who most recently ran the day-to-day support activities at Andrews Air Force Base, including flight line infrastructure support for Air Force One. Long is a University of South Florida alumnus with a bachelor's of arts in business management. The COO role focuses on human capital/resources, services and infrastructure, safety and security, and business operations that impact a cross section of faculty and employees.



John Burger

Chief, Cyber Security; Colonel, USCENTCOM

Colonel John Burger is the chief of Cyber Division at U.S. CENTCOM

Colonel John Burger is Chief of the Joint Cyber Center at United States Central Command responsible for the planning, integration and execution of cyberspace operations in the USCENTCOM AOR. He leads a staff of 115 military, civilians and contractors to assure the CDRs freedom of maneuver in cyberspace and deny the same to our adversaries. He designs and implements information assurance programs to secure cyber key terrain, and develops defensive cyberspace plans to "see, block, and maneuver" defensive forces against threats to friendly networks. Working with our Allies and Partners, he develops Cyber Security Cooperation plans to enable our partners to protect themselves in cyberspace. He integrates cyberspace force application with the air, land, and maritime domains in support of OPLANs. Interacts daily with the Joint Staff, USCYBERCOM, the Intelligence Community, and the Interagency. Principle advisor to the CENTCOM CDR on all cyberspace matters.

Higher Education Advisory Council

Establishing the Florida Center for Cybersecurity

Meeting Minutes

November 7, 2013 (3:30 to 4:30 p.m.)
Conference Call

Participants:

Spyros Magliveras – Florida Atlantic University,
Ross Hinkle – University of Central Florida
Rick Maxey – Florida Polytechnic
Ryan Noble – New College of Florida
Pam Northrup – University of West Florida

Rob Totterdale – Florida Gulf Coast University
Mike Russo – Florida State University
Diedre Evans – Florida A&M University
Ralph Wilcox – University of South Florida
Moez Limayem – University of South Florida
Sri Sridharan – University of South Florida

1. Introduction/Announcement

Ralph Wilcox (Provost of the Host University): Highlighted the Legislature's Proviso language and the action plan to deliver a report authored by the Board of Governor's (BOG) that should result in the establishment of the Florida Center for Cybersecurity (FCC).

The proviso states that the FCC should:

- Foster job growth
- Focus on educating K-12 and university students
- Enhance the current capabilities of the workforce
- Position Florida as a leading state in Cybersecurity
- Work with businesses in FL to promote Cybersecurity
- Perform applied research associated with educational needs
- And more.....

At this point, participants were asked to identify needs and challenges associated with creating a collaborative effort in successfully establishing the FCC

2. Discussion on needs and challenges

Ryan Noble

- Leveraging a collaborative effort would benefit the college to enable students to become workforce ready in Cybersecurity and be competitive in the job market

- While the college educates employees about the need and importance of Cybersecurity, it is equally important to educate those in K-12 as well

Spyros Magliveras

- Established a CAE in IA in 2003 (NSA recognition)
- Focus on cryptography, IS, Healthcare compliance & Security policies
- *Question:* How will universities collaborate?
- *Moez Limayem's response:* See the center as an entity to leverage the synergy of different Florida institutions to train students and tackle research projects for securing grants. If the funding from legislature is secured, then seed money will be given to the center for these collaborative efforts
- *Ralph Wilcox added:* The center will leverage the amazing breadth of expertise across the state; collaboration across departments will be interdisciplinary, and this collaboration will extend across universities in all of Florida.

Ross Hinkle

- University of Central Florida has a broad, global perspective when it comes to Cybersecurity, focusing on energy, food, and supply chain security in their program
- Would like to see: boundaries around Cybersecurity more clearly defined
- UCF has programs in Digital Forensics, which are also broad and culturally global

Rob Totterdale

- Established a class in security “early on”
- Teaching and extending the CS program in Forensics
- Excited to leverage the FCC opportunity and collaborate

Diedre Evans

- CAE in IA – with 100 to 150 students; with certifications from the NSA and Department of Homeland Security
- Educating high school and middle school teachers about the importance of Cybersecurity
- Impact on workforce

Pam Northrup (Karen speaking)

- How will the center match workforce needs with student needs?
- Need to tune student skills to make them “workforce ready”
- Define the boundaries of Cybersecurity as noted by Ross Hinkle above

Rick Maxey

- Excited about collaboration

- Currently teaching students on this subject
- Currently working closely with Cybersecurity industries
- Working closely with faculty involved with industry-driven research

Mike Russo

- The CSO and CPO for Florida State University; 11 years prior, was the state CIO
- Unemployment rate in Cybersecurity professions is zero; in DC, the unemployment rate in Cybersecurity professions is -7%
- Running a program for K-12 and state colleges
- What does Cybersecurity look like? Strategy must be aligned with laws
- The program needs a model that is different, with functional areas translated into a curriculum
- How will the center meet SANS security controls?
- Florida is behind nationally in Cybersecurity
- *Sri Sridharan's response:* There is more demand than supply in Florida. The center will be located in close proximity to McDill Air Force Base and will therefore, leverage relationship with CENTCOM and SOCOM.

3. Other thoughts/ Closing Remarks/ Summarization

Rob Totterdale

- We need a skills (capabilities) inventory for what exists across Florida
- Collaborate by having a central repository for input and information

Spyros Magliveras

- Suggested possible face to face meeting at USF soon to better understand these issues

Mike Russo

- Proviso language – legislature wants to understand the strategy for teaching people to fill jobs needed; tie this into the “laws” of FL
- Align to put in place the educational component
- Deadline – December?

Ralph Wilcox

- Points to consider: proviso language, driving force to position Florida as a leader in Cybersecurity; Cybersecurity – needs to be clearly defined; educating students is a priority; collaboration with businesses and industry leaders; educate, train, and foster economic development; attract businesses to relocate or startup in the state – all a high priority to Governor Scott and Legislative leadership.
- Defense contracts need to be a focus as well
- This should quickly develop into a Nationwide effort

- Focus on sectors like defense, healthcare, finance, utilities, transportation, and government
- Copy of the report will be distributed to this group as soon as possible
- Follow-up call in 7-10 days
- The scope and ambition of the initiative is more of a question than whether or not there will be legislative support
- BOG and USF engaged in a collaborative effort to build the report; the final draft will likely be out the following week

Sri Sridharan added:

- Keeping students, companies and jobs in Florida as they seek training and education in Cybersecurity

Action Plans:

- a. Schedule a follow-up call soon
- b. Distribute the BOG report to this group
- c. Schedule a face to face meeting with this group ASAP

Letters of Support Table of Contents

| | |
|---|----|
| Florida Bankers Association..... | 57 |
| Citi..... | 59 |
| SunTrust..... | 60 |
| Jabil Circuits..... | 61 |
| Tech Data..... | 62 |
| Raymond James..... | 63 |
| Nielsen..... | 64 |
| TECO..... | 65 |
| IBM..... | 66 |
| USAA..... | 67 |
| Florida High Tech Corridor..... | 68 |
| Draper Laboratory..... | 69 |
| USF Research and Innovation..... | 70 |
| NFSTC..... | 72 |
| USF Center for Urban Transportation Research..... | 73 |
| Tampa Port Authority..... | 74 |
| Crystal Clear Technologies..... | 75 |
| Calhoun International..... | 77 |
| Vykin Corporation..... | 78 |
| Celestar..... | 79 |
| Diversified Incorporated of Tampa Bay..... | 80 |
| Edmonds Enterprise..... | 81 |
| GoBU Consulting..... | 82 |
| Iron Clad Technology Services..... | 83 |
| Navelite..... | 84 |
| Quiet Professionals..... | 85 |
| Quantum Technology Sciences..... | 86 |
| Solvability LLC..... | 87 |
| Tampa Bay Innovation Center..... | 88 |



FLORIDA BANKERS ASSOCIATION

ALEX SANCHEZ
PRESIDENT & CEO

November 15, 2013

The Honorable Rick Scott
Governor, State of Florida
The Capitol
Plaza Level
Tallahassee, FL 32399

Dear Governor Scott:

I would like to add my support to the creation of a Florida Center for Cybersecurity (FCC) to be hosted at the University of South Florida (USF). President Genshaft has made this a priority for the university and the FCC would be a tremendous win-win for our state and USF and would also have a positive impact on one of Florida's major private employers, the banking industry. Maintaining and developing the appropriate technologies to protect our customers' information and privacy is a top priority for Florida bankers.

The FCC at USF would further enhance economic development by using one of our major urban universities to develop cybersecurity practices and measures to place Florida in a leadership position. In addition:

- Cybersecurity (CS) is crucial in protecting the banking industry;
- There is a pressing need to hire talents in CS but, unfortunately, there not enough graduates in Florida to satisfy this high demand;
- There are several pockets of CS expertise in some Florida universities but there is a need for a FCC to make Florida a leading state in CS. Such a center will also attract many other companies who are hungry for CS talent to Florida;
- USF is well poised to host the FCC because of its current strong CS foundations, unique inter-disciplinary approach to CS and its location.

1001 THOMASVILLE ROAD • SUITE 201 • P.O. BOX 1360 • TALLAHASSEE, FL 32302-1360
TELEPHONE 850-224-2265 • FAX 850-224-2423

The Honorable Rick Scott
November 15, 2013
Page 2

In a recent article in *American Banker*, Adrienne Haden, an assistant director of banking supervision and regulation at the Federal Reserve Bank, stated:

"One impact of the DDoS attacks against U.S. financial institutions has been to increase awareness of the potential for well-organized or coordinated attacks with the intent of disruption of operations, possibly through destruction of access to business information," said Haden.

The creation of the FCC at a Florida university like USF would position Florida as a national leader in cybersecurity and its related high-skilled workforce through education, community engagement and innovative, interdisciplinary research.

Please feel free to call me if I can be of further assistance or if you would like to discuss this matter further. Thank you.

Sincerely,



Alex Sanchez
President and CEO
Florida Bankers Association

3800 Citigroup Center
A3/05
Tampa, FL 33610



November 22, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Governor Scott:

As a global financial institution with approximately 200 million customer accounts, Citi has the security of our customers' information and our operations at the forefront of our attention at all times. We have a focused information security strategy and dedicated resources to execute it. We continuously monitor and analyze threats and look for opportunities to further strengthen our controls. We work closely with a variety of suppliers to ensure we have access to top-notch security technology and can adapt to the changing internet landscape.

Regionally here in Tampa Bay, we have a longstanding community partnership and collaboration with the University of South Florida and its various Colleges, spanning our mutual interests and histories over the past thirty years; it is a very strong, diverse and resourceful relationship. Over the past several years in particular we have interacted with the University to identify highly skilled, well trained talent to fill highly technical roles that also require financial expertise. More recently we have engaged in discussions, recruitment and curriculum development in related subject areas of accounting, finance, information technology and cybersecurity. We believe the University's development of the Florida Center for Cybersecurity (FCC) will positively impact the country's preparedness to face growing threats to public and private business operations.

Citi, along with our peers and colleagues throughout the State, will benefit greatly from having the Center for Cybersecurity squarely focused within our marketplace. We encourage your administration's serious consideration of the USF administration's request for the support and funding of this timely, leadership capability in Florida.

Sincerely and cordially,

A handwritten signature in black ink that reads "Gregg Morton".

Gregg Morton
President, Citi Tampa

Citi



Allen Brinkman
Chairman, President & CEO

SunTrust Bank
401 E. Jackson Street
20th Floor
Tampa, FL 33602
Tel 813.224.2505
allen.brinkman@suntrust.com

November 18, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe Street
Tallahassee, FL 32399-0001

Dear Governor Scott,

Our national and economic security depends on the reliable functioning of this nation's critical infrastructure, especially in an interconnected, data-driven world. We rely on the Internet and other computer networks to run systems that help light our homes, provide fuel for our cars, and ensure that our water is safe to drink. Each day, trillions of dollars of electronic transactions flow across the payment networks and settlement systems that touch nearly every corner of our financial system and help keep track of funds in business and consumer accounts.

However, the cyber threat to critical infrastructure is growing. It represents one of the most serious challenges that the United States must confront. Because the majority of our critical infrastructure is owned and operated by private companies, facing this threat requires government and industry to work together to strengthen our digital defenses.

Safeguarding critical infrastructure is fundamental to preserving the stability of our financial system. The dependence of the global financial system on a rapid and accurately functioning technological infrastructure cannot be overstated. At the same time, cybersecurity threats pose significant financial, compliance, and reputational risks that can reverberate throughout the financial system.

In recognition of the crucial role that technological infrastructure plays in the operation of financial markets and the economy as a whole, financial institutions and market utilities are subject to regulation and examination standards relating to network and systems integrity. More broadly, the same logic applies to critical infrastructure organizations in other industries.

The Florida Center for Cybersecurity will help put Florida on the map in this critical area. It will not only help to meet the educational needs and workforce demands of companies in the state, but it will provide a resource for companies across the country and across the world – like SunTrust. I am asking for your support in joining SunTrust and the many other Florida companies that support this center so that Florida can truly be a leader in this strategically vital arena.

Regards,

A blue ink signature of Allen R. Brinkman, written in a cursive style.

Allen R. Brinkman



November 11, 2013

Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Governor Scott,

As a proud member of the Fortune 200, with our worldwide headquarters based here in Florida, Jabil is blessed to serve 150 of the most recognized product companies across the globe. At \$18B in revenue, with 40+ manufacturing centers, reaching 30+ countries, we offer a wide range of manufacturing, design, and supply chain services. Our efforts touch a variety of end markets, such as, Aerospace and Defense, Healthcare, Industrial, Clean Tech, Consumer goods, Automotive, Wearable computing, Mobile Devices, Data storage, Packaging, Wireless infrastructure, and Enterprise hardware.

As you might imagine, we handle significant amounts of customer data. Securing this information is of paramount importance. The inability to offer that assurance to our customers would pose a serious threat to our long and celebrated success.

As such, it is my honor to offer support and endorsement of the Florida Center for Cyber security, which promises to be a tremendous state asset and a national model of excellence. The FCC will ensure that companies like Jabil have the cyber security resources they need, as well as produce the kind of talented graduates that we would like to employ here in Florida. I look forward to exploring innovative ideas and opportunities with the FCC.

I am eager to see the FCC and all the good work it is capable of come to fruition. Please join me in support.

Thank you,

A handwritten signature in black ink, appearing to read "Mark", is placed above the printed name.

Mark Mondello
Chief Executive Officer

10560 DR. MARTIN
LUTHER KING, JR. ST N.
ST. PETERSBURG,
FLORIDA 33716
+1 727.577-9749
+1 727.579-8529
WWW.JABIL.COM



Robert M. Dutkowsky
Chief Executive Officer

November 11, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 South Monroe Street
Tallahassee, FL 32399-0001

Dear Governor Scott,

At Tech Data, one of our highest priorities is protecting our data and network infrastructure so that we can best serve our customers. In the past several years, with the expansion of mobile devices, cloud-based services and other web-dependent activities, this critical activity has become significantly more challenging. Cybersecurity is now one of our most urgent and important needs.

Being a home-grown Florida business that has expanded into the state's second-largest Fortune 500 company, Tech Data wants to hire more talented Florida graduates with cybersecurity training to help us fortify our defenses. However, we are not finding enough graduates with the necessary skills. There are fragmented efforts in cybersecurity education and services scattered across the state, but Florida has no central cybersecurity power-base and no reliable pipeline of skilled cybersecurity professionals. As a result, we've instead had to recruit employees and contract with companies from outside of Florida which is expensive and time-consuming. In short, we are spending time and money on a service that should be part of Florida's economic development.

Creating a Florida Center for Cybersecurity would greatly benefit a company like Tech Data and, many other Florida businesses across a spectrum of industries throughout the state. It would help us expand as we better utilize energy that we have been using on patchwork cybersecurity efforts. It would afford us the opportunity to place Florida students in high-tech internships that would lead to high-paying jobs. I am confident this solution would help lure other large companies, who are also seeking cybersecurity talent, to migrate their business to Florida.

The University of South Florida, with its strong cybersecurity knowledge-base, interdisciplinary approach, and location near business and defense entities in Tampa Bay, is well-positioned to host this revolutionary workforce driver.

I kindly urge you to support and invest in this important initiative, for the betterment of all of Florida.

Respectfully,

A handwritten signature in blue ink, appearing to read 'R. Dutkowsky', written over the word 'Respectfully'.

Robert Dutkowsky, CEO

RAYMOND JAMES®

November 14, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Governor Scott,

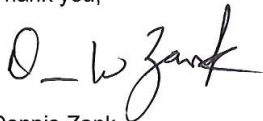
I want to kindly ask for your support of a critical endeavor in the state of Florida, the Florida Center for Cybersecurity. For Raymond James, one of the state's largest financial institutions, there is nothing more important than ensuring the security of our customers' data and our assets. We are convinced that a statewide Cybersecurity hub would provide a vital asset not only for our company, but for companies across the nation and the world. Florida can, and should, seize this opportunity to become a leader in this field.

Serving approximately 2.5 million accounts in more than 3,000 locations throughout the U.S., Canada and across the world, Raymond James is deeply involved in today's fast moving and ever changing global economy. We are familiar with the real dangers of cyber-threats, and we are constantly on the lookout for new solutions and talented Cybersecurity experts. This is a need that will only continue to grow as our world moves more and more online.

A Florida Center for Cybersecurity would ensure that companies like Raymond James have the Cybersecurity resources they need, as well as produce the kind of talented graduates that we would like to employ. USF's status as a top 50 research university, positions it well to provide advanced research on Cybersecurity topics. Over 10% of our associates working in Information Security roles today are USF graduates and we benefit from USF's ability to produce strong performers. We fully expect that by adding degrees in Cybersecurity it would further enhance that in the future.

I look forward to exploring opportunities with the FCC, and I know my fellow business leaders will feel the same way.

Thank you,



Dennis Zank
Chief Operating Officer
Raymond James Financial

cc: Dean Moez Limayem, University of South Florida, College of Business

DENNIS W. ZANK
Chief Operating Officer
Raymond James Financial, Inc.

880 Carillon Parkway // St. Petersburg, FL 33716
D 727.567.4007 // T 800.248.8863 // F 727.567.8312 // raymondjames.com



Robert L. McCann, Jr.
Executive Vice President

November 13, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Governor Scott,

For more than ninety years Nielsen has been measuring consumer behavior as a means to enable manufacturers, broadcasters, retailers and others to build their businesses and compete more effectively. Today, Nielsen serves a broad cross section of different industries that span more than one hundred countries around the world and the Nielsen Global Technology & Innovation Center in Tampa Bay (where Nielsen employs more than 2,000 professionals) is a vital resource used by Nielsen to serve this varied client portfolio.

At the very heart of the Nielsen business model is the consumer and the need for consumer privacy. Indeed, Nielsen makes extraordinary efforts all across the world to protect both the foundation of our databases (consumer measurements) and the proprietary insights we provide to clients. The Company would essentially be unable to properly do its job if it could not provide these important data protections and hence that is why cybersecurity is important to Nielsen. It is why Nielsen would certainly be very supportive of efforts to establish a cybersecurity hub in Florida.

The Florida Center for Cybersecurity will help put Florida on the map in this critical area. It will not only help to meet the educational needs and workforce demands of companies in the state, but it will provide a resource for companies across the country and across the world – like Nielsen.

I hope you will join Nielsen and the many other Florida companies that support this center so that Florida can truly be a leader in this strategically vital arena.

Thank you,

A handwritten signature in blue ink that reads "Robert L. McCann".

Robert L. McCann
Executive Vice President

The Nielsen Company
501 Brooker Creek Blvd., Oldsmar, FL 34677
tel 813 366 5544 fax 813 366 0053
www.nielsen.com



GORDON L. GILLETTE
PRESIDENT

November 14, 2013

Rick Scott
Governor
State of Florida
Tallahassee, FL

Dear Governor Scott:

I am writing in support of the creation of the Florida Center for Cybersecurity (FCC) at the University of South Florida. As the President of Tampa Electric Company and as past Chairman of the Board at the Florida Reliability Coordinating Council (FRCC), I am very focused on the pressing need to hire talented individuals with cybersecurity knowledge and to further cybersecurity research and knowledge. The FRCC is one of 8 member regions of the North American Electric Reliability Council (NERC), which is responsible for the reliability of the electricity grid for our entire continent. NERC is responsible for issuing and maintaining cyber and other security standards and the FRCC is responsible for implementing them in peninsular Florida. There are 58 electric utilities in Florida and all are working to comply with ever-changing cybersecurity standards, so the need for such a Center is substantial for our industry alone.

There are several pockets of cybersecurity expertise in other Florida universities, but I feel that the University of South Florida (USF) is the best qualified to host the FCC due to its current strong cybersecurity foundations, unique inter-disciplinary approach to cybersecurity and its central location. To illustrate the location related advantages, the FRCC, Tampa Electric, Duke Energy -Florida and Seminole Electric Cooperative, some of Florida's larger electric companies, are all headquartered in the Tampa Bay area. It is on the basis of the foregoing that I whole-heartedly support the creation of the Florida Center for Cybersecurity at USF.

Sincerely,

A handwritten signature in blue ink, appearing to be "GLG", is written below the word "Sincerely,".

GLG:tdw

P.O. BOX 111 TAMPA, FL 33601-0111
813-228-4492 FAX 813-228-4290
GLGILLETTE@TECOENERGY.COM

1 Nov 2013

Governor Rick Scott
Capitol
Tallahassee, FL

Dear Governor Scott:

I manage two classified IBM research, development, test & evaluation facilities in the Tampa/St Pete area supporting our military COCOMs. At IBM, one of our highest priorities is ensuring the complete protection of associated data and network infrastructures to best maintain the integrity of our customers and partners. With the expansion of mobile devices, cloud-based services and other web-dependent activities, providing protection of data has become significantly more challenging. Ensuring effective cybersecurity is now one of our most urgent and important needs.

As a global technology leader, IBM supports the development and hiring of talented graduates around the world, and, with our presence in Florida, we look to support increased opportunities to work with cybersecurity students and professionals within the state to help fortify defenses for us, our customers and our nation.

A major issue noted is the limited availability of educated and experienced cybersecurity resources nationwide. And I've noticed that although there are fragmented efforts in cybersecurity education and services scattered across the state, Florida has no central cybersecurity power-base and no reliable pipeline of skilled cybersecurity professionals. We continue to do business, out of state, partnering to provide cybersecurity services on what could be increased economy for the state *if* the proper base were present.

A Florida Center for Cybersecurity would be a game-changer. It could serve to meet the vital needs of Florida companies across a spectrum of industries. And, just as Florida is known as the military combatant command powerhouse in the US, this move would help establish Florida as a cybersecurity leader for the nation, luring additional talent, companies and opportunities to Florida.

The University of South Florida, with its strong cybersecurity knowledge-base, interdisciplinary approach, and location near major business and defense entities in Tampa Bay, is well-positioned to host this revolutionary workforce driver.

I look forward to your strong and timely support in this important initiative, for the betterment of all of Florida.

Respectfully,

Tony Smith
Tony Smith, PMP, CISSP
St. Petersburg Site Location Executive
IBM Global Business Services
tony.smith@us.ibm.com

IBM



9800 Fredericksburg Road
San Antonio, Texas 78288

November 19, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Governor Scott,

For more than nine decades, USAA has protected its members from a wide variety of physical and information security threats. With the rise of cyberspace crime, USAA and other private sector companies continue to remain vigilant in this area. We are seeking your assistance in establishing the Florida Center for Cybersecurity, a proposed collaboration between governmental and private entities to ensure optimal protection of our customers and the citizens of your state from cyber security threats.

It is important for us to work together to share and receive the latest procedures and best practices for guarding against known and emerging security threats. The Florida Center for Cybersecurity will be a conduit for early security threat warnings and a catalyst for receiving timely notification and authoritative information designed to help protect critical systems and assets from physical and cyber threats. The Center will also help meet the educational needs and workforce demands of companies and public services in the state, and be a model for private / public cooperation to detect and prevent cyber security crime.

I hope you will join USAA and the many other Florida companies that support this Center so that Florida can truly be a leader in this strategically vital security arena.

Sincerely,

A handwritten signature in black ink, appearing to read "Robert Hoyland".

Robert Hoyland
Vice President, Financial Foundations
United Services Automobile Association



November 6, 2013

Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Gov. Scott:

On behalf of the Florida High Tech Corridor Council (FHTCC) and its economic development, workforce, higher education and industry partners, I am proud to support the Florida Center for Cybersecurity at the University of South Florida (USF).

This proposed program has the potential to greatly enhance Florida's future economy by cultivating a high tech, high-wage workforce in the rapidly growing field of cybersecurity. As a specialized STEM field, cybersecurity is a critical component of both financial business and national defense, two sectors that are heavily concentrated in Tampa Bay.

The University of South Florida has a proven track record of leadership in advanced research, interdisciplinary collaboration and community partnership—all key ingredients in supporting the development of a cybersecurity Center of Excellence that will drive the creation of new jobs, attraction of new companies and cultivation of highly skilled talent. USF's partnerships in the Tampa Bay region will foster connections among many of Florida's largest companies, as well as several of the nation's most important national defense bases.

Charged with growing high tech industry and innovation through partnerships that support research, marketing, workforce and entrepreneurship, FHTCC is supportive of projects that will meet industry needs now and in the future. On behalf of the Council, I am proud to ask for your commitment to growing our great state's innovation-based economy through this initiative.

Best regards,

A handwritten signature in black ink that reads 'Randy Berridge'.

Randy Berridge
President

A regional economic development initiative of:



1055 AAA Drive
Suite 140
Heathrow, FL 32746
PH. 407.708.4630
FX. 407.708.4635
www.FloridaHighTech.com



November 5, 2013

The Honorable Rick Scott
Governor, State of Florida
The Capitol
400 S. Monroe Street
Tallahassee FL 32399

Re: Letter of Support for the Florida Center for Cybersecurity

Dear Governor Scott:

I am writing this letter to express my support for the establishment of an investment into the Florida Cybersecurity Center of Excellence (FCC) to be set up at University of South Florida.

Cybersecurity is a serious issue today and it affects all businesses, citizens, Government and national security. Data protection is of vital importance to a healthy economy. Financial services industry, Healthcare, Energy, Utilities industries are especially vulnerable, not to mention the Department of Defense.

The FCC will be of monumental value to all businesses and the Government, built on a public private partnership. After reviewing the vision, mission and goals of the center, we lend our support, without any hesitation, to this effort and intend to work closely with the center.

The FCC will help with workforce development (create jobs, and high paying jobs), provide expert consulting services and will aid in the growth of Florida's economy.

The FCC will be a complimentary effort to assisting Draper's ongoing work in cyber forensics, identity management, mobile software, and secure data links here in Florida.

We strongly urge investment in this center and emphasize that time is of the essence.

Thank You.

A handwritten signature in black ink, appearing to read "Shankar Sundaram".

Shankar Sundaram
Center Director, Draper Laboratory

DRAPER BIOENGINEERING CENTER AT USF
3802 SPECTRUM BLVD | SUITE 201 | TAMPA | FLORIDA | 33612-9220
P: 813.465.5400 | F: 813.465.5401 | W: WWW.DRAPER.COM



November 5, 2013

The Honorable Rick Scott
Governor, State of Florida
The Capitol
400 S. Monroe Street
Tallahassee, FL 32399

Dear Governor Scott:

USF Research and Innovation is very pleased to write this letter in support of the establishment and investment into the Florida Cybersecurity Center of Excellence to be housed at the University of South Florida. The proposed Cybersecurity Center of Excellence at USF will position the State of Florida as the national leader in cybersecurity, create new high-paying jobs, serve as the statewide facilitator of cybersecurity education, act as a "one stop-shop" cybersecurity clearing house for the statewide business and higher education communities, and attract new financial, healthcare, transportation, utility, and defense entities to Florida. The Cybersecurity Center will also provide an avenue for collaboration for the numerous exports on this topic throughout the state.

Along with USF's solid foundation in the cybersecurity arena and its ideal location to security experts at MacDill Air Force Base, the University of South Florida is one of the nation's top 73 public research very high universities and one of 40 public research universities nationwide with very high research activity that is designated as community engaged by the Carnegie Foundation for the Advancement of Teaching. The dedication of USF researchers, students, and staff has contributed to the phenomenal growth in research that USF has experienced over the past 27 years. In FY1986, the University received \$22.3 million in external funding for research projects. In FY1995, research awards had reached over \$100 million and in FY2013, USF generated over \$413.6 million in sponsored research activity. According to the National Science Foundation (NSF), USF ranks 50th in the nation for total research expenditures among all U.S. universities, public and private, and is ranked 33rd in total research expenditures and 30th in federal research expenditures for public universities. In 1990, USF became a member of the Oak Ridge Associated Universities. A designation that allows USF to participate in research collaborations with national laboratories, federal agencies, other educational and governmental entities, and the private sector.

The Technology Transfer Office was established at USF in 1990 to facilitate the commercialization of university intellectual property, including patents and copyrights. As a result, USF ranked in the top 10 world-wide for granted U.S. patents among all universities in 2010 and 2011. In 2012, USF was in the top 15 for the number of startup companies and in the top 25 for the number of licenses and options,

USF RESEARCH & INNOVATION • OFFICE OF THE SENIOR VICE PRESIDENT
University of South Florida • 3702 Spectrum Blvd., Suite 165 • Tampa, FL 33612-9445
(813) 974-5570 • Fax (813) 974-4962 • www.research.usf.edu

when compared to other U.S. universities in a survey by the Association of University Technology Managers. In recent years, USF founded and remains the home of the National Academy of Inventors (NAI), a non-profit member organization with over 2,000 individual inventor members and Fellows spanning more than 100 U.S. universities, and governmental and non-profit research institutions. The USF Chapter of the NAI has 270 USF faculty, staff, students, and alumni members, who collectively hold more than 1,400 U.S. patents.

As you can see, the University of South Florida is dedicated to the discovery of new knowledge, insights, and forms of expression through significant innovative research and other creative activity. Please accept this letter as an indication of the Office of Research and Innovation's commitment and strong desire to support this Center and all our faculty and their research endeavors.

Sincerely yours,



Paul R. Sanberg, Ph.D., D.Sc.
Senior Vice President for Research & Innovation



7881 114th Avenue North
Largo, FL 33773
ph (727) 549-6067
fx (727) 549-6070
www.nfstc.org

November 19, 2013

The Honorable Rick Scott
Office of the Governor
State of Florida
The Capitol
400 S. Monroe Street
Tallahassee, FL 32399-0001

Dear Governor Scott,

Since 1995, the National Forensic Science Technology Center (NFSTC) has been supporting law enforcement, criminal justice and military professionals through training and innovative programs. In that time, we have seen digital and cyber communications tools and technologies grow tremendously, both as an investigative tool and as a weapon for espionage, commercial and individual crime. As a result, the need for well-trained cybersecurity professionals has grown right along with it.

NFSTC is writing in support of establishing the Florida Center for Cybersecurity (FCC) and creating an educational and commercial hub in our state. This is a great opportunity to further build Florida's strengths in STEM education as well as workplace stability and attractiveness.

The Florida Center for Cybersecurity will help put Florida on the map in this critical area. It will not only help to meet the educational needs and workforce demands of companies in the state, but will provide a valuable resource across the country and around the world.

I hope you will join NFSTC and the many other Florida companies that support this initiative to establish Florida as a strategic leader in cybersecurity.

Warm regards,

Kevin Lothridge, CEO
Kevin.lothridge@nfstc.org

NFSTC is a 501(c)3 not-for-profit corporation.



November 4, 2013

Office of Governor Rick Scott
State of Florida
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Gov. Scott,

In today's modern world of mobile technology and constant connectivity, our businesses and in fact nearly all facets of modern life, increasingly rely on cybersecurity to ensure that information and assets are protected. Threats come from all directions.

This is not only a problem that affects transportation. From information to process credentials to access ports and airports to information collected on toll and expressways, the data security issues are more relevant today than ever before. Cybersecurity has quickly become one of the most serious issues our nation has ever faced. The country needs an infusion of highly skilled cybersecurity professionals. Florida can take the lead and we are well positioned to do so.

Now is the time for investing in a statewide center for cybersecurity. As the leader in this field, Florida will be the example for others states to follow. Ensuring that Florida is on the cutting-edge of this global industry will encourage job growth as our talent pool is enriched.

I wholeheartedly support the creation of the Florida Cybersecurity Center, to be housed at the University of South Florida, and I urge you to do so as well by investing in its future. It would be an investment that would deliver rich returns for all of Florida's businesses and residents.

Thank you,

A handwritten signature in blue ink, appearing to read "Jason Bittner", is written over the "Thank you," text.

Jason Bittner
Director



University of South Florida • 4202 E. Fowler Avenue CUT100 • Tampa, FL 33620-5375
(813) 974-3120 • FAX (813) 974-5168 • www.cutr.usf.edu



TAMPA PORT AUTHORITY

November 25, 2013

Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Governor Scott:

On behalf of the Tampa Bay Port Authority, I am proud to support the Florida Center for Cybersecurity at the University of South Florida (USF).

This proposed program has the potential to greatly enhance Florida's future economy by cultivating a high tech, high-wage workforce in the rapidly growing field of cybersecurity. As a specialized STEM field, cybersecurity is a critical component of the Transportation Industry.

The University of South Florida has a proven track record of leadership in higher education, applied research, interdisciplinary collaboration and community partnership. All of these are key ingredients which support the development of a Cybersecurity Center of Excellence.

The Center will drive the creation of new jobs, attract new companies and cultivate highly skilled talent. Furthermore, USF's partnerships in the Tampa Bay region will foster connections between some of Florida's largest companies and the transportation industry.

The Tampa Port Authority is supportive of this critical project and timely initiative. On behalf of the Port Authority, I am proud to ask for your commitment and support this initiative.

Best Regards,

A handwritten signature in blue ink that reads "Paul Anderson". The signature is fluid and cursive.

Paul Anderson, President & CEO



November 4, 2013

Gov. Rick Scott
Capitol
Tallahassee, FL

Dear Gov. Scott,

Thank you for your recent letter on Oct 4 congratulating me for Crystal Clear Technologies recent recognition as a nominee for Tampa Chamber of Commerce Small Business of the Year Award. In your letter you mentioned Florida's unemployment rate and a focus on creating jobs. As a Woman Owned Small Business based in St Petersburg, we struggle to hire talented graduates with cybersecurity training to help us fortify our defenses, largely because the supply is not currently available.

There are fragmented efforts in cybersecurity education and services scattered across the state, but Florida has no central cybersecurity power-base and no reliable pipeline of skilled cybersecurity professionals. Due to the demand of this skillset and lack of supply within Florida, we've instead had to contract with companies in Maryland, Texas, and Washington DC just to name a few. We've also struggled with filling positions for Govt related cyberdefense with United States Major Commands (USMAJCOM's) which we contract with.

Our highest priority at Crystal Clear Technologies is protecting the data and network infrastructure of our customers throughout the world. The expansion of mobile devices, cloud-based services and other web-dependent activities has made our efforts significantly more challenging. Cybersecurity is now one of our most urgent and important focal points.

A Florida Center for Cybersecurity would be a significant step forward for the state of Florida. It would meet the vital needs of Florida companies across a spectrum of industries. It would help us expand—as we better utilize energy that we have been using on patchwork cybersecurity efforts. I am confident it would help lure other large companies who are hungry for cybersecurity talent to Florida. The University of South Florida, with its strong cybersecurity knowledge-base, interdisciplinary approach, and location near business and defense entities in Tampa Bay, is well-positioned to host this revolutionary workforce driver.

5555 Central Ave. St. Petersburg, Florida 33710

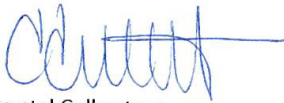
Ph: 727.321.8888

Fx: 727.683.9360

November 4, 2013

I urge you to support and invest in this important endeavor, for the betterment of all of Florida.

Respectfully,



Crystal Culbertson
Chief Executive Officer
Crystal Clear Technologies, Inc.
8(m) Woman Owned Small Business
www.crystalcleartec.com

5555 Central Ave. St. Petersburg, Florida 33710

Ph: 727.321.8888

Fx: 727.683.9360



November 1, 2013

The Honorable Rick Scott
Office of the Governor
The Capitol
400 S Monroe St
Tallahassee, FL 32399-0001

Dear Governor Scott,

I am writing this letter to express my support for the establishment of and continued investment into the Florida Cybersecurity Center of Excellence (FCC) at University of South Florida. As you are aware, Cybersecurity is a serious issue in our nation as it affects all businesses, citizens, as well as federal, state and local governments. We have also found that other critical institutions such as financial services, Healthcare, Energy, and Utilities are especially vulnerable as well.

I strongly believe that the FCC will be of monumental value to all stakeholders in the Cybersecurity arena. The FCC will position Florida as a leader in Cybersecurity efforts as well as serve as the statewide facilitator of Cybersecurity education. Lastly, the FCC can assist in developing a Cybersecurity workforce, which will attract defense, financial, healthcare industries to our state and aid in the growth of Florida's economy.

After reviewing the vision, mission and goals of the center, Calhoun International lends its support, without any hesitation, to this effort. We also intend to work closely with the center to assist in its very important mission.

Thank you for your attention to this very critical issue.

Sincerely,

Roger Swinford
President and CEO
Calhoun International

CALHOUN INTERNATIONAL
100 North Tampa St Suite 2330
Tampa, FL 33602



20 November 2013

Office of Governor Rick Scott
State Of Florida
The Capitol
400 S. Monroe Street
Tallahassee, FL 32399

Dear Governor Scott,

I was excited and encouraged to hear about the potential plans to bring the Florida Center for Cyber Security to Tampa in partnership with the University of South Florida.

Vykin Corporation is a Florida resident, veteran owned small business, headquartered in Tampa, FL. We at Vykin provide Information Technology, Intelligence Analysis and Cyber Security solutions to US national agencies and combatant commands operating in seven states and eleven countries.

We know firsthand how important cyber security will be to the safety and economic security of the citizens of the great state of Florida and to the United States as a whole.

We believe Tampa, like no other place in Florida, provides a unique environment where outstanding higher education institutions are co-located with corporate cyber excellence and US Combatant Commands fighting the cyber security war every day.

I see an amazing opportunity to link Tampa based cyber small businesses such as Vykin, Celestar Corporation , AC4S and Crystal Clear Technologies with local universities to provide unique internship opportunities grounded in real world problem sets. I am certain my colleagues would join me in leading such initiatives and would commit corporate resources to ensure the FCSC gets off to the best possible start.

I am confident we have all the pieces in place to develop the best cyber security specialists in the country and make Tampa synonymous with Cyber Security excellence. I ask that you give the creation of this center the full support of your office and help ensure it becomes a reality.

Best Regards,

A handwritten signature in black ink, appearing to read "E. Bachl", written over a horizontal line.

Edward A. Bachl
CEO

400 N Ashley Drive, Suite 1440 • Tampa, FL • 33606
Phone: (888) 809-0025 • Fax: (866) 535-7954
www.vykincorp.com

20 November, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe Street
Tallahassee, FL 32399-0001

Dear Governor Scott,

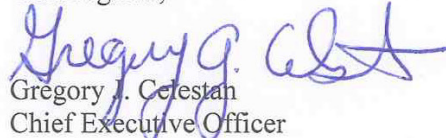
Celestar Corporation is a Service Disabled Veteran Owned Small Business headquartered in Tampa, FL that specializes in providing innovative and cost effective intelligence support to U.S. Government clients and Private Industry.

Our company began as a purely intelligence consulting and training enterprise at United States Central Command in 2004, but continues to grow as it proves itself to be a viable solution for many clients. Since 2004, Celestar Corporation has seen an expansion to other organizations; to include the Defense Intelligence Agency, U.S. State Department and the U.S. Army National Guard. Celestar currently has personnel serving in 10 states as well as overseas locations. Cybersecurity is very important to our business operations and is an essential component in providing services to our clients, which is why Celestar is very supportive of establishing a cybersecurity hub in Florida.

The USF Florida Center for Cybersecurity will help to attract other business and agencies which can benefit from the intellectual capital assembled at the campus. It will not only help to meet the educational needs and workforce demands of companies in Hillsborough County and the State of Florida, but will also provide a resource for companies across the country and around the world.

We urge you to support this center so that Florida can truly be a leader in this strategically vital arena.

With regards,


Gregory J. Celestan
Chief Executive Officer



9501 EAST U.S HWY 92 / TAMPA, FLORIDA / 33610



DIVERSIFIED INCORPORATED OF TAMPA BAY
12907 Hickorywood Lane
Largo, FL 33774

November 4, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Sir:

I am writing this letter to express my support for the establishment of and investment into the Florida Cybersecurity Center of Excellence (FCC) to be set up at University of South Florida.

Cybersecurity is a serious issue today and it affects all businesses, citizens, Government and national security. Data protection is of vital importance to a healthy economy. Financial services industry, Healthcare, Energy, Utilities industries are especially vulnerable, not to mention the Department of Defense.

The FCC will be of monumental value to all businesses and the Government, built on a public private partnership. After reviewing the vision, mission and goals of the center, we lend our support, without any hesitation, to this effort and intend to work closely with the center.

The FCC will help with workforce development (create jobs, and high paying jobs), provide expert consulting services and will aid in the growth of Florida's economy.

We strongly urge investment in this center and emphasize that time is of the essence.

Thank You.

Diane Zader

Diane Zader
President
Diversified Incorporated of Tampa Bay

Toll Free - 888-3DIV-INC
888-334-8462

www.div-inc.com



Office of the President
4202 E. Fowler Ave, CGS 401
Tampa, FL 33620-4401

Dear President Genshaft,

Recently I became aware of the state of Florida's initiative to establish the Florida Center for Cyber security at the University of South Florida. As a former Director of DISA, and former Director of Command, Control, Communications, and Computers (J-6) for US CENTCOM, I know that creating a forward-thinking and proactive network of academic, business, and both public and public sector cyber security training programs, will be invaluable to those you serve. I could envision USF becoming the academic center for Cyber trends, research, and technology incubation, and a highly respected institution where industry, public, private, and the DoD, could come to test new capabilities and facilitate network sustainment through simulation and expert assistance. I note the success you have had creating a "Stem Camp" as a threshold experience for Floridian youth. Initiatives like yours, to raise the levels of interest for our future cyber work force, are truly inspirational and sorely needed.

The University of South Florida has the ability to create an important bridge between the owners and operators of critical and vulnerable infrastructure and those entities best positioned to develop a more secure cyber network.

I support and endorse the University of South Florida's Florida Center for Cyber security and look forward to hearing about the comprehensive cyber programs USF designs to keep America safe and nation's economy strong.

Sincerely

A handwritten signature in dark ink, appearing to read "Al Edmonds", is written over a light blue horizontal line.

Al Edmonds
LT/General, USAF (Retired)
Chairman and CEO
(Former Director, Defense Information Systems Agency-DISA)

2760 Eisenhower Avenue, Suite 202
Alexandria, Virginia 22314

www.edmondses.com

Office: (703) 778-7070

Fax: (703) 778-7060



November 4, 2013

Office of Governor Rick Scott

State of Florida

The Capitol

400 S. Monroe St.

Tallahassee, FL 32399-0001

I am writing this letter to express my support for the establishment of and investment into the Florida Cybersecurity Center of Excellence (FCC) to be set up at University of South Florida.

Cybersecurity and data protection is vital importance to a healthy economy. Financial services industry, Healthcare, Energy, Utilities industries in particular the Department of Defense rely on data security to protect the American way of life. Unfortunately, current technologies are not adequate to maintain the security of that data and those who wish to do us harm are constantly creating new ways to access our data.

I spent 18 years in acquisition as a Contracting Officer, Program Manager and the Technical industrial Liaison Officer for the United States Special Operations Command. During my time there, I was amazed that the local academia did not take advantage of the opportunities the command offered in developing leading edge technologies. I believe that the FCC will help to change that environment to create an opportunity for greater interaction between USSOCOM and academia to help foster technologies that are beneficial to both the Government and Civilian sectors.

I strongly urge investment in the FCC and hope that the state of Florida will move quickly to support this endeavor.

Thank You.

Joseph R Daum, D.B.A

President

GoBU Consulting, LLC

IRONCLAD

TECHNOLOGY SERVICES

11/1/2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Sir,

I am writing this letter to express my support for the establishment of and investment in the Florida Cyber Security Center of Excellence (FCC) to be set up at University of South Florida.

Today's environment requires vigilance and expertise to thwart the continued attempts of cyber-attack on US Infrastructure targets belonging to private business and government agencies at all levels.

The FCC will be of monumental value to the aforementioned targets and it is our belief that the lessons learned from this sorely needed resource will provide huge dividends. After reviewing the vision, mission and goals of the center, we lend our support, without any hesitation, to this effort and intend to work closely with the center.

The FCC will help with workforce development (create jobs, and high paying jobs), provide expert consulting services and will aid in the growth of Florida's economy.

We strongly urge investment in this center and emphasize that time is of the essence.

Thank You.



Tony Land
Executive Vice President
Ironclad Technology Services LLC



November 2, 2013

TO: Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

REFERENCE: USF Cybersecurity Center of Excellence

Dear Governor Scott,

I am writing this letter to express my support for the establishment of and investment into the Florida Cybersecurity Center of Excellence (FCC) to be set up at University of South Florida.

Cybersecurity is a serious issue today and it affects all businesses, citizens, Government and national security. Data protection is of vital importance to a healthy economy. Financial services industry, Healthcare, Energy, Utilities industries are especially vulnerable, not to mention the Department of Defense.

The FCC will be of monumental value to all businesses and the Government, built on a public private partnership. After reviewing the vision, mission and goals of the center, we lend our support, without any hesitation, to this effort and intend to work closely with the center.

The FCC will help with workforce development (create jobs, and high paying jobs), provide expert consulting services and will aid in the growth of Florida's economy. I strongly urge investment in this center and emphasize that time is of the essence.

Being a retired Army Sergeant Major after serving just over 20 years in Special Operations (the last 14 of which were in Delta Force), I can attest to the criticality of such an academic program. The future security of the United States will depend on our youth's ability to maintain and enhance Cybersecurity. I can think of no better place for a program such as this having three major commands; USSOCOM, USCENTCOM and USSOCCENT located within minutes from the USF campus.

Thank You.

Sincerely,

Andrew S. Wilson

Digitally signed by Andrew S. Wilson
DN: cn=Andrew S. Wilson, o=NavELite, LLC, ou,
email=andrew.wilson@navelite.com, c=US
Date: 2013.11.02 02:33:05 -04'00'

Andrew Wilson President & CEO

WWW.NAVELITE.COM / (888) 928-8696

WHEN SURVIVAL COUNTS



November 2, 2013

TO: Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

REFERENCE: USF Cybersecurity Center of Excellence

Dear Governor Scott,

I am writing this letter to express my support for the establishment of and investment into the Florida Cybersecurity Center of Excellence (FCC) to be set up at University of South Florida.

Cybersecurity is a serious issue today and it affects all businesses, citizens, Government and national security. Data protection is of vital importance to a healthy economy. Financial services industry, Healthcare, Energy, Utilities industries are especially vulnerable, not to mention the Department of Defense.

The FCC will be of monumental value to all businesses and the Government, built on a public private partnership. After reviewing the vision, mission and goals of the center, we lend our support, without any hesitation, to this effort and intend to work closely with the center.

The FCC will help with workforce development (create jobs, and high paying jobs), provide expert consulting services and will aid in the growth of Florida's economy. I strongly urge investment in this center and emphasize that time is of the essence.

Being a retired Army Sergeant Major after serving just over 20 years in Special Operations (the last 14 of which were in Delta Force), I can attest to the criticality of such an academic program. The future security of the United States will depend on our youth's ability to maintain and enhance Cybersecurity. I can think of no better place for a program such as this having three major commands; USSOCOM, USCENTCOM and USSOCENT located within minutes from the USF campus.

Thank You.

Sincerely,

Andrew S. Wilson

Digitally signed by Andrew S. Wilson
DN: cn=Andrew S. Wilson, o=Quiet Professionals,
LLC, ou, email=andy@quietprofessionalsllc.com,
c=US
Date: 2013.11.02 02:31:45 -04'00'

Andrew Wilson President & CEO

Superior Skills, Proven Performance

WWW.QUIETPROFESSIONALLLC.COM / 727-488-9926 / 36181 EAST LAKE ROAD, SUITE 220, PALM HARBOR, FL 34685



Quantum Technology Sciences, Inc.
1980 North Atlantic Avenue, Suite 201
Cocoa Beach, FL 32931
Phone (321) 868-0288 / Fax (321) 868-0303

November 5, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Governor Scott:

I am writing this letter to express my support for the establishment of an investment into the Florida Cybersecurity Center of Excellence (FCC) to be set up at University of South Florida.

Cybersecurity is a serious issue today and it affects all businesses, citizens, Government and national security. Data protection is of vital importance to a healthy economy. Financial services industry, Healthcare, Energy, Utilities industries are especially vulnerable, not to mention the Department of Defense.

The FCC will be of monumental value to all businesses and the Government, built on a public private partnership. After reviewing the vision, mission and goals of the center, we lend our support, without any hesitation, to this effort and intend to work closely with the center.

The FCC will help with workforce development (create jobs, and high paying jobs), provide expert consulting services and will aid in the growth of Florida's economy.

We strongly urge investment in this center and emphasize that time is of the essence.

Thank You,

A handwritten signature in black ink, appearing to read "Freddie Garcia", written over a horizontal line.

Freddie "Chick" Garcia, Jr.
CEO/Chairman of the Board
Quantum Technology Sciences, Inc.



November 1, 2013

Dear Governor Scott:

I am writing this letter to express my support for the establishment of and investment into the Florida Cybersecurity Center of Excellence (FCC) to be set up at University of South Florida.

Cybersecurity is a serious issue today and it affects all businesses, citizens, Government and national security. Data protection is of vital importance to a healthy economy. Financial services industry, Healthcare, Energy, Utilities industries are especially vulnerable, not to mention the Department of Defense.

Creating the center in this critical market will make Florida a leader in this area, and will contribute to the ongoing growth of the IT workforce in our area.

The FCC will be of monumental value to all businesses and the Government, built on a public private partnership. After reviewing the vision, mission and goals of the center, I lend my support, without any hesitation, to this effort and intend to work closely with the center.

The FCC will help with workforce development (create jobs, and high paying jobs), provide expert consulting services and will aid in the growth of Florida's economy.

I strongly urge investment in this center and emphasize that time is of the essence.

A handwritten signature in cursive script that reads "Jenny W. Clark".

Jenny W. Clark

Director

Decosimo-Solvability, LLC

10721 Donbese Avenue

Tampa, FL 33615



7887 Bryan Dairy Road, Suite 220, Largo, FL 33777
www.tbinnovates.com

Main Office: 727-547-7340
Fax Number: 727-547-7350

November 5, 2013

Office of Governor Rick Scott
State of Florida
The Capitol
400 S. Monroe St.
Tallahassee, FL 32399-0001

Dear Governor Scott:

I am writing this letter to express my support for the establishment of and investment into the Florida Cybersecurity Center of Excellence (FCC) to be set up at University of South Florida.

Cybersecurity is a serious issue today and it affects all businesses, citizens, Government and national security. Data protection is of vital importance to a healthy economy. Financial services industry, Healthcare, Energy, Utilities industries are especially vulnerable, not to mention the Department of Defense.

The FCC will be of monumental value to all businesses and the Government, built on a public private partnership. After reviewing the vision, mission and goals of the center, we lend our support, without any hesitation, to this effort and intend to work closely with the center.

The FCC will help with workforce development (create jobs, and high paying jobs), provide expert consulting services and will aid in the growth of Florida's economy.

We strongly urge investment in this center and emphasize that time is of the essence.

Thank You,

A handwritten signature in black ink, appearing to read "Tonya Elmore".

Tonya Elmore, President & CEO