LEGISLATIVE BUDGET BOARD
Austin, Texas

FISCAL NOTE, 89TH LEGISLATIVE REGULAR SESSION

May 16, 2025

TO: Honorable Charles Schwertner, Chair, Senate Committee on Business & Commerce

FROM: Jerry McGinty, Director, Legislative Budget Board

IN RE: **HB150** by Capriglione (Relating to the establishment of the Texas Cyber Command as a component institution of The University of Texas System and the transfer to it of certain powers and duties of the Department of Information Resources.), **As Engrossed**

Estimated Two-year Net Impact to General Revenue Related Funds for HB150, As Engrossed: a negative impact of ($135,536,236) through the biennium ending August 31, 2027.

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	($69,264,269)
2027	($66,271,967)
2028	($65,539,711)
2029	($71,101,059)
2030	($72,496,056)

All Funds, Five-Year Impact:

Fiscal Year	Probable Savings/(Cost) from *General Revenue Fund* 1	Probable Savings/(Cost) from *Permanent University Fund* 0045	*Change in Number of State Employees from FY 2025*
2026	($69,264,269)	($25,000,000)	65.0
2027	($66,271,967)	($35,353,200)	130.0
2028	($65,539,711)	$0	130.0
2029	($71,101,059)	$0	130.0
2030	($72,496,056)	$0	130.0

Fiscal Analysis

The bill establishes the Texas Cyber Command (Command) which is a component of The University Texas System and administratively attached to The University of Texas at San Antonio. The Command is responsible for cybersecurity for the state, including functions currently performed by the Department of Information Resources (DIR). The Command is established to prevent and respond to cybersecurity incidents that affect governmental entities and critical infrastructure in the state, and among other responsibilities, is responsible for developing tools to enhance cybersecurity defenses, facilitating education and training of a cybersecurity workforce, establishing appropriate cybersecurity standards in collaboration with DIR, and creating

partnerships needed to effectively carry out the Command's functions.

Among other provisions, the bill would require the Command to (1) promote public awareness of cybersecurity issues; (2) develop cybersecurity best practices and minimum standards for governmental entities; (3) develop and provide cybersecurity compliance training to state agencies and covered entities on cybersecurity measures and awareness; (4) administer a Cybersecurity Threat Intelligence Center; (5) provide support to state agencies and covered entities experiencing a cybersecurity incident and respond to cybersecurity reports; (6) administer a Digital Forensics Laboratory ; (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; (10) collaborate with DIR to ensure information resources and information resources technologies obtained by DIR meet established cybersecurity standards and requirements; (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 permits the Command to recover the cost of providing direct technical assistance, training services, and other services to covered entities when reasonable and practical.

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 the bill, are transferred to the Command, and all DIR employees who primarily perform duties related to cybersecurity, including employees who provide administrative support for those services, become employees of the Texas Cyber 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 that October 1 of each even-numbered year.

Methodology

For purposes of this analysis, it is assumed that any functions previously performed by DIR will have the same costs for the Command, including FTEs that are currently employed by DIR that will be transferred to the Command. Based on information provided by DIR, 17.3 FTEs will be transferred in fiscal year 2027 and 26 FTEs will be transferred in FY 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.

The University of Texas System indicates that acquiring and renovating a suitable property to headquarter the Command in San Antonio is estimated at a total cost of $60.4 million, which includes the costs to construct a dedicated Sensitive Compartmented Information Facility required by the Cyber Threat Intelligence Center, a dedicated operations center, and a Digital Forensics Laboratory. These costs are split between $25.0 million in fiscal year 2026 and $35.4 million in fiscal year 2027. The University of Texas System indicates plans to incorporate the costs of this facility into future planning for Permanent University Fund allocations.

The University of Texas System indicates that start-up costs are estimated at $12.7 million in fiscal year 2026 and $4.0 million in fiscal year 2027 for necessary equipment, service contracts, subscriptions, memberships, training/certifications, and equipment maintenance. Other Operating Expenses in fiscal year 2026 total $11.3 million and includes equipment, rent and one-time costs for the development/implementation of an accounting and budgeting system for this agency.

Beginning in fiscal year 2026, The University of Texas System estimates that 65 FTEs would need to be hired to implement provisions of the bill. Beginning in fiscal year 2027, it is estimated that approximately 130 full-time equivalents would be required to fulfill all the responsibilities and duties of the Command as articulated in the bill, including 24 FTEs for the Cyber Threat Intelligence Center, 24 FTEs for the Digital Forensics

Laboratory, 35 FTEs for the Cybersecurity Incident Response Unit, and 10 FTEs for Compliance and Training. The balance of 37 FTEs comprising the minimum required for the Director's Office, facilities support for 24-hour operations, and critical IT/information security support. This total does not include the full-time equivalents employed by DIR in the cybersecurity area. It does not include personnel assigned to the regional security operations centers, which are managed today under contract to DIR; nor does it include any government officials assigned to other state agencies with cyber-related responsibilities. The total salaries and wages and retirement benefits for the 65 FTEs in fiscal year 2026 is estimated at $8.5 million. The total costs for the 130 FTEs in fiscal year 2027 is estimated at $17.0 million.

Because the Cyber Threat Intelligence Center, Cybersecurity Incident Response Unit, and Digital Forensics Laboratory are each new additions, the administrative support of The University of Texas at San Antonio will be required to develop new position descriptions and facilitate tailored recruitment activities. The University of Texas System indicates that to fulfill their assigned duties, there would be travel costs of $0.8 million beginning in fiscal year 2026 and increasing to $1.2 million by fiscal year 2030.

The University of Texas System indicates that the Command's mission scope is significantly greater than that assigned currently to DIR. To fulfill the required duties and responsibilities, they anticipate the need for 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 is approximately $36.0 million beginning in fiscal year 2026 and increasing to $43.8 million by fiscal year 2030.

Local Government Impact

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

Source Agencies: 300 Trusteed Programs Within the Office of the Governor, 302 Office of the Attorney General, 304 Comptroller of Public Accounts, 313 Department of Information Resources, 401 Military Department, 405 Department of Public Safety, 575 Texas Division of Emergency Management, 710 Texas A&M University System Administrative and General Offices, 720 The University of Texas System Administration, 781 Higher Education Coordinating Board

LBB Staff: JMc, RStu, LBO, GO, NV