

The Florida Senate
BILL ANALYSIS AND FISCAL IMPACT STATEMENT

(This document is based on the provisions contained in the legislation as of the latest date listed below.)

Prepared By: The Professional Staff of the Appropriations Committee on Transportation, Tourism, and Economic Development

BILL: CS/CS/SB 1266

INTRODUCER: Appropriations Committee on Transportation, Tourism, and Economic Development;
Commerce and Tourism Committee and Senator Calatayud

SUBJECT: Cybersecurity Internships

DATE: February 6, 2026

REVISED: _____

	ANALYST	STAFF DIRECTOR	REFERENCE	ACTION
1.	<u>Dike</u>	<u>McKay</u>	<u>CM</u>	<u>Fav/CS</u>
2.	<u>Griffin</u>	<u>Nortelus</u>	<u>ATD</u>	<u>Fav/CS</u>
3.	_____	_____	<u>AP</u>	_____

Please see Section IX. for Additional Information:

COMMITTEE SUBSTITUTE - Substantial Changes

I. Summary:

CS/CS/SB 1266 creates the Cybersecurity Experiential Learning Program within the Department of Commerce (department). Under the bill, the department must partner with the University of South Florida's (USF) Center for Cybersecurity program (Cyber Florida) to design the program for implementation at other universities and institutions in the state to increase the state's cybersecurity workforce. The bill outlines annual reporting requirements and provides sunset provisions for the Legislature's sustenance of the Cybersecurity Experiential Learning Program.

This bill may have an indeterminate impact on the department and institutions of higher education relating to the creation of the program. However, the creation of the program is subject to appropriation. See Section V., Fiscal Impact Statement.

The bill takes effect July 1, 2026.

II. Present Situation:

NCAE-C Programs

The National Security Agency (NSA) launched the National Centers of Academic Excellence in 1999 to promote education and research in cybersecurity, produce professionals with cyber expertise[to] expand the cybersecurity workforce, and reduce vulnerabilities in national

infrastructure.¹ The National Centers of Academic Excellence in Cybersecurity (NCAE-C) program is managed by the NSA's National Cryptologic School, alongside other federal partners.² To receive a designation under this program, institutions must complete validation of their programs of study.³

Academic institutions may choose from three designations under the NCAE:

- The cyber defense (CAE-CD) designation is awarded to regionally accredited schools offering cybersecurity degrees and certificates.
- The cyber research (CAE-R) designation is awarded to Department of Defense schools, military academies with PhD programs, and other institutions with specific doctoral programs.
- The cyber operations (CAE-CO) designation applies to technical higher education programs focused on computer science, computer engineering, and/or electrical engineering.⁴

As of February 2024, NCAE had over “480 designated institutions across 48 states, the District of Columbia, and Puerto Rico. There are 153 associate programs and degrees, 243 Cyber Defense bachelors and graduate programs, 20 Cyber Operations bachelors and graduate programs, and 80 institutions hold the Research designation.”⁵

The following Florida institutions hold one of the three designations:

- Florida Agricultural and Mechanical University.
- Florida Atlantic University.
- Florida Memorial University.
- Florida State University.
- Eastern Florida State College.
- University of Central Florida.
- University of Florida.
- University of North Florida.
- University of South Florida.
- University of West Florida (UWF).
- Florida Institute of Technology.
- Florida International University.
- Jacksonville University.
- Miami Dade College.
- Nova Southeastern University.
- Pensacola State College.
- St. Petersburg College.⁶

¹ Nat'l Ctr. of Acad. Excellence in Cybersecurity, *Program Book*, available at https://www.caecommunity.org/_files/ugd/fd9f4b_4248a3dedef84805adcc9d1a3bf78fd4.pdf (last visited Jan. 21, 2026).

² Nat'l Sec. Agency, *National Centers of Academic Excellence in Cybersecurity*, available at <https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/> (last visited Jan. 21, 2026).

³ *Id.*

⁴ *Id.*

⁵ Nat'l Ctr. of Acad. Excellence in Cybersecurity, *supra* note 1.

⁶ *Id.*

Cyber Florida Pilot Program

In 2014, the Legislature created Cyber Florida in s. 1004.444, F.S., within USF to make Florida a national leader in cybersecurity and expand the state cybersecurity workforce. The goals of Cyber Florida include creating jobs in the state's cybersecurity industry, facilitating research and development initiatives with, forming partnerships with major military installations, attracting cybersecurity companies to Florida, and sharing cybersecurity knowledge, resources, and training.⁷

In 2024, the Legislature updated s. 1004.444, F.S., allowing Cyber Florida to assist any state-funded initiatives that relate to: (1) cybersecurity training, professional development, and education for state and local government employees; and (2) increasing the cybersecurity effectiveness of the state and local government technology platforms and infrastructure.

As part of this pilot at USF, Cyber Florida hosts:

- The Aligned Realistic Cyberattack Simulation (ARCS) Range, which provides cyber and IT training for Florida public sector employees.⁸
- Firstline, which provides public sector training in cybersecurity.⁹
- The Critical Infrastructure Program, which provides free access to cybersecurity risk assessments and resources for specific organizations.¹⁰
- Operation K12, to include cybersecurity education in K-12 classrooms across the state with lesson plans, labs, and more.¹¹
- CyberWorks, to provide cybersecurity training with a focus on transitioning veterans, military spouses, first responders, and career-changers.¹²
- CyberHub, an online platform with free tools and education resources, including a protected online laboratory for students and researchers to investigate software without compromising the security of other devices.¹³
- The Security Operations Center Apprentice Program (SOCAP), which is a paid internship program for USF students studying cybersecurity.¹⁴
- PhaseZero, which fills critical gaps in funding for cybersecurity entrepreneurs and fosters research partnerships.¹⁵
- The Cybersecurity and Information Technology Pathways Program, partnered with the Florida Department of Education, to fund projects which prepared students for cybersecurity and IT jobs.¹⁶
- The National Institute of Standards and Technology (NIST) Ramps Program, which partners with organizations and laboratories to provide students with hands-on training.¹⁷

⁷ Cyber Florida, *Our Mission*, available at <https://cyberflorida.org/about/> (last visited Jan. 21, 2026).

⁸ Cyber Florida, *The ARCS Range*, available at <https://cyberflorida.org/arcs-range/> (last visited Jan. 21, 2026).

⁹ Cyber Florida, *Firstline*, available at <https://cyberflorida.org/firstline/> (last visited Jan. 21, 2026).

¹⁰ Cyber Florida, *Critical Infrastructure Program*, available at <https://cyberflorida.org/cip/> (last visited Jan. 21, 2026).

¹¹ Cyber Florida, *Operation K12*, available at <https://cyberflorida.org/opk12/> (last visited Jan. 21, 2026).

¹² Cyber Florida, *CyberWorks*, available at <https://cyberflorida.org/cyberworks/> (last visited Jan. 21, 2026).

¹³ Cyber Florida, *CyberHub*, available at <https://cyberflorida.org/florida-cyberhub/> (last visited Jan. 21, 2026).

¹⁴ Cyber Florida, *SOCAP*, available at <https://cyberflorida.org/socap/> (last visited Jan. 21, 2026).

¹⁵ Cyber Florida, *phaseZero*, available at <https://cyberflorida.org/phasezero/> (last visited Jan. 21, 2026).

¹⁶ Cyber Florida, *Cyber/IT Pathways*, available at <https://cyberflorida.org/pathways/> (last visited Jan. 21, 2026).

¹⁷ Cyber Florida, *NIST Ramps Program*, available at <https://cyberflorida.org/nist-ramps-program/> (last visited Jan. 21, 2026).

At UWF, the pilot program hosts workforce development and community outreach programs, including:

- The National Cybersecurity Workforce Development Program, CyberSkills2Work, which provides free education and career development for eligible transitioning military, first responders, veterans, military spouses, and government personnel.¹⁸
- The UWF Florida Cybersecurity Training Program, which provides free training for eligible university, college, K-12, state, county, and city employees.¹⁹
- The UWF Cyber Skills Exercise, an intensive cybersecurity one-day training program eligible transitioning military members, first responders, veterans, military spouses, and State, Local, Tribal, and Territorial (SLTT) government personnel.²⁰
- The Cybersecurity Education in Critical Infrastructure Protection (CECIP) Project, which develops training courses with hands-on, laboratory experiences to offer workforce development certificates.²¹
- GenCyber Experience Camps, which provide K-12 students and teachers with introductory cybersecurity education.²²
- Cybersecurity Ambassadors, which sends UWF students to K-12 schools in Northwest Florida to teach cybersecurity expertise and awareness.²³
- CyberPatriot, which is a cybersecurity competition for middle and high school students.²⁴
- The 502 Project, partnered with other Florida higher education institutions, which connects high school students with professional mentors and teaches them new cybersecurity skills.²⁵
- ITEN Wired, which is a cybersecurity and IT conference for industry leaders, educators, entrepreneurs.²⁶
- Women in CyberSecurity, which is a Florida affiliate group supporting the recruitment, retention, and advancement of women in cybersecurity.²⁷

III. Effect of Proposed Changes:

Findings

Section 1 creates s. 1004.0983, F.S., explaining that the state’s cybersecurity workforce is essential to state and national security, multi-sector state economic resilience, and the protection of critical infrastructure while also providing that the state has a persistent shortfall in its supply

¹⁸ UWF, *Center for Cybersecurity*, available at <https://uwf.edu/centers/center-for-cybersecurity/> (last visited Jan. 21, 2026) (“The University of West Florida Center for Cybersecurity has been awarded a \$9.6 million grant from the U.S. Department of War CIO Cyber Academic Engagement Office to expand the National Cybersecurity Workforce Development Program. The program will prepare over 4,688 professionals over the next two years for 24 industry certifications and 41 emerging cybersecurity and AI work roles through 62 new educational pathways.”).

¹⁹ *Id.*

²⁰ *Id.* (“These exercises are part of the National Cybersecurity Workforce Development Program, CyberSkills2Work®, and funded by the Cybersecurity and Infrastructure Security Agency (CISA)”).

²¹ *Id.*

²² UWF Center for Cybersecurity, *Community Outreach*, available at <https://uwf.edu/centers/center-for-cybersecurity/community-outreach/> (last visited Jan. 21, 2026).

²³ *Id.*

²⁴ *Id.*

²⁵ *Id.*

²⁶ *Id.*

²⁷ *Id.*

of qualified cybersecurity professionals. Section 1 provides additional findings related to the two successful pilot programs at USF and the University of West Florida which demonstrated the feasibility and effectiveness of combining cybersecurity internships, federal security clearance readiness, and CompTIA Security+ certification as critical elements of workforce development for students and to the need for an expanded capacity to develop a more qualified cybersecurity workforce through experiential learning opportunities in cybersecurity for students.

Cybersecurity Program

In subsection (2), the bill creates the Cybersecurity Experiential Learning Program (program) within the department, subject to legislative appropriation. The department must use ten percent of appropriated funds in the 2026-2027 fiscal year to enter into an agreement with Cyber Florida to collaborate in designing the program for implementation at a minimum of one state university or Florida College institution during the 2026-27 school year.

Under subsection (3) of the bill, Cyber Florida is to determine and report back to the department on the following:

- The specific internship opportunities and experiential learning opportunities that the US Department of Commerce's NIST believes will be the most impactful on a student's job placement in high-demand cybersecurity roles in Florida;
- A review of best practices for cybersecurity experiential learning opportunities in place at other NCAE-C institutions that can be replicated at institutions within Florida;
- A recommendation for the minimum qualifications a student should possess or meet prior to enrolling in an experiential learning program;
- A listing of the state universities and Florida College System institutions what wish to participate in the program, along with an expected number of students to be served at each institution during the fiscal year; and
- A listing of employers in the state with openings, or anticipated openings, in cybersecurity roles or in other industries that require a security clearance.

Subsection (3) also provides that Cyber Florida is to make a recommendation to the department for the disbursement of available funds for the program to maximize statewide impact, improve job placement, and support economic growth in Florida's defense industry.

Subsection (4) provides that in each fiscal year that funds have been appropriated, or if the program has an unspent balance from a prior appropriation which can continue to support program operations, the department may:

- Implement the program and directly disburse funds to participating institutions; and
- Enter into a mutually agreed upon multi-year contract with Cyber Florida to administer the program statewide and disburse available funding to participating institutions.

The bill further provides that any disbursement made under subsection (4) is subject to approval by the Department.

Reporting

Beginning January 15, 2028, and on January 15 following the completion of a fiscal year in which the program operates, the department must submit a report to the Governor, the President of the Senate, and the Speaker of the House of Representatives. The report must include:

- The number of students participating at each institution as well as a listing of the specific outcomes, skills, or credentials earned by students through the program which contributed to job placement;
- The number of students who have completed an experiential learning opportunity and have subsequently entered federal, state, or private sector cybersecurity jobs in the state, and the number of students provided security clearance preparation training for other fields;
- Recommendations for program improvements, including potential integration with other state workforce initiatives and potentially expanding the program to workforces supporting national security.

Effective Date

The bill sets forth an effective date of July 1, 2026.

IV. Constitutional Issues:**A. Municipality/County Mandates Restrictions:**

None.

B. Public Records/Open Meetings Issues:

None.

C. Trust Funds Restrictions:

None.

D. State Tax or Fee Increases:

None.

E. Other Constitutional Issues:

None identified.

V. Fiscal Impact Statement:**A. Tax/Fee Issues:**

None.

B. Private Sector Impact:

None.

C. Government Sector Impact:

The creation of the Cybersecurity Experiential Internship and Clearance Readiness Program within the Department of Commerce will have a significant, negative yet indeterminate impact on the department. Additionally, there may be increased costs for institutions of higher education to implement this bill. However, the creation of the program is subject to appropriation.

VI. Technical Deficiencies:

None.

VII. Related Issues:

None.

VIII. Statutes Affected:

This bill creates section 1004.0983 of the Florida Statutes.

IX. Additional Information:**A. Committee Substitute – Statement of Substantial Changes:**

(Summarizing differences between the Committee Substitute and the prior version of the bill.)

CS/CS by Appropriations Committee on Transportation, Tourism, and Economic Development on February 4, 2026:

The committee substitute provides Legislative findings related to cybersecurity workforce and directs the Department of Commerce, subject to legislative appropriation, to create and operate the Cybersecurity Experiential Learning Program beginning in Fiscal Year 2026-2027, requires a portion of initial funding be used to contract with Cyber Florida at the University of South Florida to design and plan the program, sets out planning, reporting, and administrative duties (including identifying internship opportunities and participating institutions and authorizing how funds may be disbursed), and specifies an expiration date of July 1, 2032.

CS by Commerce and Tourism Committee on January 21, 2026:

The amendment removes the section appropriating \$11.9 million to the Department of Commerce to implement the bill.

B. Amendments:

None.