FLORIDA HOUSE OF REPRESENTATIVES
BILL ANALYSIS

This bill analysis was prepared by nonpartisan committee staff and does not constitute an official statement of legislative intent.

BILL #: CS/HB 1081	**COMPANION BILL:** SB 1266 (Calatayud)
TITLE: Cybersecurity Internships	**LINKED BILLS:** None
SPONSOR(S): Sirois	**RELATED BILLS:** None

Committee References

Careers & Workforce
15 Y, 0 N, As CS

SUMMARY

Effect of the Bill:
The bill creates, subject to appropriation, the Cybersecurity Experiential Internship and Clearance Readiness Program within the Department of Commerce to accelerate the development of Florida's cybersecurity workforce by increasing Florida's highly qualified, clearance-ready cybersecurity graduates.

Fiscal or Economic Impact:
None.

JUMP TO SUMMARY ANALYSIS RELEVANT INFORMATION BILL HISTORY

ANALYSIS

EFFECT OF THE BILL:

The bill provides legislative findings and intent to build on current cybersecurity initiatives operating at the University of South Florida (USF) and the University of West Florida (UWF). To that end and subject to appropriation, the bill creates the Cybersecurity Experiential Internship and Clearance Readiness Program (Program) within the Department of Commerce (Commerce). The bill requires Commerce to enter into an agreement with the Florida Center for Cyber Security (Cyber Florida) within the USF to implement the Program in collaboration with all National Security Agency National Centers of Academic Excellence in Cybersecurity (NCAE-C)-designated state universities and Florida College System institutions. The Program must include the following components:

- increasing the number of experiential cyber risk analyst internships statewide by using an instrumented platform of automated assessments with employers based in this state in the defense, finance, health care, transportation, utility, and critical infrastructure sectors;
- providing intern-supporting organizations with actionable, prioritized analytics, reporting, and risk mitigation action plans to enhance cyber resilience across this state;
- delivering a federal security clearance readiness curriculum, including comprehensive background checks preparation, national security information and protection training, clearance application preparation and vetting, and mentoring for selected participants;
- providing CompTIA Security+ certification training and examination for selected participants;
- coordinating with state, federal, and private sector partners to facilitate placement of graduates in high-demand cybersecurity roles; and
- providing access to datasets for statewide cyber assessments, research, and development. (Section 1).

The bill requires that the Program be available at all NCAE-C-designated state universities and Florida College System (FCS) institutions by the beginning of the 2026-27 academic year.

Under the bill, Commerce is required to submit an annual report, beginning January 1, 2027, and continuing through January 1, 2032, to the Governor, the President of the Senate, and the Speaker of the House of Representatives that contains all of the following information:

- the number of students participating in internships, clearance readiness preparation, and CompTIA Security+ certification programs at each institution;
- the number of students who have earned CompTIA Security+ certification and the number of students who have completed internship and clearance readiness milestones;
- the number of students who subsequently reported entering federal, state, or private sector cybersecurity positions requiring a federal public trust or national security clearance, and any available data on those positions; and
- recommendations for program improvements, including potential integration with other state workforce initiatives. (Section 1).

The bill provides for the expiration of the Program on January 1, 2032. (Section 1).

The effective date of the bill is July 1, 2026. (Section 2).

RELEVANT INFORMATION

SUBJECT OVERVIEW:

Cybersecurity Background

Over the last decade, cybersecurity has rapidly become a growing concern. Cyberattacks are growing in frequency and severity. Cybercrime was expected to annually inflict $8 trillion worth of damage globally.[1] The United States is often a target of cyberattacks, including attacks on critical infrastructure, and has been a target of more significant cyberattacks[2] over the last 14 years than any other country.[3] The Colonial Pipeline is an example of critical infrastructure that was attacked, disrupting what is arguably the nation's most important fuel conduit.[4]

Ransomware is a type of cybersecurity incident where malware[5] that is designed to encrypt files on a device renders the files and the systems that rely on them unusable. In other words, critical information is no longer accessible. During a ransomware attack, malicious actors demand a ransom in exchange for regained access through decryption. If the ransom is not paid, the ransomware actors will often threaten to sell or leak the data or authentication information. Even if the ransom is paid, there is no guarantee that the bad actor will follow through with decryption.

In recent years, ransomware incidents have become increasingly prevalent among the nation's state, local, tribal, and territorial government entities and critical infrastructure organizations.[6] For example, Tallahassee Memorial Hospital was hit by a ransomware attack early in 2023, and the hospital's systems were forced to shut down,

---

[1] Cybercrime Magazine, *Cybercrime to Cost the World $8 Trillion Annually in 2023*, https://cybersecurityventures.com/cybercrime-to-cost-the-world-8-trillion-annually-in-2023/ (last visited Jan. 20, 2026).

[2] "Significant cyber-attacks" are defined as cyber-attacks on a country's government agencies, defense, and high-tech companies, or economic crimes with losses equating to more than a million dollars. Specops, *The Countries Experiencing the Most 'Significant' Cyber-attacks*, https://specopssoft.com/blog/countries-experiencing-significant-cyber-attacks/ (last visited Jan. 20, 2026).

[3] *Id*.

[4] S&P Global, *Pipeline operators must start reporting cyberattacks to government: TSA orders*, https://www.spglobal.com/commodityinsights/en/market-insights/latest-news/electric-power/052721-pipeline-operators-must-start-reporting-cyberattacks-to-government-tsa-orders?utm_campaign=corporatepro&utm_medium=contentdigest&utm_source=esgmay2021 (last visited Jan. 20, 2026).

[5] "Malware" means hardware, firmware, or software that is intentionally included or inserted in a system for a harmful purpose. https://csrc.nist.gov/glossary/term/malware (last visited Jan. 20, 2026).

[6] Cybersecurity and Infrastructure Agency, *Ransomware 101,* https://www.cisa.gov/stopransomware/ransomware-101 (last visited Jan. 20, 2026).

impacting many local residents in need of medical care.[7] Likewise, Tampa General Hospital detected a data breach in May of 2023, which may have compromised the data of up to 1.2 million patients.[8]

Florida Center for Cybersecurity

Cyber Florida is housed within USF and was first established in 2014.[9] The goals of Cyber Florida are to:[10]

- position Florida as the national leader in cybersecurity and its related workforce primarily through advancing and funding education, and research and development initiatives in cybersecurity and related fields, with a secondary emphasis on, and community engagement and cybersecurity awareness;
- assist in the creation of jobs in the state's cybersecurity industry and enhance the existing cybersecurity workforce through education, research, applied science, and engagements and partnerships with the private and military sectors;
- act as a cooperative facilitator for state business and higher education communities to share cybersecurity knowledge, resources, and training;
- seek out research and development agreements and other partnerships with major military installations and affiliated contractors to assist, when possible, in homeland cybersecurity defense initiatives;
- attract cybersecurity companies and jobs to the state with an emphasis on defense, finance, health care, transportation, and utility sectors; and
- conduct, fund, and facilitate research and applied science that leads to the creation of new technologies and software packages that have military and civilian applications and which can be transferred for military and homeland defense purposes or for sale or use in the private sector.

If Cyber Florida receives a request for assistance from the Department of Management Services, Florida Digital Service, or another state agency, Cyber Florida is authorized, but may not be compelled by the agency, to conduct, consult on, or otherwise assist any state-funded initiatives related to:

- Cybersecurity training, professional development, and education for state and local government employees, including school districts and the judicial branch.
- Increasing the cybersecurity effectiveness of the state's and local governments' technology platforms and infrastructure, including school districts and the judicial branch.

Since 2022, Cyber Florida has received annual appropriations:

Fiscal Year	Appropriation Amount
2022-23[11]	$ 20,500,000
2023-24[12]	$ 10,500,000
2024-25[13]	$ 35,500,000
2025-26[14]	$ 35,500,000
Total:	$ 102,000,000

National Centers of Academic Excellence in Cybersecurity

The NCAE-C program is managed by the National Security Agency's National Cryptologic School. Federal partners include the Cybersecurity and Infrastructure Security Agency, the Federal Bureau of Investigation, the National

[7] Tallahassee Democrat, *TMH says it has taken 'major step' toward restoration after cybersecurity incident* (Feb. 15, 2023) https://www.tallahassee.com/story/news/local/2023/02/14/tmh-update-hospital-has-taken-major-step-toward-restoration/69904510007/ (last visited Jan. 20, 2026).
[8] Alessandro Mascellino, Infosecurity Magazine, *Tampa General Hospital Data Breach Impacts 1.2 Million Patients* (Jul. 24, 2023), https://www.infosecurity-magazine.com/news/tampa-hospital-data-breach/ (last visited Jan. 20, 2026).
[9] Chapter 2014-56, L.O.F.
[10] Section 1004.444(2), F.S.
[11] Specific Appropriation 157A, s. 2, ch. 2022-156, L.O.F.
[12] Specific Appropriation 156, s. 2, ch. 2023-239, L.O.F.
[13] Specific Appropriation 160, s. 2, ch. 2024-231, L.O.F.
[14] Specific Appropriation 161, s. 2, ch. 2025-198, L.O.F.

Institute of Standards and Technology/National Initiative on Cybersecurity Education, the National Science Foundation, the Department of Defense Office of the Chief Information Officer, and U.S. Cyber Command.[15]

NCAE-C program aims to create and manage a collaborative cybersecurity educational program with community colleges, colleges, and universities that:

- establishes standards for cybersecurity curriculum and academic excellence;
- includes competency development among students and faculty;
- values community outreach and leadership in professional development;
- integrates cybersecurity practice within the institution across academic disciplines; and
- actively engages in solutions to challenges facing cybersecurity education.[16]

All regionally accredited two-year, four-year, and graduate-level institutions in the United States are eligible to apply to become a CAE-C designated institution. An institution or program must apply for re-designation every five academic years.[17] Academic institutions may choose from three designations.[18] The designation process is a combination of elements related to the institution focused on outputs for determining academic achievement. This combination assures that the institution meets the desired characteristics of a CAE institution, and that the academic delivery to students is producing the qualified workforce needed by the nation. CAE-designated institutions must complete validation of a program of study, which is a series of courses and experiences that a student can reasonably accomplish in the course of attaining a degree or completing a certificate.[19]

Among Florida's state colleges and state universities, nine state universities[20] and 13 state colleges[21] are NCAE-C-designated.[22]

CompTIA Security+ certification

CompTIA Security+ is an early-career cybersecurity certification that validates essential skills in securing tech networks, detecting threats, and responding to cybersecurity incidents. Designed for tech professionals beginning or advancing in cybersecurity, CompTIA Security+ certification is useful for roles such as security administrator, security specialist, network administrator, systems administrator, and security analyst.[23] The certification is vendor-neutral certification that establishes foundational knowledge in cybersecurity and can be used as a stepping-stone to advanced certifications like CISSP, CISM or SecurityX.[24]

---

[15] National Security Agency, *National Centers of Academic Excellence in Cybersecurity*, https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/ (last visited Jan. 20, 2026).
[16] *Id*.
[17] Centers of Academic Excellence in Cybersecurity Community, *What is a CAE-C?*, https://www.caecommunity.org/what-is-a-cae-c (last visited Jan. 20, 2026).
[18] The three designations are Center of Academic Excellence in Cyber Defense (CAE-CD), Center of Academic Excellence in Cyber Operations (CAE-CO), and Center of Academic Excellence in Cyber Research (CAE-R). *See* Centers of Academic Excellence in Cybersecurity Community, *What is a CAE-C?*, https://www.caecommunity.org/what-is-a-cae-c (last visited Jan. 20, 2026).
[19] National Security Agency, *National Centers of Academic Excellence in Cybersecurity*, https://www.nsa.gov/Academics/Centers-of-Academic-Excellence/ (last visited Jan. 20, 2026).
[20] The universities are: Florida Agricultural and Mechanical University; Florida Atlantic University; Florida International University; Florida State University; University of Central Florida; University of Florida; University of North Florida; University of South Florida; and University of West Florida.
[21] The FCS Institutions are: Chipola College; Daytona State College; Eastern Florida State College; Florida State College at Jacksonville; Indian River State College; Miami Dade College; Palm Beach State College; Pensacola State College; Santa Fe College; Seminole State College; St. Petersburg College; Tallahassee State College; and Valencia College.
[22] Centers of Academic Excellence in Cybersecurity Community, *CAE Institution Map*, https://maps.caecommunity.org/ (last visited Jan. 20, 2026)
[23] CompTIA, *Security +: Resources*, https://www.comptia.org/en-us/certifications/security/#resources (Jan. 14, 2026)
[24] *Id*.

The CompTIA Security+ exam is available at Pearson VUE testing centers or online with remote proctoring.[25] The current version of the exam consists of a maximum of 90 multiple-choice and performance-based questions over 90 minutes.[26]

Internships

Internships have become essential to career preparation. They bridge the gap between academic knowledge and industry expectations, helping students develop the competencies that a technology-driven workforce demands. Internships help students:

- Apply classroom learning in professional settings.
- Clarify career interests and strengths.
- Gain exposure to tools, timelines, and team environments.
- Build a professional network.
- Strengthen resumes and job interviews.[27]

Significantly, more than 70 percent of employers plan to maintain or increase intern hiring.[28] Paid interns average more job offers and higher starting salaries than unpaid interns and non-interns.[29] Over two-thirds of 2024 graduates nationwide completed at least one internship.[30]

Current Initiatives

USF launched the Security Training Collaborative (Collaborative) in 2020 through a partnership with Security Management International, a consulting firm based in Washington, D.C. The Collaborative is a 16-week internship program where students gain hands-on experience far beyond traditional classroom learning. They take part in exercises with the Secret Service, U.S. Marshals and Capitol Police, while weekly sessions with national security experts introduce them to the latest trends in intelligence and security. The Collaborative leverages Cyber Florida and the Global and National Security Institute's Future Strategist Program at USF to give students additional resources and opportunities.[31]

In 2024, the UWF received funding to develop a pilot program that helps students prepare security clearance applications and understand the process of applying for a security clearance. The program will also facilitate internships with Florida-based defense companies that require security clearances. [32]

---

[25] *Id*.
[26] CompTIA, *Security+: Overview*, https://www.comptia.org/en-us/certifications/security/#overview (Jan. 14, 2026).
[27] University of South Florida, Bellini College of Artificial Intelligence, Cybersecurity and Computing, *Internships*, https://www.usf.edu/ai-cybersecurity-computing/academics/internships.aspx (last visited Jan. 20, 2026).
[28] National Association of Colleges and Employers, *More the 70% of Organizations Expect to Increase or Maintain Intern Hiring Despite Overall Dip in Hiring*, https://www.naceweb.org/talent-acquisition/internships/more-than-70-percent-of-organizations-expect-to-increase-or-maintain-intern-hiring-despite-overall-dip-in-hiring (last visited Jan. 20, 2026).
[29] *See* National Association of Colleges and Employers, *Job Outlook 2024*, pp. 6 and 32, *available at* https://www.naceweb.org/docs/default-source/default-document-library/2023/publication/research-report/2024-nace-job-outlook.pdf and National Association of Colleges and Employers, *Executive Summary The 2024 Student Survey Report*, p. 4, *available at* https://www.naceweb.org/docs/default-source/default-document-library/2024/publication/executive-summary/2024-nace-student-survey-executive-summary-four-year.pdf?Status=Master&sfvrsn=4d77a2d1_3
[30] National Association of Colleges and Employers, *Executive Summary The 2024 Student Survey Report*, p. 4, *available at* https://www.naceweb.org/docs/default-source/default-document-library/2024/publication/executive-summary/2024-nace-student-survey-executive-summary-four-year.pdf?Status=Master&sfvrsn=4d77a2d1_3.
[31] University of South Florida, *USF builds national security talent pipeline through innovative program*, https://www.usf.edu/news/2025/usf-builds-national-security-talent-pipeline-through-rare-program.aspx (Jan. 20, 2026).
[32] University of West Florida, *UWF awarded $320,210 to help students understand and prepare applications for security clearance*, https://mdi.kyj.mybluehost.me/uwf-awarded-320210-to-help-students-understand-and-prepare-applications-for-security-clearance/ (Jan. 20, 2026).

RECENT LEGISLATION:

YEAR	BILL #/SUBJECT	HOUSE/*SENATE* SPONSOR(S)	OTHER INFORMATION
2024	CS/CS/CS/HB 1555 - Cybersecurity	Giallombardo/ *Collins*	The bill became law on July 1, 2024.

BILL HISTORY

COMMITTEE REFERENCE	ACTION	DATE	STAFF DIRECTOR/ POLICY CHIEF	ANALYSIS PREPARED BY
Careers & Workforce Subcommittee	15 Y, 0 N, As CS	1/20/2026	Kiner	Wolff
THE CHANGES ADOPTED BY THE COMMITTEE:	• Aligned the expiration date of the Program with the due date of the final required report. • Removed a recurring appropriation from the bill and made the establishment of the Program subject to appropriation.			

THIS BILL ANALYSIS HAS BEEN UPDATED TO INCORPORATE ALL OF THE CHANGES DESCRIBED ABOVE.
