Committee on Military and Veterans Affairs, Space, and Domestic Security

CS/HB 7055 — Cybersecurity

by State Affairs Committee; State Administration and Technology Appropriations Subcommittee; Reps. Giallombardo, Fischer, and others (CS/CS/SB 1670 by Appropriations Committee; Military and Veterans Affairs, Space, and Domestic Security; and Senator Hutson)

The bill amends the state's Cybersecurity Act that requires the Florida Digital Service (FLDS) and the heads of state agencies to meet certain requirements to enhance the cybersecurity of state agencies. Currently, state agencies must provide cybersecurity training to their employees, report cybersecurity incidents, and adopt cybersecurity standards. However, there are no such requirements for local governments.

Current law does not specifically address ransomware, which is a form of malware designed to encrypt files on a device, rendering any files unusable. Malicious actors then demand ransom in exchange for decryption.

CS/HB 7055 prohibits state agencies and local governments from paying or otherwise complying with a ransomware demand.

The bill defines the severity level of a cybersecurity incident in accordance with the National Cyber Incident Response Plan.

State agencies and local governments will be required to report ransomware incidents and high severity level cybersecurity incidents to the Cybersecurity Operations Center and the Cybercrime Office within the Florida Department of Law Enforcement as soon as possible but no later than times specified in the bill. Local governments must also report to the local sheriff.

The bill also requires state agencies to report low level cybersecurity incidents and provides that local governments may report such incidents. State agencies and local governments must also submit after-action reports to FLDS following a cybersecurity or ransomware incident.

CS/HB 7055 requires the Cybersecurity Operations Center to notify the President of the Senate and Speaker of the House of Representatives of high severity level cybersecurity incidents. The notice must contain a high-level overview of the incident and its likely effects. In addition, the Center must provide the President of the Senate, Speaker of the House of Representatives, and the Cybersecurity Advisory Council with a consolidated incident report on a quarterly basis.

The bill requires state agency and local government employees to undergo certain cybersecurity training within 30 days of employment and annually thereafter.

The bill requires local governments to adopt cybersecurity standards that safeguard the local government's data, information technology, and information technology resources.

The bill expands the purpose of the Cybersecurity Advisory Council to include advising local governments on cybersecurity and requires the Council to examine reported cybersecurity and ransomware incidents to develop best practice recommendations. The Council must submit an annual comprehensive report regarding ransomware to the Governor, President of the Senate, and Speaker of the House of Representatives.

The bill creates new criminal penalties and fines for certain ransomware offenses against a government entity.

If approved by the Governor, these provisions take effect July 1, 2022.
Vote: Senate 38-0; House 110-0