

**By** the Committee on Appropriations; the Appropriations Committee on Agriculture, Environment, and General Government; the Committee on Governmental Oversight and Accountability; and Senator Collins

576-03801-24

20241662c3

1                   A bill to be entitled  
2       An act relating to cybersecurity; amending s.  
3       287.0591, F.S.; providing that certain firms are  
4       disqualified from being awarded specified state  
5       contracts if certain conditions exist; amending s.  
6       1004.444, F.S.; providing that the Florida Center for  
7       Cybersecurity may also be referred to as "Cyber  
8       Florida"; providing that the center is established  
9       under the direction of the president of the University  
10      of South Florida, or his or her designee; revising the  
11      mission and goals of the center; authorizing the  
12      center to take certain actions relating to certain  
13      initiatives; requiring the Department of Management  
14      Services to contract with an independent verification  
15      and validation provider for specified services for all  
16      agency staff and vendor work to implement the  
17      enterprise cybersecurity resiliency program; requiring  
18      such provider to complete an assessment of the current  
19      program by a specified date; requiring that the  
20      assessment include recommendations based on certain  
21      evaluations; requiring that the contract require that  
22      monthly reports and deliverables be simultaneously  
23      provided to specified entities and parties; providing  
24      an effective date.

25  
26 Be It Enacted by the Legislature of the State of Florida:

27  
28       Section 1. Subsection (7) is added to section 287.0591,  
29       Florida Statutes, to read:

576-03801-24

20241662c3

30 287.0591 Information technology; vendor disqualification.-

31 (7) To protect the state's digital infrastructure from  
32 foreign invasion and digital terrorism, if a firm registered  
33 with the state's information technology state term contract or  
34 any firm performing information technology, systems integration,  
35 digital solution engineering, or technology management  
36 consulting work for state agencies has been found to have shared  
37 security information, including, but not limited to, login and  
38 password credentials, with companies or individuals in non-  
39 United States Trade Agreements Act compliant nations without the  
40 prior written consent of the contracting governmental client in  
41 dealings with state or federal contracts in the United States or  
42 its territories in the past 7 years, the firm must be  
43 disqualified from being awarded any state contract for work to  
44 be performed for the state, any special district, or any  
45 municipal subdivision.

46 Section 2. Section 1004.444, Florida Statutes, is amended  
47 to read:

48 1004.444 Florida Center for Cybersecurity.-

49 (1) The Florida Center for Cybersecurity, which may also be  
50 referred to as "Cyber Florida," is established within the  
51 University of South Florida, under the direction of the  
52 president of the university or the president's designee.

53 (2) The mission and goals of the center are to:

54 (a) Position Florida as the national leader in  
55 cybersecurity and its related workforce primarily through  
56 advancing and funding education and, research and development  
57 initiatives in cybersecurity and related fields, with a  
58 secondary emphasis on, and community engagement and

576-03801-24

20241662c3

59 cybersecurity awareness.

60 (b) Assist in the creation of jobs in the state's  
61 cybersecurity industry and enhance the existing cybersecurity  
62 workforce through education, research, applied science, and  
63 engagements and partnerships with the private and military  
64 sectors.

65 (c) Act as a cooperative facilitator for state business and  
66 higher education communities to share cybersecurity knowledge,  
67 resources, and training.

68 (d) Seek out research and development agreements and other  
69 partnerships with major military installations and affiliated  
70 contractors to assist, when possible, in homeland cybersecurity  
71 defense initiatives.

72 (e) Attract cybersecurity companies and jobs to this ~~the~~  
73 state, with an emphasis on the defense, finance, health care,  
74 transportation, and utility sectors.

75 (f) Conduct, fund, and facilitate research and applied  
76 science that leads to the creation of new technologies and  
77 software packages that have military and civilian applications  
78 and that can be transferred for military and homeland defense  
79 purposes or for sale or use in the private sector.

80 (3) Upon receiving a request for assistance from the  
81 Department of Management Services, the Florida Digital Service,  
82 or another state agency, the center is authorized, but may not  
83 be compelled by the agency, to conduct, consult on, or otherwise  
84 assist any state-funded initiatives related to:

85 (a) Cybersecurity training, professional development, and  
86 education for state and local government employees, including  
87 school districts and the judicial branch; and

576-03801-24

20241662c3

88 (b) Increasing the cybersecurity effectiveness of the  
89 state's and local governments' technology platforms and  
90 infrastructure, including school districts and the judicial  
91 branch.

92 Section 3. (1) In order to ensure the use of best practices  
93 and seamless functionality within the enterprise, the Department  
94 of Management Services shall contract with an independent  
95 verification and validation (IV&V) provider to provide IV&V  
96 services for all agency staff and vendor work needed to  
97 implement the enterprise cybersecurity resiliency program.

98 (2) The IV&V provider shall complete an assessment of the  
99 current program by December 1, 2024. The assessment must  
100 include, but need not be limited to, recommendations based on  
101 the evaluation of:

102 (a) The use of Cybersecurity Operations Center tools  
103 relative to their inherent capabilities to enhance efficiency  
104 and effectiveness;

105 (b) The existing processes to identify and address  
106 inefficiencies and areas requiring improvement;

107 (c) The interoperability among different systems to ensure  
108 compatibility and facilitate smooth data exchange;

109 (d) The alignment of strategic initiatives and resource  
110 allocation with organizational objectives; and

111 (e) The effectiveness of established communication channels  
112 to facilitate collaboration and dissemination of information  
113 across state entities.

114 (3) The IV&V contract must require that monthly reports and  
115 deliverables be simultaneously provided to the Department of  
116 Management Services, the Executive Office of the Governor's

576-03801-24

20241662c3

117 Office of Policy and Budget, the chair of the Senate  
118 Appropriations Committee, and the chair of the House of  
119 Representatives Appropriations Committee.

120 Section 4. This act shall take effect July 1, 2024.