LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 89TH LEGISLATIVE REGULAR SESSION

May 28, 2025

TO: Honorable Dustin Burrows, Speaker of the House, House of Representatives

FROM: Jerry McGinty, Director, Legislative Budget Board

IN RE: **HB150** by Capriglione (Relating to the establishment of the Texas Cyber Command and the transfer to it of certain powers and duties of the Department of Information Resources.), **As Passed 2nd House**

Estimated Two-year Net Impact to General Revenue Related Funds for HB150, As Passed 2nd House: a negative impact of ($138,716,366) through the biennium ending August 31, 2027. There would be an additional indeterminate cost to the state dependent on the costs to acquire and renovate a property in San Antonio that has a sensitive compartmented information facility.

The bill would make no appropriation but could provide the legal basis for an appropriation of funds to implement the provisions of the bill.

General Revenue-Related Funds, Five- Year Impact:

Fiscal Year	Probable Net Positive/(Negative) Impact to *General Revenue Related Funds*
2026	($68,476,294)
2027	($70,240,072)
2028	($68,130,072)
2029	($70,114,572)
2030	($72,198,297)

All Funds, Five-Year Impact:

Fiscal Year	Probable Savings/(Cost) from *General Revenue Fund* 1	*Change in Number of State Employees from FY 2025*
2026	($68,476,294)	65.0
2027	($70,240,072)	130.0
2028	($68,130,072)	130.0
2029	($70,114,572)	130.0
2030	($72,198,297)	130.0

Fiscal Analysis

The bill establishes the Texas Cyber Command (Command) as a state agency that is responsible for cybersecurity for this state, including functions currently performed by the Department of Information Resources (DIR). The Command would be authorized to enter into an interagency agreement with another state agency to provide administrative support services and a facility located in San Antonio that has a sensitive compartmented information facility. The Command is established to prevent and respond to cybersecurity incidents that affect governmental entities and critical infrastructure in this state, and among other

responsibilities, is responsible for providing leadership, guidance, and tools to enhance cybersecurity defenses, facilitating education and training of a cybersecurity workforce, monitoring and coordinating cyber threat intelligence and information systems, creating partnerships needed to carry out the Command's functions, and receiving all cybersecurity incident reports from state agencies and covered entities.

Among other provisions, the bill would require the Command: (1) promote public awareness of cybersecurity issues; (2) develop cybersecurity best practices and minimum standards for governmental entities; (3) develop and provide training to state agencies and covered entities on cybersecurity measures and awareness; (4) administer the cybersecurity threat intelligence center under Section 2063.201; (5) provide support to state agencies and covered entities experiencing a cybersecurity incident and respond to cybersecurity reports received under Subchapter D and other reports as appropriate; (6) administer the digital forensics laboratory under Section 2063.203; (7) administer a statewide portal for enterprise cybersecurity threat, risk, and incident management, and operate a cybersecurity hotline available for state agencies and covered entities 24 hours a day, seven days a week; (8) collaborate with law enforcement agencies to provide training and support related to cybersecurity incidents; (9) serve as a clearinghouse for information relating to all aspects of protecting the cybersecurity of governmental entities, including sharing appropriate intelligence and information with governmental entities, federal agencies, and covered entities; (10) collaborate with DIR to ensure information resources and information resources technologies obtained by DIR meet the cybersecurity standards and requirements established under this chapter; (11) offer cybersecurity resources to state agencies and covered entities as determined by the command; (12) adopt policies to ensure state agencies implement sufficient cybersecurity measures to defend information resources, information resources technologies, and sensitive personal information maintained by the agencies; (13) collaborate with federal agencies to protect against, respond to, and recover from cybersecurity incidents; and (14) establish a cybersecurity incident response unit. The bill authorizes the Command to recover the cost of providing direct technical assistance, training services, and other services to covered entities when reasonable and practical, as well as make certain emergency purchases when responding to a cybersecurity incident.

The bill would require the Command to require each state agency, not including university systems or institutions of higher education, to complete an information security assessment and a penetration test every two years.

Under provisions of the bill, not later than December 31, 2026, all functions and activities performed by DIR that relate to cybersecurity under Chapter 2063, Government Code, as added by this Act, or network security under Chapter 2059, Government Code, as amended by this Act, are transferred to the Texas Cyber Command, and all DIR employees who primarily perform duties related to cybersecurity under Chapter 2063, Government Code, as added by this Act, or network security under Chapter 2059, Government Code, as amended by this Act, become employees of the Command. The employees would continue to work in the same physical location unless moved in accordance with a memorandum of understanding.

The bill would make the Command subject to the Texas Sunset Act and require them to submit a report to the Legislative Budget Board that prioritizes, for the purposes of receiving funding, state agency cybersecurity projects, no later than October 1 of each even numbered year.

Methodology

This analysis assumes that any functions previously performed by DIR will have the same costs for the Command, including FTEs that are currently employed by DIR that would be transferred to the Command. Based on information provided by DIR, 27.4 FTEs will be transferred in fiscal year 2027, and 41.0 FTEs will be transferred in fiscal year 2028. Costs associated with implementing provisions of the bill may be offset by revenue collected by the Command for technical assistance, training services, and other services. The amount tied to these collections is unknown and have not been factored into this analysis.

It is assumed that the Cyber Command would require additional full-time equivalent (FTE) positions in addition to the number of FTEs that would be transferred from DIR. This analysis estimates that 65 FTEs would be needed to implement the bill in fiscal year 2026. Beginning in fiscal year 2027, 130 FTEs would be required to fulfill all the responsibilities and duties of the Command as articulated in the bill, including 24.0 FTEs for the Cyber Threat Intelligence Center, 24.0 FTEs for the Digital Forensics Laboratory, 35.0 FTEs for the Cybersecurity Incident Response Unit, 10.0 FTEs for Compliance and Training, and 37.0 FTEs for the

Director's Office, facilities support for 24 hour operations, and critical IT/information security support. Personnel costs for 65 FTEs in fiscal year 2026 is estimated to be $8,476,294. Costs for 130 FTEs in fiscal year 2027 is estimated to be $17,140,072.

This analysis assumes that start-up costs would be $12,700,000 in fiscal year 2026, and $4,000,000 in fiscal year 2027 for necessary equipment, service contracts, subscriptions, memberships, training/certifications, and equipment maintenance. Other Operating Expenses in fiscal year 2026 are estimated to be $11,300,000 for equipment, rent and one-time costs for the development and implementation of an accounting and budgeting system for the Command.

This analysis assumes that the Command's mission scope is significantly greater than that assigned currently to DIR. It is assumed that the Command would likely require a substantial volume of contracted services in niche and high value services by a range of cybersecurity providers. The types of operational services and level of technical capabilities required for the Command, including proactive threat hunting for cyber threats on state computer and network system, extend beyond what
DIR currently provides and are likely to differ in key respects from those offered under the Managed Security Services contract currently in place. The University of Texas System indicates that costs for these contract personnel are approximately $36.0 million beginning in fiscal year 2026 and increasing to $43.8 million by fiscal year 2030.

There would be an indeterminate cost to the state for the Command to enter an interagency contract with another state agency for the purpose of providing administrative support to the Command and for a facility in San Antonio that has a sensitive compartmented information facility (SCIF). These costs would likely include the construction of the SCIF, a dedicated operations center, and a digital forensics laboratory. Because the entity with which the Command would enter an interagency contract is unknown, these costs cannot be determined at this time.

Local Government Impact

No significant fiscal implication to units of local government is anticipated.

Source Agencies: 313 Department of Information Resources

LBB Staff: JMc, RStu, LCO, CSmi, NV