

Florida Center for
Cybersecurity
at the University of South Florida



RESPONSE

to

National Institute of Standards and Technology (NIST)
Request for Information



Strengthening the Cybersecurity of Federal Networks and
Critical Infrastructure: Workforce Development

Prepared by the
Florida Center for Cybersecurity
in collaboration with the
State University System of Florida



July 27, 2017

To whom it may concern:

The State of Florida is uniquely positioned to respond to the National Institute of Standards and Technology's (NIST) Request for Information (RFI).

In 2014, the Florida Legislature created the Florida Center for Cybersecurity (FC²) located at the University of South Florida (USF) to address this very concern. This unique organization was established to specifically address the concerns raised by Executive Order 13800 of May 11, 2017, "Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure," section 3.d - *Workforce Development*. Under this legislative mandate, FC² provides focus, organization, a cohesive workforce development strategy, and avenues for collaboration among the 12 universities in the State University System (SUS) which cover the entire state of Florida. FC² will coordinate Florida's commitment to meet the cybersecurity challenges of today, while preparing for the future.

Cyber attacks cost over \$400B a year in lost IP (Intellectual Property), downtime and recovery. The private sector and Government spend over \$200B per year protecting this infrastructure. Unfortunately, there are not enough trained professionals to combat this problem. In the US alone, this year, over 350,000 jobs will go unfilled due to the lack of cyber talent.

The FC² has the unique capability to rapidly and effectively coordinate across the SUS to leverage Florida's leading experts in cybersecurity workforce development, and showcase some of the areas in which Florida is leading the way in growing and developing the cybersecurity workforce.

There are multiple centers of excellence in cybersecurity across the State University System of Florida today including:

- USF (host institution for FC²) is a top tier research university with faculty focusing on a multitude of topics in cybersecurity,
- University of Florida (UF), a member of the Association of American Universities (AAU), supports a research center dedicated to cybersecurity,


- Florida Atlantic University (FAU) has a center dedicated to cryptography, a very essential science in cybersecurity,
- University of Central Florida (UCF) has developed educational and research programs in modeling and simulation of behavioral cybersecurity, and
- Collectively, FC² has enabled 43+ educational degree and/or certificate programs to activation in just the 12 state universities.

FC², working with the educational institutions across the state, is able to leverage the appropriate resources, faculty expertise, and tools to address educational and research challenges in cybersecurity. Since its inception, FC² has supported workforce development efforts through the development of multiple programs, and at various educational levels, across the state. FC² also supports multiple outreach programs to expand collaboration between government, the private sector and academia in the areas of cybersecurity workforce development and research.

FC², in coordination with the State University System (SUS), has prepared this response to the NIST's RFI. The information contained in this RFI response represents the views of the leading faculty and academic researchers in cybersecurity across the State of Florida, as well as views from leading cybersecurity practitioners. This comprehensive approach to cybersecurity is indicative of the FC²'s ability to lead the effort to build the cybersecurity workforce throughout the State of Florida and to meet the broader pressing needs of the nation.

The State University System of Florida is pleased to endorse this response, and appreciates the continued support of NIST and its efforts to address this critical issue affecting our nation.

Sincerely,



Marshall M. Criser III
Chancellor

Florida Center for
Cybersecurity
at the University of South Florida



July 27, 2017

To whom it may concern:

The cybersecurity workforce gap is one of the most pressing issues facing the world today. Various research studies and surveys point to over 1.8 million unfilled cybersecurity positions by 2022. This is an alarming and staggering number. With the explosion of the Internet of Things and the evolution toward a more connected society, the economy and security of our nation is at great risk. Without a strong cybersecurity workforce, we face the potential for billions of dollars in losses. One insurance firm recently stated that the cost of a large cyberattack could exceed the cost of Hurricane Katrina. There can be no doubt that cybersecurity plays a critical role in our lives for the foreseeable future.

Since its inception, the Florida Center for Cybersecurity (FC²) has been coordinating efforts among diverse stakeholders within the state of Florida to build a robust cybersecurity workforce. FC² is committed to making strategic investments in education, training, research and community engagement to make Florida a leader in cybersecurity. The Center's efforts have seen the launch and expansion of cybersecurity programs across the state. These efforts have created unparalleled collaboration and cooperation among the institutions of our State University System (SUS) as well as private industry, government and the military. Through these efforts, the Center will drive creation of the cybersecurity workforce required to meet the challenges facing the nation.

I am pleased to present this response to NIST's RFI. It represents input from many of the leading cybersecurity faculty and practitioners from across the state of Florida. FC² is pleased to be able to participate in the dialogue and provide insights on cybersecurity workforce development. FC² facilitated and coordinated this response, leveraging the thought leadership, innovation and practical experience in cybersecurity workforce development of experts from across Florida. As with any project, collaborative effort wins the day, and FC² exemplifies this by uniting the SUS institutions to build a stronger and larger cybersecurity workforce.

Sincerely,

Sri Sridharan

Director, Florida Center for Cybersecurity

Florida Center for Cybersecurity
4202 East Fowler Avenue, ISA 7020 • Tampa, Florida 33620-7120
(813) 974-2604 • FAX (813) 974-5580

Contents

- Preface I
- Acknowledgments 3
- I. General Information 4
- II. Current Metrics and Data for Cybersecurity Education, Training, and Workforce Development. 6
- III. Workforce Categories Specialty Areas, Roles, and Knowledge 7
- IV. Policies for Workforce Education and Training Efforts 8
- V. Employer Expectations and Valued Skills 9
- VI. Most Effective Workforce Development Programs in the US Today. 10
- VII. Challenges Facing the Nation Regarding Workforce Development 11
- VIII. The Effect of Technological Advancement on a Cybersecurity Workforce 12
- IX. Steps to Continue, Modify, or Discontinue Existing Programs 13
- X. Conclusion 16
- Appendix: The State University System of Florida 17

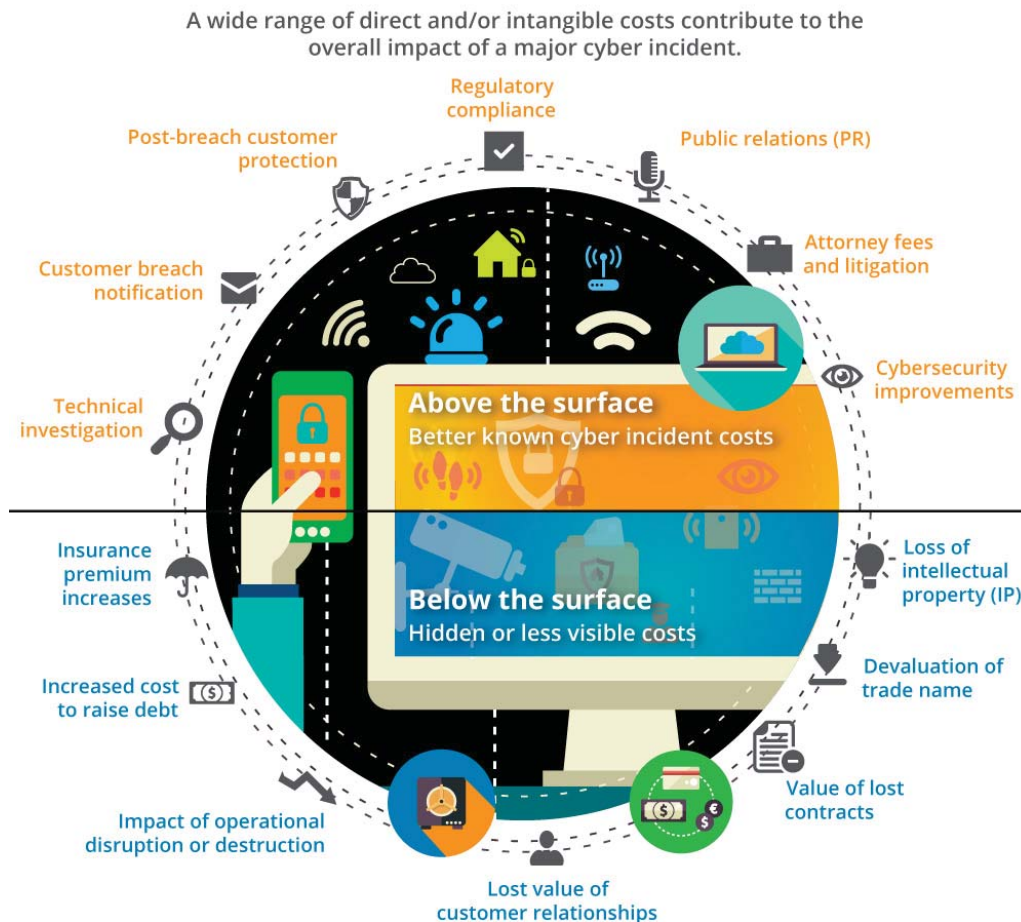
Preface

The problem facing our nation today and into the future: building the cybersecurity workforce.

The nation's critical infrastructure, along with the networks and services that power our economy, are at risk. Cyberattacks compromise our ability to protect intellectual property and put at risk the capital that fuels economic growth. They disrupt key networks and services, destroy critical systems and data, and undermine trust in our day-to-day transactions. These attacks threaten our advantage in cyberspace, and they come at an economic cost in terms of downtime and recovery.

Consequently, the private sector and the government invest almost \$100 billion per year in

new security technologies, solutions, and services. An equivalent amount is invested in internal security staff hires, a projected growth rate of over 15% per year for the foreseeable future. By 2020, total spend on external and internal support will approach \$250 billion worldwide. The private sector is driving innovation with an investment of over \$15 billion since 2012 in new start-ups—creating new security innovation hubs, public-private partnerships, and fueling entrepreneurship across the country. Cybersecurity is a critical and growing issue that impacts and permeates every segment of the global economy. Adding to the challenge for both the private and public sectors is the fact that there



is an inadequate labor supply and an escalating workforce need. Currently, over 700,000 people are employed in the field of cybersecurity in the United States, with an estimated gap of 350,000 in 2017. In Florida alone, there are over 25,000 job availability postings that exist for cybersecurity personnel—with positions in engineering, security operations, audit, and management.

In 2014, the Florida State Legislature directed the creation of the Florida Center for Cybersecurity (FC²) to work with the State University System (SUS) to position Florida as a national leader in cybersecurity. With that in mind, FC², in collaboration with the SUS institutions, has prepared this response—pooling the collective knowledge and perspective of our statewide partners to provide a comprehensive viewpoint on this critical topic. The responses indicate areas that



are working, areas that need improvement, and areas that are not effective, which should perhaps be discontinued. This document represents the findings of leading academic and practitioner researchers in cybersecurity workforce development. The responses indicate there are no silver bullets or shortcuts to creating the qualified workforce required to meet the demands of both today and the future. It is evident, however, that there are several indicatives in place that are

beginning to take root and support these efforts. By making appropriate strategic investment in cybersecurity workforce development, progress is being made, and FC² will continue to work collaboratively across the SUS to further develop and grow Florida's cybersecurity workforce.

The response to this RFI reflects the expertise of academic and professional experts from a majority of the universities that are part of the State University System of Florida. Collectively, their input provides a broad picture of the challenges and opportunities related to cybersecurity workforce development. It should be noted that Florida is unique in having a centralized hub in the Florida Center for Cybersecurity, which works across the State University System to facilitate collaboration between the public and private sectors. By connecting stakeholders from multiple private and public entities, FC² is the driving force in encouraging cross-sector partnerships focused on significantly growing Florida's cybersecurity workforce. This will be accomplished by supporting each SUS cybersecurity program's goals, providing incentives to encourage collaborative cybersecurity research, and expanding cybersecurity outreach programs. FC² will also support efforts to expand cybersecurity education programs at the K-12 level to further develop the cybersecurity talent pipeline as well as the ongoing expansion of veterans' training programs and initiatives focused on building information sharing and collaboration tools to support statewide cybersecurity programs.

Cybersecurity Skills Crisis

Too Many Threats

 **62%**
INCREASE
IN BREACHES
IN 2013¹

1 IN 5 
ORGANIZATIONS
HAVE **EXPERIENCED**
AN APT ATTACK⁴

US \$3
TRILLION
TOTAL GLOBAL
IMPACT OF
CYBERCRIME³

 **8 MONTHS**
IS THE AVERAGE TIME
AN ADVANCED THREAT
GOES UNNOTICED ON
VICTIM'S NETWORK⁸

2.5
BILLION 
EXPOSED RECORDS AS
A RESULT OF A DATA BREACH
IN THE PAST 5 YEARS⁵

Too Few Professionals

 **62%**
OF ORGANIZATIONS
HAVE NOT INCREASED
SECURITY TRAINING
IN 2014⁶

 **1 OUT OF 3**
SECURITY PROS ARE
NOT FAMILIAR WITH
ADVANCED PERSISTENT
THREATS⁷

 **<2.4%**
GRADUATING STUDENTS
HOLD COMPUTER
SCIENCE DEGREES⁹

 **1 MILLION**
UNFILLED SECURITY
JOBS WORLDWIDE⁹

83% 
OF ENTERPRISES CURRENTLY
LACK THE RIGHT SKILLS AND
HUMAN RESOURCES TO PROTECT
THEIR IT ASSETS¹⁰

Enterprises are under siege from
a rising volume of cyberattacks.

At the same time, the global demand for skilled professionals sharply outpaces supply. Unless this gap is closed, organizations will continue to face major risk. Comprehensive educational and networking resources are required to meet the needs of everyone from entry-level practitioners to seasoned professionals.

SOURCES: **1.** Increased Cyber Security Can Save Global Economy Trillions, McKinsey/World Economic Forum, January 2014; **2.** M-Trends 2013: Attack the Security Gap, Mandiant, March 2013; **3.** Increased Cyber Security Can Save Global Economy Trillions, McKinsey/World Economic Forum, January 2014; **4.** ISACA's 2014 APT Study, ISACA, April 2014; **5.** Increased Cyber Security Can Save Global Economy Trillions, McKinsey/World Economic Forum, January 2014; **6.** ISACA's 2014 APT Study, ISACA, April 2013; **7.** ISACA's 2014 APT Study, ISACA, April 2014; **8.** Code.org, February 2014; **9.** 2014 Cisco Annual Security Report; **10.** Cybersecurity Skills Haves and Have Nots, ESG, March 2014



Acknowledgments

FC² would like to acknowledge and thank the following contributing authors for their support in preparing this RFI Response.

University of Florida, Mr. Rob Adams

University of Central Florida, Dr. Bruce Caulkins

University of West Florida, Dr. Eman El-Sheikh

University of South Florida, Dr. Nasir Ghani

University of North Florida, Dr. Patrick Kreidl

Florida State University, Mr. Mike Russo

Florida International University, Dr. Himanshu Upadhyay

I. General Information

Are you involved in cybersecurity workforce education or training?

As the third most populous state in the nation, Florida is home to diverse demographics and population growth that has driven business relocation and/or expansion within the state. A state that previously saw its economic engine fueled by tourism and citrus production is rapidly evolving to a high-tech economy with growth in key industry sectors, including financial services, healthcare, insurance, and information technology services. With the shift to a more IT-focused economy, Florida has seen IT sector companies establish new business data centers in key metropolitan areas and the emergence of new 24/7 Security Operations Centers (SOCs) that provide continuous security monitoring. Now more than ever, this evolving landscape has driven the need for skilled cybersecurity professionals, a tech-savvy talent pipeline, and the services that are needed to protect growing data security needs and support business operations.

The Florida Center for Cybersecurity and the State University System of Florida

The Florida Center for Cybersecurity (FC²) was created by the Florida Legislature in 2014 to secure Florida's place as a national leader in cybersecurity. FC² is a statewide resource supporting and collaborating with all twelve institutions in the State University System (SUS). FC² serves as a centralized hub for creating connections, building partnerships, capitalizing on opportunities and encouraging collaboration among stakeholders in industry, academia, government and defense.

Consisting of 12 institutions, the State University

System serves more than 350,000 students and currently offers 75 baccalaureate and graduate programs directly related to computer science as well as numerous concentration and certificate programs at each level. With facility, equipment, faculty, and staff support for each of these programs, the state's comprehensive capacity to educate a cybersecurity workforce and produce thousands of graduates in this field is unparalleled.

Some of the SUS resources—beyond standard academic programs—devoted specifically to cybersecurity include:

- Florida State University's Cybersecurity Center for Research, Education and Policy
- Florida Atlantic University's Center for Cryptology and Information Security
- Florida Gulf Coast University's Cybersecurity Workforce Education Program
- Florida International University's Hemispheric Cybersecurity Forum
- Florida Polytechnic University's Cybersecurity Lab
- University of Central Florida's Center for Cybersecurity and Cybersecurity Labs
- University of Florida's Florida Institute for Cybersecurity Research
- University of West Florida's Center for Cybersecurity

Each of these initiatives provides additional capacity, cybersecurity educational programming, and research to not only the academic community, but government and private sectors as well.

FC² is strategically positioned to leverage these abundant resources. Rather than each of these institutions and units acting independently and/or competing with one another, they work together through FC² to provide an effective mix of educational programming and degree levels to meet the changing needs of industry and other stakeholders. FC² works closely with both public and private partners to assess their workforce needs and collaborates with institutions in the university system to align academic offerings accordingly.

This bridge between academia and industry also creates a pathway for joint research initiatives, internship opportunities, and dual-purpose programming to benefit current practitioners and students.

Since the creation of FC², the Center has made great progress by focusing on three operational pillars—Education, Research, and Outreach.

Education

FC² encourages and supports efforts to enhance and expand cybersecurity education programs at SUS institutions across the state to address cybersecurity workforce gaps. Major initiatives focused on growing the cyber talent pool include:

- Supporting cybersecurity curriculum and program development at SUS institutions
- Developing and supporting pipeline programs for veterans and K—12 students
- Facilitating collaboration and information-sharing between SUS universities through the SUS Advisory Council on Cybersecurity

Research

FC² supports efforts of SUS institutions to secure National Center of Academic Excellence designations, including USF's recent designation

as a National Center of Academic Excellence in Cyber Defense Research. The Center hosts an annual Research Symposium, bringing together industry, academic researchers from across the SUS, and students to share their work, learn about new cybersecurity research, and connect with fellow researchers from across Florida.

Outreach

FC² participates in and supports numerous events to build awareness and encourage dialogue on key cyber topics. Recent activities include an event, co-hosted with *The Christian Science Monitor Passcode*, for a discussion on ransomware and sponsorship of B-Sides Orlando 2017, a security event that connects industry veterans with new and aspiring cyber experts. The Florida Center for Cybersecurity's Annual Conference—its signature event—takes place at the Tampa Convention Center. The conference brings together technical and non-technical stakeholders from industry, government, academia, students, and the military to share information, network, explore ideas, and learn about emerging trends and today's hottest cyber topics.

FC² is led by a director who is a seasoned professional, a proven business leader and entrepreneur. The director is supported by a world-class Board of Advisors, with each member contributing significant experience in cybersecurity, intelligence, and other critical areas. The scope of their expertise includes business launch, research, mathematics, government, and technology.

The cyber threat landscape is constantly evolving and new technologies, tools and approaches continue to advance. The SUS and FC² are committed to leading the way toward the development of a robust cyber economy in Florida that is at the forefront in producing

new technologies and developing a statewide infrastructure that supports a growing talent pipeline—education of thousands—to ensure Florida’s economic future. Growth in advanced cyber research and applied research in leading technologies and methods to include cybersecurity in the cloud, advanced cryptography, continuous authentication, and machine learning, along

with development of high-impact programs, partnerships and other initiatives will be the focus in 2017–18 and beyond, thus demonstrating that we have the human capital, creativity, resources, and determination to make Florida “the cyber state”—a national model that other states will emulate.

II. Current Metrics and Data for Cybersecurity Education, Training, and Workforce Development

What current metrics and data exist for cybersecurity education, training, and workforce development, and what improvements are needed in the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs?

The National Security Agency (NSA) and Department of Homeland Security (DHS) jointly sponsor the National Centers of Academic Excellence in Cyber Defense Education (CAE-CD), Two-Year Education (CAE-2Y) and Research (CAE-R) and Cyber Operations (CAE-CO) Programs. These programs set the national standards and guidelines for excellence in cybersecurity education, training, and workforce development. The goal of these programs is to reduce vulnerability in our national information infrastructure by promoting higher education and research in cybersecurity and producing a growing number of professionals with necessary cybersecurity expertise.

All regionally accredited two-year, four-year and graduate level institutions in the U.S. are eligible to apply for the CAE-CD Program. Prospective schools are designated after meeting stringent CAE criteria and mapping curricula to a core set of cyber defense knowledge units. CAE-CD institutions receive formal recognition from the U.S. government as well as opportunities for

prestige and publicity for their role in securing our nation’s information systems. A list of CAE-CD designated institutions and additional program information is available at <https://www.iad.gov/NIETP/index.cfm>.

Complementary in nature, the CAE-Cyber Operations Program focuses on technologies and techniques related to specialized cyber operations (e.g. collection, exploitation, and response) to enhance the national security posture of our nation. A list of CAE-CO designated institutions and additional program information is available at <https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/>.

A variety of organizations publish reports that include data, metrics and recommendations on cybersecurity education, training and workforce development. The Partnership for Public Service and Booz Allen Hamilton published *Cyber In-Security: Strengthening the Federal Cybersecurity Workforce* (2009) and *Cyber In-Security II: Closing the Federal Talent Gap* (2015) identified findings and recommendations for attracting and retaining cybersecurity talent in the federal government. (ISC)² in partnership with Booz Allen Hamilton published biannual reports on information security, including the most recent 2017 (ISC)² *Global Information Security Workforce Study*, which

provide data and recommendations for growing the global information security workforce (2017).

According to a 2015 analysis from the Bureau of Labor Statistics, more than 209,000 cybersecurity jobs in the U.S. are unfilled, and postings are up 74% over the past five years (2015, <http://peninsulapress.com/2015/03/31/cybersecurity-jobs-growth/>). A recent ISACA report estimates that the global shortage of qualified cybersecurity professionals will reach 2 million by 2019 and Cybersecurity Ventures predicts 3.5 million cybersecurity job openings by 2021 (2017, <https://www.herjavecgroup.com/cybersecurity-jobs-report-2017-edition/>).

To enhance the collection, organization, and sharing of information about cybersecurity education, training, and workforce development programs, we recommend systematic expansion of the NSA/DHS National Centers of Academic Excellence (CAE) Program. This will increase the number of institutions offering high quality cybersecurity education and training programs and thus enhance cybersecurity workforce development. The NSA recently established a network of CAE National Resource Centers (CNRs) and CAE Regional Resource Centers (CRRs) to advance cybersecurity education and workforce development across the nation. This program will help increase the number of CAE-

designated institutions across the nation, enhance cybersecurity knowledge and skills of faculty at those institutions, and enhance collaborations that advance cybersecurity education, training, and research.

Partnerships among academia, government, and industry, along with dynamic tools are needed to facilitate the collection, organization, and sharing of up-to-date information about cybersecurity education, training, and workforce development. Such partnerships and tools can help educators and employers keep up with the rapidly changing landscape of cybersecurity jobs and workforce needs, and strategically strength our nation's workforce.

CyberSeek, a partnership between the National Institute of Standards and Technology (NIST) National Initiative for Cybersecurity Education (NICE), Burning Glass, and CompTIA, is a powerful tool that provides up-to-date, detailed, actionable data about supply and demand in the cybersecurity job market (2017, <http://cyberseek.org>). Such a tool can be enhanced in several ways to support and help expand workforce development initiatives. For example, expanding job categories to cover critical infrastructure and other emerging job needs and linking the tool to employment opportunities can take an already powerful tool to the next level.

III. Workforce Categories *Specialty Areas, Roles, and Knowledge*

Is there sufficient understanding and agreement about workforce categories, specialty areas, work roles, and knowledge/skills/abilities?

The NICE National Cybersecurity Workforce Framework (NCWF) defines a detailed and comprehensive set of categories (7), specialty areas

(32), and work roles (52). In particular, categories contain groups of specialty areas whereas work roles include detailed tasks and KSAs (knowledge, skills, and abilities). The intention is to guide a range of players in the cybersecurity field, e.g., employers, workers, students, educators, etc. This framework was developed after extensive

consultation and feedback from a wide range of partners and is quite detailed and comprehensive. Specifically, it covers roles across the entire cybersecurity job spectrum, e.g., design/implementation of cybersecurity systems, application and operation of cybersecurity systems, information collection and investigation activities, support and maintenance, and overall management and governance, etc. As such, this framework is very complete. However, the broader question is how widely accepted, and adopted) this framework is across the cybersecurity domain.

To address the above concern, a cursory scan can be done to check sample cybersecurity job listings on various websites (e.g. monster.com, indeed.com, wayup.com). Overall, this exercise shows that the NCWF categories are sufficient to detail the detailed roles and requirements

of each listing. However, the adoption of these exact NCWF categories and specialty areas by employers is not yet evident. For example, the above scan also indicates that most employers use different terminologies to define job roles and their associated skills sets. For example, the “Threat Analysis” specialty area in the NCWF has a much higher-level definition, whereas several job listings for “Threat Analyst” specify much more detailed networking-level protocol skill sets. Direct mention or reference to any of the NCWF categories is not found in any of the sampled job listings either. Similar observations are also noted for many sample governmental cybersecurity job listings, e.g., DoD, Department of Commerce, etc. Hence, there is still the need to develop a stronger consensus/harmonization of NCWF workforce categories between all key players (government, industry, educators, etc.)

IV. Policies *for Workforce Education and Training Efforts*

Are appropriate cybersecurity policies in place in your organization regarding workforce education and training efforts and are those policies regularly and consistently enforced?

In general, most university education/training policies appear to be targeted for the cybersecurity workforce (e.g., the university’s security professionals). For users and students, most schools do not have many cyber-related policies, but out of necessity provide limited internal education/training opportunities for the campus cyber workforce. Some schools also make opportunities available through formal contracted coursework for the cyber workforce, while other schools—especially those institutions affiliated directly with DoD—encourage participation in commercial certification courses in cyber-related

fields, partly due to the DoD mandate of cyber commercial certificates as shown in DoD Directive 8140.01.

Policies on cybersecurity education do exist in academia for specialized areas, such as in the HIPAA-covered environments; however, most of their training-related policies focus on cybersecurity awareness activities to prevent certain high-visibility attacks from occurring. Currently, phishing and ransomware attacks are two prominent examples of “just in time” cyber-awareness training made available within academic institutions today.

Academia has the unique situation where the normal balance between cybersecurity and the need to share information can be out of balance at times, since the school usually focuses on the

overriding need to share information broadly and easily. However, schools are moving toward better security by mandating more secure authentication and non-repudiation techniques to satisfy their responsibilities to defend and protect their students' and workers' information. Further, academic institutions that have direct working relationships with government entities have a more pressing need to secure their information and network connections.

With respect to students' privacy and rights, one federal law is particularly noteworthy: the Family Educational Rights and Privacy Act (FERPA) of

1974 protects student records privacy review and disclosure rights. The law guarantees these rights for both current and former students at all universities and colleges.

Additionally, FERPA specifies that faculty and staff in most circumstances may not disclose personally-identifiable information (PII) about students or release their educational records to third parties without receiving written and signed consent. PII examples include any data or information that includes the students' names, their parents' names, family members, and the students' social security numbers.

V. Employer Expectations *and Valued Skills*

What types of knowledge or skills do employers need or value as they build their cybersecurity workforce? Are employer expectations realistic? Why or why not? Are these expectations in line with the knowledge and skills of the existing workforce or student pipeline? How do these types of knowledge and skills vary by role, industry, and sector, (e.g., energy vs financial sectors)?

Cybersecurity touches every aspect of information technology. This relatively new field has not had the time or attention necessary to address the unusually large number of hacks and breaches. The result is a void of over one million vacant jobs seeking individuals with strategic and technical information security and privacy skills. Many of these skill sets do not require advanced degrees but employers are expecting a demonstration of knowledge in the form of international certifications offered by reputable organizations like (ISC)², ISACA, and PMI, etc. These certifications require rigorous exams and many years of experience in the field which tends to slow down the hiring process.



Some universities have begun to address this workforce shortage. Most continue to teach 90s curriculum and have not adapted to the new needs of the nation. On the other side, employers expect individuals that have the skills to solve major cybersecurity issues when they receive an advanced degree when, in fact, it takes much more. It requires a combination of people, processes, and technology. Although most cybersecurity skill sets are similar across industries and sectors, there is no single solution, and, as a result, cybersecurity must be approached strategically and comprehensively by considering policy, training, risk management, incident response, and survivability. Those focus areas linked with the right people provide a formula for success.

VI. Most Effective *Workforce Development Programs in the US Today*

Which are the most effective cybersecurity education, training, and workforce development programs being conducted in the United States today? What makes those programs effective? What are the goals for these programs and how are they successful in reaching their goals? Are there examples of effective/scalable cybersecurity, education, training, and workforce development programs?

There is an urgent need for a well-trained cybersecurity workforce in the government and private sectors. An effective cybersecurity education for undergraduate and graduate students, using a well-designed curriculum, is essential to meet this need. The emergence of the Internet of Things, which promises an unprecedented number of Internet-connected devices, makes the demand for cybersecurity education stronger than ever. This demand calls for not just an enhanced effort, but also a paradigm shift from traditional computer and information security education, which typically assumes that the hardware underlying the information systems is secure and trustworthy. Hence, there is a critical need to redesign cybersecurity curriculum such that the nation's STEM student population is ready to take on future cybersecurity challenges.

One example is Florida International University's cybersecurity program, termed Cyber Fellows. In this program, the fellows work with professors, scientists and researchers to develop cyber test technologies for DoD. They gain hands-on experience while performing research and developing test technologies. The Cyber Fellows publish papers/posters as well as participate in conferences to keep up with the trends in cybersecurity. The Cyber Fellows also participate

in 10-week summer internships at various DoD locations where they gain real-world industry experience.

Another example within the state of Florida is a scholarship program called SURPASS, a collaborative effort between two SUS universities, University of Florida (UF) and Florida International University (FIU). Both universities serve diverse student populations and offer strong internationally recognized hardware and systems security research programs, and extensive curricular offerings in cybersecurity, with the goal of addressing this need. Specifically, this program provides scholarships to encourage some of the best and brightest students in the state of Florida to pursue careers in hardware and systems security (HSS). We share these examples as demonstration of the positive outcomes that can be obtained when academic institutions pool their collective resources in support of the common objective of growing and enhancing the cyber workforce.

Currently, there are multiple online and classroom educational programs providing certifications, bachelor's degrees, and advanced degrees in cybersecurity. These programs provide training at beginner, intermediate, and advanced levels. Multiple SUS institutions are offering bachelor's-, master's- and Ph.D.-level programs in various areas of cybersecurity. Major courses offered through these programs include network security, malware analysis, ethical hacking, reverse malware engineering, fundamentals of cybersecurity, C++ programming, cyber forensics, data organization, and terrorism.

There are also various training and certification

programs available from Coursera, edX, and Udacity to learn about cybersecurity at various levels. In addition, private companies like New Horizon offer vendor-specific (e.g., Microsoft,

Cisco) cybersecurity training and certifications in addition to the certifications (e.g., CISSP, Security+, CompTIA) recognized by professional bodies.

VII. Challenges *Facing the Nation Regarding Workforce Development*

What are the greatest challenges and opportunities facing the Nation, employers, and workers in terms of cybersecurity education, training, and workforce development?

Cybersecurity education, training, and workforce development challenges and opportunities exist at all levels. The challenges are not just technical in nature; many issues arise from the behavioral, cultural, regulatory, and fiscal realms of cybersecurity. While our national K–12 education system is currently funded primarily by state and local governments, an increase in funding and direction by the federal government is needed with respect to cybersecurity training and education.

On an individual level, cybersecurity awareness, training, and education must occur early in his or her life. Continued and expanded support of the Science, Technology, Engineering, and Mathematics (STEM) initiatives need to continue at all grade levels. The STEM courses should have an expanded set of cyber-related curricula, focused on awareness and current threats in cyberspace. The STEM training should be persistent and consistent throughout the individual's life. This lifelong learning construct in cyber must continue unabated into the college years, where individuals are educated in the advanced cybersecurity concepts and current threats. This training should be mandated by all academic institutions.

On the corporate level, workforce development

and training in cyber are key components to success. Over time, the mandatory training in K–12 and in colleges and universities will allow corporations and public organizations, to focus less on current threats and cyber awareness as those subjects will be covered in school. Corporations and public organizations will now be enabled to focus their cyber-related training on targeted threats to their organizations and advanced level security measures and counter-measures needed to address those threats.

Information sharing is important as well, as private and public organizations need to be encouraged to share novel attack vectors seen and experienced with DHS and other governmental agencies. This is a cultural change of sorts, where these organizations have historically been reticent to share problems they have experienced in cyberspace.

A gap analysis report must be conducted at the federal level to determine the overriding needs and funding priorities at all educational levels. This report should look at “best of breed” accomplishments by various state and local organizations while highlighting the needs of schools in general. The report should also recommend funding targeted at local, state and federal levels towards needed solutions across the board. Finally, each state should be encouraged by the federal government to establish a cyber grading system that looks at each county's work in cyber education from K–12 and evaluates each

county's grade in accordance with the federal standards established.

A second gap analysis report must be conducted at the federal level to determine cyber workforce standards and needs in the public and private sectors. This report should focus on the job titles and descriptions for most cybersecurity workforce positions in order to establish a baseline of jobs that can be used in organizations nation-wide.

A federal vision for cybersecurity education and workforce development needs to be established in a similar fashion to the 2015 DoD Cyber Strategy document (2017, http://www.defense.gov/Portals/1/features/2015/0415_cyber-strategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf). The DoD Cyber Strategy established a requirement for the development of the cyber forces and structure within the DoD. The document also focused on

the building of cyber capabilities and workforce within the DoD to defend DoD networks, systems, and information. While the DoD Cyber Strategy is not a perfect template to use at a national level, it does provide some worthwhile insights on the strategy and capabilities that each state and local government, as well as employers, should focus on with respect to cybersecurity awareness and training.

To address these underlying issues, as a nation we must focus on the challenges in a holistic fashion. Cooperation must be expanded and in some cases, established between local, state, and federal entities and employers to support the need for cybersecurity awareness, training and workforce development. Cooperation between governmental agencies and private organizations with respect to information sharing needs to continue to grow and be supported at all levels.

VIII. The Effect of Technological Advancement on a Cybersecurity Workforce

How will advances in technology (e.g., artificial intelligence, Internet of Things, etc.) or other factors affect the cybersecurity workforce needed in the future? How much do cybersecurity education, training, and workforce development programs need to adapt to prepare the workforce to protect modernized cyber physical systems (CPS)?

In many instances, training, education, and workforce development are the first items cut when private and public sector organizations are looking for places to save money. This approach will adversely affect current and future cybersecurity workforce issues. We know that the cybersecurity workforce of today is not sufficient to address current needs or needs of tomorrow. That will be compounded in the future as we are faced with more complicated infrastructure and

technology.

Technology shows no signs of slowing down. In fact, it's a certainty that the pace will only increase. Security and privacy training must keep pace in order to meet future needs. How we equip and train our cybersecurity workforce will determine how well we protect the confidentiality, integrity, availability, and privacy of data.

In addition to technological training, cybersecurity education needs to take a multidisciplinary approach, including business, legal, ethical, and other "soft sciences" to prepare cybersecurity professionals for future challenges. Cybersecurity is a multidisciplinary science, and professionals of the future need to understand various facets of the field, from privacy concerns to business risk management and ethical implications. These

soft skills are as important as the hard technical skills. To quote leading cybersecurity educators at Harvard Extension School, “Security is not a technical thing. Security is a multifaceted thing that includes technology, design, law, privacy,

forensics, and much more. It’s everybody’s business.” (2017, <https://www.extension.harvard.edu/inside-extension/why-cybersecurity-skills-are-demand>).

IX. Steps to Continue *Modify, or Discontinue Existing Programs*

What steps or programs should be continued, modified, discontinued, or introduced to grow and sustain the Nation’s cybersecurity workforce, taking into account needs and trends? What steps should be taken

i. At the federal level?

In general, increased funding should be provided by federal agencies across the board to support a range of cybersecurity workforce training programs/initiatives. In particular, there is a clear need to expand university internship programs with industry. As noted, there are not enough internship openings for students [2]. Hence such programs must be expanded, and, as much as possible, they should work to place students in real network operation center (NOC) environments to accelerate transition. There is also a need to provide increased funding opportunities for Historically Black Colleges and Universities (HBCU) and Minority Serving Institutions (MSI) to diversify the pool of students receiving training in the cybersecurity field.

Furthermore, there should be an expanded push to build/introduce basic cybersecurity courses across all university degree programs as well as the middle and high school levels. Although state and local governments can be tasked with increasing support at those levels, federal funding will be critical. The development of online materials and courses should also be emphasized, as it will help increase the wider and faster adoption of related

courses between institutions (e.g. universities, school districts, etc).

Federal agencies should also work to build out new sources of talent, particularly from returning service members [2]. There have been some notable initiatives along these lines within the state of Florida (e.g. the New Skills for a New Fight collaboration between USF and JPMorgan Chase that fast-tracked veterans into entry-level cybersecurity jobs and the Army-funded P³ initiative at USF.) These type of initiatives should be launched and/or expanded at the national level with increased matching funds from industry.

Finally, federal government agencies should also mandate the use of NCWF specialty areas when detailing all government-related cybersecurity jobs (see response to question 2 as well). This approach will ensure consistency and clarity in defining job roles and also encourage the broader adoption of related lexicons in industry. However, further efforts to define/refine workforce categories should not be pursued since the current NCWF offerings are fully adequate.

ii. At the state or local level, including school systems?

Clearly there is still a strong need to attract more students to the cybersecurity field (as noted in many surveys by governmental and industry organizations). As a result, a much broader expansion of cybersecurity-related training is required at the K–12 level, both in terms of formal

courses and teacher training programs, as well as student competitions and summer internship programs. Moreover, some of these efforts should ideally start at the middle school level, e.g., high-level courses. Many federal agencies (NIST, NSF, NSA) already support summer training programs, such as Cyber Corps. In addition, some other training programs are also available, e.g., DHS-funded NICCS teacher training, nonprofit programs such as Hacker High School (by ISECOM), etc. However, there is an urgent need to support more formalized and expanded curriculum development activities now with the goal of introducing new middle and high school-level credit-earning courses in the cybersecurity area, as noted in [4]. In general, this will require both state and county-based governing bodies to provide increased funding (as well as federal agencies, noted in Part i).

iii. By the private sector, including employers?

Employers must provide increased training opportunities (e.g., internships and apprenticeships) for students, particularly at the university and also at the high school level. There is clearly a dichotomy. Namely, the demand for internships (from students) exceeds the number of such openings (from industry, government), whereas the number of full-time job openings for skilled cybersecurity professionals (for industry, government) exceeds the number of applicants for such openings [1]. Many employers have also indicated that university graduates lack “market-ready” technical skills to directly transition to key cybersecurity roles, e.g., in operations centers or system design. Hence the most meaningful way to address this talent shortfall is to rapidly expand internship training opportunities for students by providing more incentives for organizations to hire interns and more funding programs from federal agencies to support such efforts (with

matching efforts from industry). Of particular importance are “integration” training programs to help develop broader skill sets combining multiple cybersecurity tools and systems, e.g., automation, decision making, etc.

Employers also need to play a larger and more direct role in defining cybersecurity curricula at the university and even high school levels. Employers should assist with detailed skill assessment and knowledge gap analysis to identify shortcomings in existing training programs. These initiatives will help identify more relevant cybersecurity workforce training requirements. With this in mind, federal funding agencies should stress the need for very strong industry-based engagement components in any related proposal submissions.

Employers should also play a very active role in supporting cybersecurity training competitions at the local, regional, and national levels in terms of defining the challenges, mentoring students, judging competitions, etc. While some programs like this are already in place, additional funding should be provided to expand such activities in order to recruit industry organizations.

As noted in Part i, it is vital to attract returning service members into the cybersecurity field as well, as these candidates already possess very critical domain knowledge of governmental and defense networks and operations. As a result, industry organizations should be incentivized and/or encouraged to provide funding (to complement any federal funds) as well as critical hands-on training opportunities.

iv. By education and training providers?

Universities and colleges should move toward mandating introductory cybersecurity courses/training for students across all disciplines, e.g., engineering, business, arts and science, health,



sports, etc. Given the extremely broad footprint of cyberattacks, improved basic knowledge and readiness across the entire student body is now critical. In general, this approach will also help increase the interest and enrollment in cybersecurity-related courses and degree programs.

As noted in Part iii, universities should also continue to engage with industry organizations to better update/refine their cybersecurity curricula to ensure the relevance of program offerings. The establishment of industry review boards and use of industry-based course instructors should be heavily encouraged. Universities with established cybersecurity degree programs should also work closely with HBCU and MSI institutions to build and offer critical training programs to a more diverse student body.

Finally, industry training providers offering certification programs should be encouraged to cross-reference their certificates with the NCWF-listed categories and specialty areas. This referencing will help guide students with regard to which certificates they may require (or benefit from) when pursuing a particular job category of interest.

v. By technology providers

Technology providers developing cybersecurity tools and systems must also play a vital role

in future cybersecurity training efforts. These providers should be encouraged or incentivized to establish programs to offer free training and trial usage to academic institutions to provide early exposure to students. These organizations should also collect relevant student feedback to develop more streamlined/targeted product offerings for academic training support.

References

- [1] NIST Cybersecurity Workforce Framework (NCWF) <https://www.nist.gov/itl/applied-cybersecurity/nice/resources/nice-cybersecurity-workforce-framework> .
- [2] “Cybersecurity Workforce Shortage Projected at 18 Million by 2022,” (ISC)² Blog, February 2015.
- [3] “(ISC)² Delivers Recommendations to White House Chief of Staff,” (ISC)² Blog, April 2017, http://blog.isc2.org/isc2_blog/2017/04/isc2-cybersecurity-workforce-recommendations.html.
- [4] “Recommendations on Cybersecurity for the 45th President... Use More Hackers,” *Tech Crunch*, January 2017, <https://techcrunch.com/2017/01/20/recommendations-on-cybersecurity-to-the-45th-president-use-more-hackers/>.

X. Conclusion

Key Recommendations

Make significant financial investment to

- expand the NSA/DHS National Center of Academic Excellence (CAE) Program;
- expand and enhance the CyberSeek Program;
- broaden the consensus/harmonization of the NCWF workforce categories between all key players through marketing, collaborative workshops and industry outreach;
- approach cybersecurity education and training programs strategically and comprehensively by considering policy, training, risk management, incident response and survivability;
- expand federal government internship opportunities;
- expand federal scholarship programs for cybersecurity education;
- increase cybersecurity funding opportunities for Historically Black Colleges and Universities (HBCU) and Minority Serving Institutions (MSI);
- support efforts to establish or expand cooperation between local, state, and federal entities and employers to support the need for cybersecurity awareness, training and workforce development;
- expand funding and incentives for middle and high school cybersecurity educations, including formal courses, teacher training, student competitions and summer internship programs;
- expand and support cybersecurity training programs for military veterans;
- incentivize and encourage industry participation in cybersecurity workforce training programs;
- support or establish industry curriculum review boards for cybersecurity education programs;
- encourage industry certification programs be cross referenced with the NCWF; and
- incentivize technology providers to offer free training and trial uses to academic institutions to provide early exposure to students.

FC² and its State University System partners are pleased to submit this response to NIST's Request for Information regarding Developing and Maintaining the Cybersecurity Workforce. This response is the result of the collaborative effort between FC² and a majority of the SUS universities. It should be noted that Florida is the only state with a statewide infrastructure to proactively drive collaboration efforts focused on cybersecurity research, education, and community engagement with an overarching goal of advancing critical workforce development.

FC² and the SUS look forward to supporting NIST to develop programs that will enhance the growth of the cybersecurity workforce. Critical strategic investments made today will ensure future success in defending cyberspace. FC² and our SUS partners look forward to working with NIST to develop the programs, tools, and initiatives to build the cybersecurity workforce to meet the needs of the nation's public and private sectors, and we appreciate the opportunity to add our voice to this critical issue.

Florida Agricultural and Mechanical University (FAMU)

The Florida A&M University Center for Cyber Security (FCCS) recognizes that as technology advances and the world becomes more and more computer oriented, the tasks of Cyber Defense (CD) and Information Assurance (IA) become progressively more challenging. FCCS focuses on education, research and development for all aspects of information security, including systems vulnerability assessment, theory development and formalization methodologies, and mobile computing.

Florida Atlantic University (FAU)

The Center for Cryptology and Information Security (CCIS) was established in fall 2003 as the FAU College of Science. The center seeks and promotes collaboration with information technology industries of its region, and with federal and state government departments in the areas of information security. FAU is also recognized as a National Center of Academic Excellence in Information Assurance/Cyber Defense Research (CAE-R) for academic years 2014–2019.

Florida Gulf Coast University (FGCU)

Florida Gulf Coast University, located in Ft. Myers, officially broke ground in 1995. Envisioning a university that would use technology in learning and teaching to meet emerging higher education needs for the 21st century, Florida Gulf Coast University held its first commencement in May 1998 with 81 graduates. Today FGCU enrolls over 10,000 students and offers undergraduate and graduate degree programs.

Florida International University (FIU)

The Florida International University, principally through the School of Computing and Information Sciences, the Department of Electrical and Computer Engineering, and the Applied Research Center, as well as the College of Business has been at the forefront of cybersecurity and information security, as these fields have been in the cyber business since their inception. The National Security Agency has already recognized FIU's strength in cybersecurity by designating FIU as a DHS/NSA Center of Academic Excellence in Cybersecurity Education and also designating FIU as a DHS/NSA Center of Academic Excellence in Cybersecurity Research.

Florida Polytechnic University (FPU)

Florida Polytechnic University started as a university of engineering and technology. Florida Poly was established on April 20, 2012, as a wholly innovative university dedicated to the principle that innovation occurs when research and creativity are applied to real-world challenges. Florida's only public university for engineering and technology dedicated to science, technology, engineering and mathematics (STEM) was created to be both a rigorous academic institution and a powerful resource for high-tech industries.

Florida State University (FSU)

Florida State University has established research and education regarding cybersecurity, which includes computer and information security, computer forensics, computer criminology, privacy, behavioral assessment in information systems environment, trustworthiness in human computer interaction, cyberlaw, and policy

assessment. FSU is a National Security Agency (NSA)-designated Center of Academic Excellence in Information Assurance Education (CAE-IAE), among the first eight universities in the United States since 2000. FSU is the only CAE-IAE and CAE-R designated institution in Florida.

New College of Florida (NCF)

Located in Sarasota, New College began in 1960 as a small liberal arts college, graduating its first class in 1967. Separating from the University of South Florida to become an independent honors college in 2001, New College was the eleventh university in the State University System of Florida. New College has a student-to-faculty ratio of 10:1 and enrollment of just under 800 students.

University of Central Florida (UCF)

As one of the largest universities in the United States, the University of Central Florida (UCF) has long emphasized cybersecurity education, both in the technical and human sides of cyber. The Institute for Simulation and Training (IST) at UCF conducts a graduate certificate degree on the “Modeling and Simulation of Behavioral Cybersecurity.” The UCF College of Engineering & Computer Science (CECS) has an undergraduate Minor degree on “Secure Computing and Networks” (SCAN) to provide necessary cybersecurity education for undergraduates from Computer Science and other fields. UCF’s Collegiate Cyber Defense Competition (CCDC) team has won the National Collegiate Cyber Defense Competition in three consecutive years (2014, 2015, and 2016). Finally, UCF was designated as a National Center of Academic Excellence (CAE) in Cyber Defense Education (CAE-CDE) in 2016 and Research (CAE-R) in 2017 by the National Security Agency (NSA) and the Department of Homeland Security (DHS).

University of Florida (UF)

The University of Florida hosts The Florida Institute for Cybersecurity Research (FICS Research). FICS Research was established to be the Nation’s premier multidisciplinary research institute in the advancement of cyber security as a basis for long-term partnership and collaboration among industry, academe, and government. FICS Research’s mission is to directly support research needs of industry and government partners in a cost-effective manner with pooled, leveraged resources and maximized synergy and to enhance the educational experience for a diverse set of top-quality graduate and undergraduate students. FICS Research will advance knowledge and technologies in this emerging field and ensure commercial relevance of the research with rapid and effective technology transfer and establishing spin-off companies.

University of North Florida (UNF)

UNF’s educational offerings in cybersecurity are housed primarily in its School of Computing, starting formally in 2002 with the launch of an undergraduate concentration in Computer Security Administration. The School’s cybersecurity elective courses are growing in number and cybersecurity topics are being introduced earlier in the core curriculum. Faculty are also actively organizing the curriculum to align with the most recent NSA/DHS Center of Academic Excellence in Cyber Defense designation, and UNF expects to formally apply by 2018.

University of South Florida (USF)

The University of South Florida is the eighth largest university in the United States, and offers multiple options designed to meet the growing demand for cybersecurity professionals,

including the master's in cybersecurity, graduate certificates in cybersecurity and industry-recognized certifications. As a measure of research capabilities, the Intellectual Property Owners Association has ranked USF 10th in the world in the number of US utility patents granted. Researchers are creating new knowledge and advancing frontiers of cybersecurity, engineering, science, medicine and materials. USF is a designated NSA/DHS National Center of Academic Excellence in Information Assurance/Cybersecurity for academic years 2014–2019, and it was recently designated as a National Center of Academic Excellence in Cyber Defense Research. USF serves as the host institution for the Florida Center for Cybersecurity.

University of West Florida (UWF)

The University of West Florida (UWF) provides a unique, multidisciplinary approach to cybersecurity with a variety of undergraduate and graduate cybersecurity-related programs and certificates, and is consistently named a top “military friendly” university. UWF was designated as a National Center of Academic Excellence (CAE) in Cyber Defense Education by the National Security Agency (NSA) and the Department of Homeland Security (DHS) and, more recently, named as the NSA/DHS CAE Regional Resource Center (CRRC) for the Southeast US.