

1 A bill to be entitled
2 An act relating to cybersecurity internships; creating
3 s. 1004.0983, F.S.; providing legislative findings;
4 providing legislative intent; subject to legislative
5 appropriation, creating the Cybersecurity Experiential
6 Internship and Clearance Readiness Program within the
7 Department of Commerce; requiring the department to
8 enter into an agreement with the Florida Center for
9 Cybersecurity (Cyber Florida) to implement the program
10 in collaboration with specified universities and
11 institutions; requiring that the program include
12 specified components; requiring that the program be
13 available at specified universities and institutions
14 beginning in a specified academic year; requiring the
15 department, using data and analyses provided by Cyber
16 Florida, to submit a report by a specified date and
17 annually thereafter to the Governor and the
18 Legislature; providing requirements for the report;
19 providing for expiration of the program; providing an
20 effective date.

21
22 Be It Enacted by the Legislature of the State of Florida:

23
24 **Section 1. Section 1004.0983, Florida Statutes, is created**
25 **to read:**

26 1004.0983 Cybersecurity Experiential Internship and
27 Clearance Readiness Program.—

28 (1) (a) The Legislature finds that this state's
29 cybersecurity workforce is essential to state and national
30 security, multi-sector state economic resilience, and the
31 protection of critical infrastructure. The Legislature also
32 finds that this state has a persistent shortfall in its supply
33 of qualified cybersecurity professionals relative to the
34 workforce demand and that the growing integration of digital
35 technologies in all economic sectors will exacerbate this
36 workforce gap in the future.

37 (b) The Legislature further finds that the elements of the
38 program described in this section were successfully tested and
39 refined in two pilot programs: an experiential cyber internship
40 program with the University of South Florida and a combined
41 security clearance readiness and cyber certification program
42 with the University of West Florida. Both schools are designated
43 as National Security Agency National Centers of Academic
44 Excellence in Cybersecurity (NCAE-C). The successful pilot
45 programs demonstrated the feasibility and effectiveness of
46 combining cybersecurity experiential internships, federal
47 security clearance readiness preparation, and CompTIA Security+
48 certification for students as critical elements of workforce
49 development.

50 (c) The Legislature further finds that expansion of this

51 program statewide to all NCAE-C-designated state universities,
52 Florida College System institutions, and private postsecondary
53 educational institutions will accelerate the development of a
54 highly qualified, clearance-ready cybersecurity workforce. This
55 expanded capacity to develop a more qualified cybersecurity
56 workforce is necessary to both close existing gaps and keep pace
57 with the growth in demand for cybersecurity talent within this
58 state.

59 (2) (a) The Legislature intends to establish the
60 Cybersecurity Experiential Internship and Clearance Readiness
61 Program across all NCAE-C-designated state universities, Florida
62 College System institutions, and private postsecondary
63 educational institutions beginning with the 2026-2027 academic
64 year.

65 (b) The Legislature further intends to sustain the program
66 through the 2030-2031 academic year and establish clear metrics
67 and reporting requirements to measure the impact on this state's
68 workforce and national security posture.

69 (3) Subject to appropriation, the Cybersecurity
70 Experiential Internship and Clearance Readiness Program is
71 created within the Department of Commerce. The department shall
72 enter into an agreement with the Florida Center for
73 Cybersecurity (Cyber Florida) at the University of South
74 Florida, to implement the program in collaboration with all
75 NCAE-C-designated state universities, Florida College System

76 institutions, and private postsecondary educational
77 institutions.

78 (4) The program shall include all of the following
79 components:

80 (a) Increasing the number of experiential cyber risk
81 analyst internships statewide by using an instrumented platform
82 of automated assessments with employers based in this state in
83 the defense, finance, health care, transportation, utility, and
84 critical infrastructure sectors.

85 (b) Providing intern-supporting organizations with
86 actionable, prioritized analytics, reporting, and risk
87 mitigation action plans to enhance cyber resilience across this
88 state.

89 (c) Delivering a federal security clearance readiness
90 curriculum, including comprehensive background checks
91 preparation, national security information and protection
92 training, clearance application preparation and vetting, and
93 mentoring for selected participants.

94 (d) Providing CompTIA Security+ certification training and
95 examination for selected participants.

96 (e) Coordinating with state, federal, and private sector
97 partners to facilitate placement of graduates in high-demand
98 cybersecurity roles.

99 (f) Providing access to datasets for statewide cyber
100 assessments, research, and development.

101 (5) Beginning in the 2026-2027 academic year, the program
102 must be available at all currently NCAE-C-designated state
103 universities, Florida College System institutions, and private
104 postsecondary educational institutions.

105 (6) (a) Beginning January 1, 2027, and annually thereafter
106 through January 1, 2032, the department, using data and analyses
107 provided by Cyber Florida as required by the agreement under
108 subsection (3), shall submit a report to the Governor, the
109 President of the Senate, and the Speaker of the House of
110 Representatives.

111 (b) The report must include all of the following:

112 1. The number of students participating in internships,
113 clearance readiness preparation, and CompTIA Security+
114 certification programs at each institution.

115 2. The number of students who have earned CompTIA
116 Security+ certification and the number of students who have
117 completed internship and clearance readiness milestones.

118 3. The number of students who subsequently reported
119 entering federal, state, or private sector cybersecurity
120 positions requiring a federal public trust or national security
121 clearance, and any available data on those positions.

122 4. Recommendations for program improvements, including
123 potential integration with other state workforce initiatives.

124 (7) This section expires January 1, 2032.

125 **Section 2.** This act shall take effect July 1, 2026.