State University System
Education and General
2022-2023 Legislative Budget Request
Form I

University(s):	**University of West Florida**
Request Title:	**A Cyber Coast for Florida's Future**
Date Request Approved by University Board of Trustees:	**June 17, 2021**
Recurring Funds Requested:	**$15,260,921**
Non-Recurring Funds Requested:	
Total Funds Requested:	**$15,260,921**
Please check the request type below:	
Shared Services/System-Wide Request	□
Unique Request	☒

I. Purpose – *1. Describe the overall purpose of the plan, specific goal(s) and metrics, specific activities that will help achieve the goal(s), and how these goals and initiatives align with strategic priorities and the 2021 University Accountability Plan established by your institution (include whether this is a new or expanded service/program). If expanded, what has been accomplished with the current service/program?* 2. *Describe any projected impact on academic programs, student enrollments, and student services. University of Distinction proposals should also address the requirements outlined in the separate guidance document.*

The University of West Florida has received national recognition for taking on a critical challenge facing Florida and our nation – cybersecurity workforce readiness.

In 2014, the University established the UWF Center for Cybersecurity. In short order, the Center guided the University in becoming a National Center of Academic Excellence in Cybersecurity (CAE-C), as designated by the National Security Agency and Department of Homeland Security in 2016, and received the unique designation as the CAE-C Regional Resource Center for the Southeast U.S. in 2017. In this role, UWF provides leadership to advance cybersecurity education and workforce development across the Southeast, supporting colleges and universities in Florida, Alabama, Georgia, South Carolina, Mississippi and Puerto Rico. UWF's mission and role as the Southeast CAE-C Regional Hub expanded to include Kentucky, Mississippi, Tennessee, North Carolina and the U.S. Virgin Islands, and to enhance collaborations among academia, industry and government partners. UWF serves as one of five NSA CAE-C Regional Hubs across the country.

UWF's Center for Cybersecurity has moved quickly to establish programs of excellence and has been recognized by the NSA as a model for how universities should structure their cybersecurity programs. Noteworthy achievements include the following:

- Collaborating with the Hal Marcus College of Science and Engineering to establish Florida's first stand-alone B.S. degree in Cybersecurity and the first to be designated by the NSA as a National Center of Academic Excellence in Cyber Defense program.
- The Cybersecurity for All® (uwf.edu/cyberforall) program enhances cybersecurity workforce development. Through this program, UWF has enhanced cybersecurity workforce readiness for State of Florida personnel through partnerships with the Florida Digital Services, Florida Department of Management Services and the Florida Department of State.
- The Florida Cyber Range®, launched to enhance competency-focused, hands-on skills development via education, training and competitions.

Additional recognitions include:

- UWF was selected to lead the National Cybersecurity Workforce Development Program, a nationally scalable and sustainable cybersecurity workforce program to rapidly expand the number of qualified cybersecurity professionals. UWF is leading a coalition of 10 CAE-C designated institutions across the country in this initiative, including USF – Cyber Florida and FIU (cyberskills2work.org).
- The Cybersecurity for All® program was recognized among the 2020 Innovations in Cybersecurity Education by National CyberWatch Center.
- UWF received the NSF CyberCorps® Scholarship for Service grant to prepare undergraduate and graduate UWF students for cybersecurity work roles in executive federal agencies (uwf.edu/aces).
- The UWF Center for Cybersecurity Director, Dr. Eman El-Sheikh, was appointed as the higher education representative on the Florida Cybersecurity Task Force established by Governor Ron DeSantis.
- UWF recently highlighted its partnership with the National Security Agency to advance cybersecurity education at the 2021 RSA Conference, the premier security conference attended by more than 20,000 people across the globe (NSA press release, UWF press release).

The Opportunity

"Pensacola, Escambia County, and the Gulf Coast region have the unique opportunity to create the world's best public and private sector cyber partnership, making the 'Cyber Coast' a recognized world leader in

Cybersecurity." --Brig. Gen. Gregory J. Touhill USAF (ret), First U.S. Chief Information Security Officer 2016-2017

The recession-resilient cybersecurity industry is exploding in Northwest Florida. Growth is limited only by availability of talent. The cybersecurity skills gap and shortage of skilled workforce are well-known problems. A cybersecurity jobs heat map, Cyber Seek, currently indicates more than 464,420 unfilled cybersecurity jobs across the country, with more than 21,893 unfilled jobs in Florida.

Northwest Florida is ahead of the curve as an emerging area of strength in cybersecurity with a job market that is outpacing the national average. In Pensacola, Corry Station houses the Navy's Center for Information Warfare Training, a classified school for NSA military personnel, an expanding DHS Cybersecurity and Infrastructure Security Agency (CISA), which includes the National Cybersecurity and Communications Integration Center and supports state and federal government and critical infrastructure sectors. In Fort Walton Beach, Hurlburt Field has an education and training complex for Air Force Special Operations including cybersecurity. Many industry leaders in cybersecurity have offices and major contracts in Northwest Florida including Raytheon, Northrop Grumman, General Dynamics IT, Booz Allen Hamilton and Boeing Global.

With a significant increase in resources for cybersecurity talent development, UWF can be a catalyst for expanding the cybersecurity industry, attracting more high-wage jobs to the state, and winning national and global recognition for Florida's Cyber Coast.

The Plan

Building on UWF's established strengths and accomplishments, the University aims to advance Florida as the world's premier leader in cybersecurity workforce readiness and resiliency.

This will be accomplished through innovative and scalable academic and workforce development objectives as follows:

1. Create a UWF Department of Cybersecurity, the first such department in a Florida university, to expand multidisciplinary cybersecurity curricula and research.
2. Expand the UWF Center for Cybersecurity capabilities for education, workforce development, research and outreach.
3. Develop competency-focused and high-impact learning programs to prepare students for cybersecurity careers.

4. Target and incentivize diverse populations for cybersecurity careers and workforce development, including veterans and underrepresented groups.
5. Implement programming for cybersecurity career readiness, student success and timely completion.
6. Facilitate a cybersecurity community of practice and partnerships to expand career readiness and pipelines.

The Specifics

1. **Create a UWF Department of Cybersecurity to expand multidisciplinary cybersecurity curricula and research**

In order to build and support the needed multidisciplinary curricula and research, the university requires cybersecurity faculty and staff who not only understand industry needs, but are flexible and resilient to the fast-paced changing nature of Cybersecurity. A multidisciplinary Cybersecurity program means that faculty should be recruited outside of Computer Science and Information Technology, where Cybersecurity programs are typically housed. Thus, a Department of Cybersecurity can provide the means to better build multidisciplinary curricula and better recruit multidisciplinary faculty, which are necessary to meet the state's cyber workforce needs.

The college currently has a B.S. degree program in Cybersecurity and a M.S. degree program in Cybersecurity, both of which are BOG programs of strategic emphasis. With a Department of Cybersecurity, UWF will have the capability to expand the degree programs to include security management, critical infrastructure security, homeland security, and other non-technical areas of Cybersecurity.

The multidisciplinary curricula will also include high impact practices. Therefore, we propose updating and expanding the UWF Battle Lab. The Battle Lab is a high-tech computing lab that supports student engagement, research, and outreach in network and system security.

We additionally propose creating a Cyber-Physical Systems lab and a Cyber Forensics lab for the curriculum. The Cyber-Physical Systems lab will introduce students to the Internet of Things devices, critical infrastructure, and sensor and communication systems which all interface the digital and physical domains. The Cyber Forensics lab is an environment where students investigate advanced cyber-crimes and the analysis and prevention of next-generation malware attacks.

The Department of Cybersecurity will support a Cybersecurity Honors program. High-impact practices such as undergraduate research experiences will also be required of honors Cybersecurity students. This program will produce honors Cyber graduates who are in high demand by employers and graduate schools.

To meet overall cybersecurity workforce needs, we propose to increase Cybersecurity and Cyber-related program enrollment – from approximately 900 students to over 1,600 students during a 5-year period. The resources needed to dramatically increase program enrollment, to support student success, and for UWF to become the premiere institution for Cybersecurity education are:

- Faculty and staff for a Department of Cybersecurity.
- Faculty to support an increase in sections of lower division courses and other courses impacted by Cybersecurity.
- Staff to support college infrastructure impacted by Cybersecurity.
- Success initiatives aimed at cybersecurity and cybersecurity-related students (see section 3).

2. Expand the UWF Center for Cybersecurity capabilities for education, workforce development, research and outreach

To address the demand for a well-qualified cybersecurity workforce for our region and state, UWF launched several workforce development programs, including the Cybersecurity for All® Program. This program significantly expands the cybersecurity workforce across the state and nation, and increases the number of qualified cybersecurity professionals, including among under-served and under-represented populations. The Program's innovative approach emphasizes:

- Development and delivery of core cybersecurity courses that align with the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework.
- Development of additional courses and modules to customize the program for various audiences, including K12 students and teachers, businesses, government agencies, military and veterans, and for emerging needs, including critical infrastructure security, cloud security, Internet of Things security, industrial control systems security, threat intelligence and hunting, and AI and machine learning for cybersecurity.
- Online delivery of these education and training programs and courses that includes virtual, hands-on learning experiences using the Florida Cyber Range®.
- Development of pathways for students who complete these courses to cybersecurity careers and degree programs.
- Expansion of the Cybersecurity Ambassadors program to increase cybersecurity awareness, interest and skills among diverse populations and build a strong, diverse talent pipeline.

The Florida Cyber Range® provides cutting-edge competency-focused hands-on training and operations to detect and defend against cyber threats and attacks.

The Florida Cyber Range provides a state-of-the-art, powerful, realistic training environment to support cyber exercises, operations and competitions for government, military and academia, and facilitate the development and testing of innovative cyber threat detection, defense and response solutions.

Through the Cybersecurity for All® Program, the UWF Center for Cybersecurity partnered with the Florida Digital Services and Department of Management Services to provide cybersecurity training for state personnel and enhance cybersecurity skills and resiliency across state agencies. The Center also partnered with the Florida Department of State to provide training for elections supervisors and IT personnel and enhance elections security, providing training in four major Florida cities to elections personnel from all counties ahead of the 2018 elections.

Continued investment in this program will allow us to continue to enhance cybersecurity preparedness, expand the cybersecurity workforce across the region, state and nation, and increase the number of qualified cybersecurity professionals.

Our region is also home to expanding NSA, DHS/CISA, Air Force and cybersecurity operations. UWF is seeking to expand UWF Center for Cybersecurity programs to support growing cybersecurity defense operations in Northwest Florida and increase program and certification offerings to diverse populations, including transitioning military members, veterans, women and under-represented minorities seeking to get into or improve their skills in the cybersecurity industry.

The UWF Center for Cybersecurity will establish a national best-practice model for workforce development by designing and delivering high impact learning practices through competency-focused, learner-centered, modular curricula. Educating and training existing and future workforce will involve:

- Designing and delivering competency-focused modular courses and scenario-based learning activities through Cybersecurity for All.
- Cutting-edge research incorporated into these courses.
- Using the Florida Cyber Range to integrate real-world, cyber attack and defense scenarios into learning experiences.
- Designing, developing, and offering competition-based activities to develop and enhance competencies for cybersecurity jobs.
- Designing and delivering courses for veterans and other under-represented groups to provide opportunities for them to enter, advance and prosper in cybersecurity work roles.
- Creating cybersecurity courses and competitions using the Florida Cyber Range for state and local government and small and medium businesses to assess their cyber readiness.

- Establishing an educational Security Operations Center with cutting edge software and hardware solutions that will attract local and regional businesses, government contractors and defense agencies to collaborate with UWF Center for Cybersecurity.

We propose the development of an immersive learning lab that will utilize virtual environments and artificial intelligence to enhance learning outcomes through adaptive student-centered educational experiences. A research lab will be established to enhance collaborations among UWF, SUS and other faculty that emphasize current, emerging and future cybersecurity technologies such as critical infrastructure protection, artificial intelligence, machine learning, quantum computing, grid infrastructure, autonomous surface and aerial vehicles, block chain technology, healthcare devices, IP protection and renewable energy security.

We will develop a national-level resource for scientific inquiry into cyber adversary tactics, techniques and procedures. The proposed architecture will allow multi-disciplinary study of cyber adversaries without requiring everyone have highly technical cyber expertise. This resource will attract cybersecurity researchers to UWF and Florida SUS institutions, encourage them to join or collaborate with UWF, enhance our position within the cybersecurity community and establish UWF as a national hub for cyber adversary research. This in turn will attract graduate and undergraduate students to the area who will, upon graduation, fill highly sought after cyber workforce roles.

3. **Develop competency-focused and high-impact learning programs to prepare students for cybersecurity careers**

The Cybersecurity for All program will leverage UWF's strong track record and national recognition in high-impact practices (HIPs) to enhance cybersecurity career readiness. Students will work on research projects with UWF faculty and industry mentors, and will engage in other HIPs, including internships, professional conferences, cyber competitions and competency-based skills development activities. UWF was one of the institutions selected to participate in the National Centers of Academic Excellence Pilot Program for developing and assessing competency-focused activities.

UWF offers several programs to encourage and support undergraduate and graduate research, including research support for students and faculty. UWF has strong research activities in a variety of cybersecurity research topics. Students will develop essential competencies and skills through hands-on activities using the UWF Battle Lab and the Florida Cyber Range. Students will participate in range-based exercises and cybersecurity competitions, which are critically important for cybersecurity career readiness. The activities will be mapped to competencies that align with the NICE Cybersecurity Workforce Framework work roles and CAE Knowledge Units.

4. Target and incentivize diverse populations for cybersecurity careers and workforce development including veterans, women and underrepresented groups

In order to reach a total enrollment of over 1,600 students in cybersecurity or related programs, UWF proposes the following:

- Offer multi-year scholarships to FTIC students to attend UWF to major in Cybersecurity or a Cyber-related field.
- Establish 2+2 articulation agreements within Cybersecurity and Cybersecurity-related areas with Florida and Alabama community and state colleges.
- Establish 2+2 articulation agreements with the military.
- Offer transfer students majoring in Cyber or Cyber-related programs 2-year scholarships.
- Provide students in Cyber or Cyber-related programs an opportunity to either complete an industry certification, an internship, an undergraduate research project in areas of Cybersecurity, or another high-impact activity.
- Express admit each student in the program with a 3.0 GPA or better to their UWF online graduate program of choice.

The UWF Center for Cybersecurity developed the Cybersecurity for All program to provide training and workforce development opportunities to individuals and organizations, including military, veterans, industry and public sector. The Center will recruit veterans, women and underrepresented minorities from the area to participate in the Cybersecurity Fundamentals course offered through the Cybersecurity for All program and host events to provide awareness of the growing cybersecurity career opportunities in the area and attract them to UWF undergraduate and graduate cybersecurity programs. Veterans are very highly employable by the government, especially by DHS, CISA, DoD, NSA, FBI and CIA, as many of them have active, or can readily obtain, clearance. Attracting this population to UWF and providing them with foundational cybersecurity knowledge, skills, abilities and competencies will create a growing pipeline of future cybersecurity workforce. UWF is well suited to serve this population as we are ranked fifth in the nation as a military-friendly university and have a robust Military and Veterans Resource Center for military, dependents and veteran students.

5. Implement programming for cybersecurity career readiness, student success, and timely completion.

Northwest Florida's lagging economy, high poverty and low educational attainment rate translate to many regional students who are highly capable, but severely financially disadvantaged, ethnically underrepresented and often first-generation in college. Financial assistance alone is not enough. Students must be engaged early and often to increase persistence, particularly during their first year. Thus, building a talent pipeline to the cybersecurity workforce requires coordinated, multipronged efforts to mentor, teach, prepare and engage specific student populations. Student engagement programs at UWF are founded on nationally-recognized model programs incorporating four key components:

- Academic and social integration,
- Knowledge and skill development,
- Support and motivation, and
- Monitoring and advising.

Faculty and staff resources are crucial to build programs that engage students early and often. Engagement and mentorship must occur inside and outside of the classroom. Thus, a low faculty to student ratio is critical. The requested positions will support UWF's scope of expansion, which includes:

- Increasing the STEM LLC to include a multidisciplinary Cyber LLC
- Hosting annual boot camps to prepare students for their general education
- Building skills courses within Cyber and Cyber-related programs
- Offering a two-semester sequence STEM for Life Seminar for all STEM FTIC students to ensure FTIC students (including each cyber student) are engaged throughout their first year, which includes a common read and semester themes of College Survival Skills and Maximizing/Getting Involved in College
- Redesigning other key STEM gateway courses, that impact Cybersecurity and Cybersecurity-related programs, to improve pass rates, and
- Engaging more students in undergraduate research

6. Facilitate a cybersecurity community of practice and partnerships to expand career readiness and pipelines

The program aims to develop a superior cybersecurity workforce through the creation of a scalable and sustainable community of practice. UWF will establish a Cybersecurity Alliance that brings together academia, government and industry to expand the cybersecurity workforce across the state and nation by disseminating best practices and engaging employers. Students will be encouraged to participate in the community of practice events to enhance professional and leadership development and career readiness. UWF will develop and expand the Cybersecurity Alliance, disseminate best practices, and engage additional employers across the state to build a scalable and sustainable community of practice and expanding cybersecurity workforce.

The program aims to increase the participation of women and underrepresented students through mentoring by cybersecurity faculty and professionals, K12 outreach and community engagement. UWF launched and coordinates the Women in Cybersecurity (WiCyS) Florida Affiliate. Women cybersecurity professionals and WiCyS Florida members will be recruited to serve as career mentors for female students in the program. These mentors will provide guidance on career readiness and success and professional development and host regular networking and mentoring events. Existing K12 and community outreach initiatives, including the UWF Cybersecurity Ambassadors program, will be leveraged. The Ambassadors visit local area schools to enhance and promote cybersecurity awareness and UWF cybersecurity programs.

The program will involve several outreach activities to enhance cybersecurity workforce development across the state, which are outlined below:

- Annual Cybersecurity Career Fair to promote interest in cybersecurity careers, connect with employers, and learn about job and internship opportunities.
- K12 school visits and events to promote interest in cybersecurity programs and careers.
- Annual Florida Cyber Defense Competition.
- Florida Women in Cybersecurity Affiliate events across the state and annual Florida Women in Cybersecurity Conference.

Key Partners

The proposed initiatives will involve collaborations with key partners, including but not limited to:

AFCEA	AppRiver & Zix
BAE Systems	Booz Allen Hamilton
Corry Station	Defense Information Systems Agency
Department of Homeland Security / Cybersecurity and Infrastructure Security Agency	Department of Defense
Eglin Air Force Base & Air Force Research Labs	Florida Chamber of Commerce
Florida Department of Education	Florida Department of Law Enforcement
Florida Department of Management Services / Florida Digital Services	Florida Department of State
Florida Institute for Human & Machine Cognition	FuelTrust
FloridaWest Economic Development Alliance	Global Business Solutions Inc.

General Dynamics Information Technology	Hurlburt Field
Hixardt Technologies	IBM
IT Gulf Coast & ITEN WIRED	Jacobs
KPMG	KPMG
National Flight Academy	National Security Agency
Naval Air Station Pensacola	Naval Education and Training Command
NAVSEA and Naval Surface Warfare Center	Navy Center for Information Warfare Training & Command
Navy Federal Credit Union	Navy Information Operations Command
Networks of Florida	Northrop Grumman
Raytheon	Regions
Space Florida	Trend Micro

II. Return on Investment - *Describe the outcome(s) anticipated, dashboard indicator(s) to be improved, or return on investment. Be specific. For example, if this issue focuses on improving retention rates, indicate the current retention rate and the expected increase in the retention rate. Similarly, if the issue focuses on expanding access to academic programs or student services, indicate the current and expected outcomes. University of Distinction proposals should also address the requirements outlined in the separate guidance document.*

UWF's *A Cyber Coast for Florida's Future* proposal will significantly enhance cybersecurity workforce and economic development in Florida, and will establish Florida as a national leader in cybersecurity workforce development, resiliency and innovation. The Program will establish innovative, sustainable and scalable workforce development models and support the growth of qualified cybersecurity professionals.

The Program has many anticipated benefits, including:

- Increased number of qualified cybersecurity professionals across the region, state and nation
- Increased number of cybersecurity professionals with industry certifications needed for defense work roles
- Increased engagement in cybersecurity careers
- Increased number of students and professionals with core cybersecurity knowledge, skills and competencies in alignment with the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework

- Increased number of students enrolled in cybersecurity courses and degree programs, including under-served and under-represented populations and minorities
- Increased number of pathways for students to pursue postsecondary cybersecurity education at UWF and other Florida institutions
- Increased cybersecurity awareness among K12 students and teachers
- Enhanced workforce development and economic development across the state
- Enhanced cybersecurity protection and resiliency
- Expanded multidisciplinary cybersecurity courses and programs that include innovative curricula and hands-on learning activities
- Enhanced visibility for Florida as a leader in cybersecurity workforce development and resiliency
- Expanded partnerships among business, government, military and educational partners

Key Metrics

- **Year-one accomplishment or success**
  - Establish Multidisciplinary Cybersecurity degree programs and Department of Cybersecurity
  - Increase enrollment to 300 B.S. cyber, 100 M.S. cyber and 690 cyber-related degree programs; award 50 B.S. cyber degrees, 35 M.S. cyber degrees, and 175 cyber-related degrees
  - Provide cybersecurity training courses for 240 industry and government personnel, industry certifications for 60 personnel, and an intensive cybersecurity workforce program for 60 veterans and under-represented minorities

- **Return on investment to the state**
  - Years 2 – 5: Enrollment in B.S. Cyber, M.S. Cyber, and Cyber-related degree programs increased to 1600; awarded degrees for Cyber and Cyber-related programs increased to 540
  - Years 2 - 5: Provide cybersecurity training courses for 240 industry and government personnel, industry certifications for 60 personnel, and an intensive cybersecurity workforce program for 60 veterans and under-represented minorities per year

- **Program improvement over time**
  - Increase number of degrees awarded in Cyber and Cyber-related programs to 540
  - 50 percent of graduates of Cyber and Cyber-related programs received industry certification

    - Increase number of qualified cybersecurity professionals in years 1 – 2 to 230, and in years 3 – 5 to 285

- **Program elevation to excellence and prominence**
    - NSA Centers of Academic Excellence (CAE) Cyber Defense designation for B.S. in Cybersecurity program (maintain)
    - NSA CAE Regional Hub for the Southeast U.S. (maintain)
    - NSA CAE Cyber Defense designation for B.S. in IT program (achieve)
    - NSA CAE Cyber Defense designation for M.S. in Cybersecurity program (achieve)
    - ABET accreditation for B.S. in Cybersecurity and IT programs (achieve)
    - NSA CAE Cyber Operations designation for B.S. in Cybersecurity program (achieve)

Additional Metrics

1. Increase Enrollment in Cybersecurity and Related Programs

Program	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27
Cybersecurity, Bachelor's	221	300	365	410	450	500
Cybersecurity Master's	68	100	140	180	220	250
Other Cyber/IT programs	662	690	730	770	810	850

2. Increase Degrees Awarded in Cybersecurity and Related Programs

Program	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27
Cybersecurity, Bachelor's	50	66	88	105	130	160
Cybersecurity Master's	35	50	65	85	105	130
Other Cyber/IT programs	150	165	185	205	225	250

3. Increase the Number of Qualified Cybersecurity Professionals (certifications and trainings)

Program	2021-22	2022-23	2023-24	2024-25	2025-26	2026-27
Cybersecurity for All training	240	240	240	240	240	240
Cybersecurity Industry Certifications	60	60	60	60	60	60
Cybersecurity Veterans Program	30	30	30	30	30	30
Total	330	330	330	330	330	330

The Program will also contribute to the following Performance-Based Funding Metrics in the 2020 UWF Accountability Plan:

- Percent of Bachelor's Graduates Enrolled or Employed ($25,000+)
    - The Program provides dynamic training options that meet state and national workforce needs and allow faster transition to the job market.
- Median Wages of Bachelor's Graduates Employed Full-time
    - Cybersecurity jobs command high salaries, averaging approximately $80,000 for entry-level positions.
- Percentage of Bachelor's Degrees Awarded within Programs of Strategic Emphasis
- Percentage of Graduate Degrees Awarded within Programs of Strategic Emphasis
- Percent of Baccalaureate Graduates Completing 2+ Types of High Impact Practices

III. Personnel – *Describe personnel hiring and retention plans, making sure to connect both plans to initiative(s) and goal(s) described in section I. State the amount of faculty FTE and staff FTE and estimated funding amounts used for retention and new hires in each category. In describing faculty hires, provide overall hiring goals, including academic area(s) of expertise and anticipated hiring level (e.g. assistant professor, associate professor, full professor. Please describe how funds used for faculty or staff retention will help the institution achieve its stated goals. University of Distinction proposals should clearly note how anticipated hires or retained individuals will help the institution elevate a program or area to national or state excellence.*

To establish a Department of Cybersecurity, we propose to hire one Department Chair at the full professor, two associate professors, six assistant professors, and two instructors. The goal for the Chair position is to hire a faculty who has (1) an established record teaching and research in concert with the multidisciplinary aspects of Cybersecurity, (2) implemented high-impact practices in the cybersecurity classroom and laboratories, (3) a record of student-involved and student-led research, and (4) has the vision and leadership skills to build degree programs that intersect with Engineering, Business, Health, Law, and Ethics. At the Associate level, our goal is to hire faculty who have an established record of multidisciplinary collaborations in teaching, research, and external funding. Our goal at the Assistant level is to hire faculty who have a cybersecurity background and show promise to work in multidisciplinary domains. Specifically, our goal is to hire a cybersecurity professional at the Assistant level in each of the following domains: Engineering, Business, Health, Law, and Ethics. Another overarching goal is to hire faculty with a background in Cyber-Physical Systems or Cyber Forensics in order to build the labs being proposed and to engage students in these activities.

We also propose to hire staff for the new Department of Cybersecurity. Our goal is to hire two Office Administrators, two ITS specialists to cover an increased demand on the college's IT infrastructure (Data Center, servers, Battle Lab, etc.), three academic advisors to accommodate enrollment growth, one coordinator to oversee student high-impact opportunities, and one Director for the STEM Living Learning Community to include Cybersecurity population. Another goal is to hire an Admissions coordinator and a Financial Aid coordinator to oversee the admissions process for increasing enrollment in Cybersecurity and Cyber-related areas and to oversee the distribution of scholarship aid for Cybersecurity and Cyber-related students respectively.

One of the goals of this proposal is to raise annual enrollment in Cybersecurity and Cybersecurity-related degree programs to 1600 in five years. These degree programs are supported by the Departments of Mathematics and Statistics, Physics, Computer Science, and Information Technology. To accommodate the enrollment growth in Cyber-related programs, our goal is to hire two Computer Science/Information Technology faculty at the Assistant level. To accommodate the enrollment growth in math and physics general education courses, our goal is to hire two Math faculty at the instructor level and two Physics faculty at the instructor level.

The positions outlined above will help the university build a Department of Cybersecurity and to increase enrollment to 1600 students. The positions will also help cover the demands placed on departments that support Cybersecurity.

In order to expand retention efforts for Cybersecurity and Cyber-related students as outlined in the proposal, our goal is to hire three academic advisors (stated above) and three academic support faculty, with all three faculty at the Assistant level. These positions, as well as the staff positions, are needed to keep students on track to graduate, increase participation in the STEM Living Learning Community, create boot camps, redesign key STEM gateway courses, and engage students in research, internships, certifications, and other high impact practices. These positions will allow the college to engage students early and often and are known in the literature to increase student retention.

In total, our goal is to hire 20 faculty FTE and11 staff FTE. We propose to hire according to the following plan:

Position	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Chair	1					1
Associate	2					2
Assistant	2	2	3	1		8
Instructors	2	2	1	1		6
Academic Support Faculty	1	2				3
Office Administrator	2					2
Advisor	1	1	1			3
ITS Specialist	1	1				2
Coordinator/Director	1	1				2
Admissions Coordinator	1					
Financial Aid Coordinator	1					

To expand the UWF Center for Cybersecurity capabilities for education, workforce development, research, and outreach, we propose to hire seven full professors, and two instructors. The goal is to hire three teaching faculty who have (1) established record teaching cutting-edge topics and multidisciplinary aspects of Cybersecurity, (2) implemented competency-focused, high-impact practices in cybersecurity courses, including cyber range exercises and competitions, (3) successful record of student engagement, (4) demonstrated experience in developing and delivering cybersecurity courses that align with the NIST National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, and (5) have vision to build unique competency-focused certificate programs that build pathways to career and/or degree programs. In addition, four research faculty will be hired who have (1) established record in cutting-edge and multidisciplinary Cybersecurity research, (2) demonstrated success in research external funding, grants, publications, and technology transfer, (3) record of student-engagement in research, (4) demonstrated success in leading research collaborations with academic, industry and government partners, and (5) have vision to develop innovative and collaborative solutions that advance the field and enhance state and national cybersecurity. Two instructors will also be hired to support the Cybersecurity for All Program and Immersive Learning Lab, and expand education, training and industry certification courses for broader audiences. Target areas of expertise include critical infrastructure security, cloud security, Internet of Things security, industrial control systems security, threat intelligence and hunting, and AI and machine learning for cybersecurity. The overall goal is to establish a strong faculty and instructor foundation to support the proposed programs and research, and develop best practice models and resources that could be shared with faculty at other SUS institutions.

We also propose to hire staff to support the proposed goals and expand the programs offered by the Center of Cybersecurity. To accomplish the proposed goals, one Business Developer, one Communications Director and one Marketing Specialist will be hired to support program recruitment of diverse populations, expand strategic collaborations with private and public sector partners, and enhance community impact, outreach and visibility. In addition, the expansion of the Center for Cybersecurity data center, Florida Cyber Range, immersive teaching lab and research, development and testing lab will require the hiring of one Chief Technology Officer and one Server System Administrator to support the infrastructure, technology and tools needed for education, research and outreach activities. We propose to hire one Training Manager to plan, manage and evaluate online, hybrid and face-to-face education and training offerings, including training and workforce development courses, industry certification courses, range-based exercises and workshops, and cybersecurity competitions. Increases in course offerings, workforce and training programs, research activities, and community outreach will require additional support staff. We propose one Coordinator to assist with program coordination, delivery and evaluation, one Advisor II to support student success and enrollment growth for diverse participants, including transitioning military, veterans and under-represented minorities, and one Office Specialist to support the increased administrative support across all programs.

The Center for Cybersecurity proposes to provide education and workforce development opportunities for 330 learners annually, including training courses for 240 industry and government personnel, industry certifications for 60 personnel, and an intensive cybersecurity workforce program for 60 veterans and under-represented minorities, for a total of 1650 qualified cybersecurity professionals over a 5-year period.

Faculty and staff resources are crucial to build programs that engage students early and often. To expand the efforts of the Cybersecurity for All program in providing education and workforce development opportunities to individuals and organizations, including military, veterans, underserved and underrepresented communities, industry, and the public sector; the Center proposes to hire the positions listed above. Attracting this population to UWF and providing them with foundational cybersecurity knowledge, skills, abilities, and competencies will create a growing pipeline of future cybersecurity workforce for our state and nation.

In total, our goal is to hire 9 faculty FTE and 9 staff FTE according to the following plan:

Position	Year 1	Year 2	Year 3	Year 4	Year 5	Total
Professor/teaching	2					2
Professor/research	1	4				5
Instructor	1	1				2
Assoc Dir/Business Development	1					1
Chief Technology Officer	1					1
Training Manager	1					1
Communications Director	1					1
Marketing Specialist	1					1
Coordinator		1				1
Advisor II		1				1
Office Specialist		1				1
Server System Administrator		1				1

2022-2023 Legislative Budget Request
Education and General
Position and Fiscal Summary
Operating Budget Form II
(to be completed for each issue)

University: **University of West Florida**
Issue Title: **A Cyber Coast for Florida's Future**

		NON-	
	RECURRING	**RECURRING**	**TOTAL**
Positions			
Faculty	29.00	0.00	29.00
Other (A&P/USPS)	20.00	0.00	20.00
	-------------	-------------	-------------
Total	49.00	0.00	49.00
	==========	==========	==========
Salaries and Benefits	$6,435,235	$0	$6,435,235
Other Personal Services	$775,686	$0	$775,686
Expenses	$3,550,000	$0	$3,550,000
Operating Capital Outlay	$2,000,000	$0	$2,000,000
Electronic Data Processing	$0	$0	$0
Financial Aid	$2,500,000	$0	$2,500,000
Special Category (Specific)	$0	$0	$0
	$0	$0	$0
	$0	$0	$0
	$0	$0	$0
	-------------	-------------	-------------
Total All Categories	$15,260,921	$0	$15,260,921
	==========	==========	==========