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

601-03514-24 20241662c2

A bill to be entitled

An act relating to cybersecurity; amending s. 1004.444, F.S.; providing that the Florida Center for Cybersecurity may also be referred to as "Cyber Florida"; providing that the center is established under the direction of the president of the University of South Florida, or his or her designee, and, subject to the approval of the university's board of trustees, may be assigned by the president to a college that meets certain requirements; revising the mission and goals of the center; authorizing the center to take certain actions relating to certain initiatives; requiring the Department of Management Services to contract with an independent verification and validation provider for specified services for all agency staff and vendor work to implement the enterprise cybersecurity resiliency program; requiring such provider to complete an assessment of the current program by a specified date; requiring that the assessment include recommendations based on certain evaluations; requiring that the contract require that monthly reports and deliverables be simultaneously provided to specified entities and parties; providing an effective date.

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

Section 1. Section 1004.444, Florida Statutes, is amended to read:

1004.444 Florida Center for Cybersecurity.—

(1) The Florida Center for Cybersecurity, which may also be referred to as "Cyber Florida," is established within the University of South Florida, under the direction of the president of the university or the president's designee. The president may assign the center to a college of the university if the college has a strong emphasis on cybersecurity, technology, or computer sciences and engineering, as determined and approved by the university's board of trustees.

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

(a) 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.

(b) 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.

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

(d) 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.

(e) Attract cybersecurity companies and jobs to this ~~the~~

state, with an emphasis on the defense, finance, health care, transportation, and utility sectors.

(f) 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 that can be transferred for military and homeland defense purposes or for sale or use in the private sector.

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

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

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

Section 2. (1) In order to ensure the use of best practices and seamless functionality within the enterprise, the Department of Management Services shall contract with an independent verification and validation (IV&V) provider to provide IV&V services for all agency staff and vendor work needed to implement the enterprise cybersecurity resiliency program.

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

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

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

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

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

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

(3) The IV&V contract must require that monthly reports and deliverables be simultaneously provided to the Department of Management Services, the Executive Office of the Governor's Office of Policy and Budget, the chair of the Senate Appropriations Committee, and the chair of the House of Representatives Appropriations Committee.

Section 3. This act shall take effect July 1, 2024.