BILL ANALYSIS

Senate Research Center

H.B. 150
By: Capriglione et al. (Parker)
Business & Commerce
5/19/2025
Engrossed

AUTHOR'S / SPONSOR'S STATEMENT OF INTENT

The bill's author has informed the committee of the increasing number of cyberattacks on Texas state agencies, local governments, political subdivisions, critical infrastructure, and private entities. Furthermore, these sophisticated attacks are seemingly being carried out not only by cybercriminals, but also hostile nation-state actors. Currently, in addition to their core missions of procurement and information technology, the Department of Information Resources (DIR) is tasked with certain cybersecurity responsibilities. However, the bill's author has also informed the committee that given the scale of these threats, the state's cybersecurity merits its own purpose-built agency whose sole focus is to prevent, respond to, and defend against cybersecurity threats and increase the cybersecurity posture and resiliency of the state.

H.B. 150 seeks to address this issue by establishing the Texas Cyber Command, which will execute and enhance existing cybersecurity responsibilities performed by DIR, improve the operational capacity of the state through the Cyber Threat Intelligence Center, Critical Incident Response Unit, and Forensics Laboratory, and leverage the robust cybersecurity ecosystem of the San Antonio region, including federal partners, academic institutions, and private sector entities.

H.B. 150 amends current law 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.

RULEMAKING AUTHORITY

Rulemaking authority is expressly granted to the Texas Cyber Command in SECTION 1 (Section 2063.004, Government Code) of this bill.

Rulemaking authority is expressly granted to the chief of the Texas Cyber Command in SECTION 1 (Section 2063.008, Government Code) of this bill.

Rulemaking authority previously granted to the Department of Information Resources is rescinded in SECTION 16 (Section 2063.507, Government Code) of this bill.

SECTION BY SECTION ANALYSIS

SECTION 1. Amends Subtitle B, Title 10, Government Code, by adding Chapter 2063, as follows:

CHAPTER 2063. TEXAS CYBER COMMAND

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 2063.001. DEFINITIONS. Defines "chief," "command," "covered entity," "critical infrastructure," "cybersecurity," "cybersecurity incident," "department," "governmental entity," "information resources," "information resources technologies," "local government," "sensitive personal information," and "state agency."

Sec. 2063.002. ORGANIZATION. (a) Provides that the Texas Cyber Command (command) is a component of The University of Texas System (UT system) and administratively attached to The University of Texas at San Antonio (UTSA).

(b) Provides that the command is managed by a chief appointed by the governor and confirmed with the advice and consent of the senate. Provides that the chief of the command (chief) serves at the pleasure of the governor and is required to possess professional training and knowledge relevant to the functions and duties of the command.

(c) Requires the command to employ other coordinating and planning officers and other personnel necessary to the performance of its functions.

(d) Requires UTSA, under an agreement with the command, to provide administrative support services for the command as necessary to carry out the purposes of this chapter.

Sec. 2063.003. ESTABLISHMENT AND PURPOSE. (a) Provides that the command is established to prevent and respond to cybersecurity incidents that affect governmental entities and critical infrastructure in this state.

(b) Provides that the command is responsible for cybersecurity for this state, including by performing certain tasks.

Sec. 2063.004. GENERAL POWERS AND DUTIES. (a) Requires 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 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 the Department of Information Resources (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; and

(13) collaborate with federal agencies to protect against, respond to, and recover from cybersecurity incidents.

(b) Authorizes the command to:

(1) adopt and enforce rules necessary to carry out this chapter;

(2) adopt and use an official seal;

(3) establish ad hoc advisory committees as necessary to carry out the command's duties under this chapter;

(4) acquire and convey property or an interest in property;

(5) procure insurance and pay premiums on insurance of any type, in accounts, and from insurers as the command considers necessary and advisable to accomplish any of the command's duties;

(6) hold patents, copyrights, trademarks, or other evidence of protection or exclusivity issued under the laws of the United States, any state, or any nation and may enter into license agreements with any third parties for the receipt of fees, royalties, or other monetary or nonmonetary value; and

(7) solicit and accept gifts, grants, donations, or loans from and contract with any entity to accomplish the command's duties.

(c) Requires the command, except as otherwise provided by this chapter, to deposit money paid to the command under this chapter in the state treasury to the credit of the general revenue fund.

Sec. 2063.005. COST RECOVERY. Requires the command to recover the cost of providing direct technical assistance, training services, and other services to covered entities when reasonable and practical.

Sec. 2063.007. EMERGENCY PURCHASING. Provides that, in the event the emergency response to a cybersecurity incident requires the command to purchase an item, the command is exempt from the requirements of Sections 2155.0755 (Verification of Use of Best Value Standard), 2155.083 (Electronic State Business Daily; Notice Regarding Procurements Exceeding $25,000), and 2155.132(c) (relating to requiring the Comptroller of Public Accounts of the State of Texas to monitor the purchasing practices of state agencies for certain purposes) in making the purchase.

Sec. 2063.008. RULES. Authorizes the governor to adopt rules necessary for carrying out the purposes of this chapter.

Sec. 2063.009. APPLICATION OF SUNSET ACT. Provides that the command is subject to Chapter 325 (Texas Sunset Act). Provides that, unless continued in existence as provided by that chapter, the command is abolished September 1, 2031.

SUBCHAPTER B. MINIMUM STANDARDS AND TRAINING

Sec. 2063.101. BEST PRACTICES AND MINIMUM STANDARDS FOR CYBERSECURITY AND TRAINING. (a) Requires the command to develop and annually assess best practices and minimum standards for use by governmental entities to enhance the security of information resources in this state.

(b) Requires the command to establish and periodically assess mandatory cybersecurity training that is required to be completed by all information resources employees of state agencies. Requires the command to consult with the Information Technology Council for Higher Education established under Section 2054.121 (Coordination with Institutions of Higher Education) regarding applying the training requirements to employees of institutions of higher education.

(c) Requires the command, except as otherwise provided by this subsection, to adopt policies to ensure governmental entities are complying with the requirements of this section. Requires the command to adopt policies that ensure that a person who is not a citizen of the United States us prohibited from being a member, employee, contractor, volunteer, or otherwise affiliated with the command or any entity or organization established or operated by the command under this chapter.

SUBCHAPTER C. CYBERSECURITY PREVENTION, RESPONSE, AND RECOVERY

Sec. 2063.201. CYBERSECURITY THREAT INTELLIGENCE CENTER. (a) Defines "center."

(b) Requires the command to establish a cybersecurity threat intelligence center (center). Requires the center to collaborate with federal cybersecurity intelligence and law enforcement agencies to achieve the purposes of this section.

(c) Requires the center, in coordination with the digital forensics laboratory under Section 2063.203, to:

(1) operate the information sharing and analysis organization established under Section 2063.204; and

(2) provide strategic guidance to regional security operations centers established under Subchapter G and the cybersecurity incident response unit under Section 2063.202 to assist governmental entities in responding to a cybersecurity incident.

(d) Requires the chief to employ a director for the center.

Sec. 2063.202. CYBERSECURITY INCIDENT RESPONSE UNIT. (a) Requires the command to establish a dedicated cybersecurity incident response unit to:

(1) detect and contain cybersecurity incidents in collaboration with the cybersecurity threat intelligence center under Section 2063.201;

(2) engage in threat neutralization as necessary and appropriate, including removing malware, disallowing unauthorized access, and patching vulnerabilities in information resources technologies;

(3) in collaboration with the digital forensics laboratory under Section 2063.203, undertake mitigation efforts if sensitive personal information is breached during a cybersecurity incident;

(4) loan resources to state agencies and covered entities to promote continuity of operations while the agency or entity restores the systems affected by a cybersecurity incident;

(5) assist in the restoration of information resources and information resources technologies after a cybersecurity incident and conduct post-incident monitoring;

(6) in collaboration with the cybersecurity threat intelligence center under Section 2063.201 and digital forensics laboratory under Section 2063.203, identify weaknesses, establish risk mitigation options and effective vulnerability-reduction strategies, and make recommendations to state agencies and covered entities that have been the target of a cybersecurity attack or have experienced a cybersecurity incident in order to remediate identified cybersecurity vulnerabilities;

(7) in collaboration with the cybersecurity threat intelligence center under Section 2063.201, the digital forensics laboratory under Section 2063.203, the Texas Division of Emergency Management, and other state agencies, conduct, support, and participate in cyber-related exercises; and

(8) undertake any other activities necessary to carry out the duties described by this subsection.

(b) Requires the chief to employ a director for the cybersecurity incident response unit.

Sec. 2063.203. DIGITAL FORENSICS LABORATORY. (a) Requires the command to establish a digital forensics laboratory to:

(1) in collaboration with the cybersecurity incident response unit under Section 2063.202, develop certain procedures;

(2) develop and share with relevant state agencies and covered entities cyber threat hunting tools and procedures to assist in identifying indicators of a compromise in the cybersecurity of state information systems and non-state information systems, as appropriate, for proactive discovery of latent intrusions;

(3) conduct analyses of causes of cybersecurity incidents and of remediation options;

(4) conduct assessments of the scope of harm caused by cybersecurity incidents, including data loss, compromised systems, and system disruptions;

(5) provide information and training to state agencies and covered entities on producing reports required by regulatory and auditing bodies;

(6) in collaboration with the Texas Department of Public Safety, the Texas Military Department, the office of the attorney general, and other state agencies, provide forensic analysis of a cybersecurity incident to support an investigation, attribution process, or other law enforcement or judicial action; and

(7) undertake any other activities necessary to carry out the duties described by this subsection.

(b) Requires the chief to employ a director for the digital forensics laboratory.

Sec. 2063.205. POLICIES. Requires the command to adopt policies and procedures necessary to enable the entities established in this subchapter to carry out their respective duties and purposes.

SUBCHAPTER E. CYBERSECURITY PREPARATION AND PLANNING

Sec. 2063.404. ONGOING INFORMATION TRANSMISSIONS. Requires that information received from state agencies by DIR under Section 2054.069 (Prioritized Cybersecurity and Legacy System Projects Report) be transmitted by DIR to the command on an ongoing basis.

SECTION 2. Transfers Section 2054.510, Government Code, to Subchapter A, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.0025, Government Code, and amends it, as follows:

Sec. 2063.0025. New heading. COMMAND CHIEF. Redesignates existing Section 2054.510 as Section 2063.0025. (a) Defines "state cybersecurity program." Deletes existing definition of "state information security program."

(b) Provides that the chief directs the day-to-day operations and policies of the command and oversees and is responsible for all functions and duties of the command. Deletes existing text requiring the executive director of DIR (executive director), using existing funds, to employ a chief information security officer.

(c) Requires the chief, rather than the chief information security officer, to oversee cybersecurity matters for this state including:

(1) implementing the duties described by Section 2063.059, rather than 2054.059 (Cybersecurity);

(2) developing a statewide cybersecurity, rather than information security, framework;

(3) overseeing the development of cybersecurity, rather than statewide information security, policies and standards;

(4) and collaborating with governmental entities and other entities, rather than state agencies, local governmental entities, and other entities operating or exercising control over state information systems or state-controlled data critical to strengthen this state's cybersecurity and information security policies, standards, and guidelines;

(5) overseeing the implementation of the policies, standards, and requirements, rather than guidelines, developed under this chapter, rather than under Subdivisions (3) and (4);

(6) makes conforming and nonsubstantive changes to this subsection;

(7) providing strategic direction to the network security center established under Section 2059.101 (Network Security Center) and regional security operations centers operated under Subchapter G (Project Management Practices), rather than statewide technology centers operated under Subchapter L (Statewide Technology Centers); and

(8) overseeing the preparation and submission of the report described by Section 2063.301, rather than Section 2054.0591 (Cybersecurity Report).

Makes nonsubstantive changes to this subsection.

SECTION 3. Transfers Section 2054.0592, Government Code, to Subchapter A, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.006, Government Code, and amends it, as follows:

Sec. 2063.006. CYBERSECURITY EMERGENCY FUNDING. Redesignates existing Section 2054.0592 as Section 2063.006. Authorizes the command, rather than DIR, if a cybersecurity event creates a need for emergency funding, to request that the governor or Legislative Budget Board (LBB) make a proposal under Chapter 317 (State Budget Execution) to provide funding to manage the operational and financial impacts from the cybersecurity event.

SECTION 4. Transfers Section 2054.519, Government Code, to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.102, Government Code, and amends it, as follows:

Sec. 2063.102. STATE CERTIFIED CYBERSECURITY TRAINING PROGRAMS. Redesignates existing Section 2054.519 as Section 2063.102. (a) Makes conforming changes to this subsection.

(b) Requires that a cybersecurity training program, to be certified under Subsection (a):

(1) focus on forming appropriate cybersecurity habits, rather than information security habits, and procedures that protect information resources; and

(2) teach best practices and minimum standards established under this subchapter, rather than teach best practices for detecting, assessing, reporting, and addressing information security threats.

(c)-(e) Makes conforming changes to these subsections.

SECTION 5. Transfers Section 2054.5191, Government Code, to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.103, Government Code, and amends it, as follows:

Sec. 2063.103. New heading: CYBERSECURITY TRAINING REQUIRED. Redesignates existing Section 2054.5191 as Section 2063.103. (a) Requires each elected or appointed official and employee of a governmental entity who has access to the entity's information resources or information resources technologies to annually complete a cybersecurity training program certified under Section 2063.102. Deletes existing text requiring each state agency to identify state employees who use a computer to complete at least 25 percent of the employee's required duties. Deletes existing text requiring an employee identified by the state agency and each elected or appointed officer of the agency, at least once each year, to complete a cybersecurity training program certified under Section 2054.519. Makes a conforming change.

Deletes existing text of Subsection (a-1)(1) requiring a local government, at least once each year, to identify local government employees and elected and appointed officials who have access to a local government computer system or database and use a computer to perform at least 25 percent of the employee's or official's required duties. Deletes existing text of Subsection (a-1)(2) requiring a local government, at least once each year, to require the employees and officials identified under to complete a cybersecurity training program certified under Section 2054.519.

(b) Redesignates existing Subsection (a-2) as Subsection (b). Authorizes the governing body of a governmental entity or the governing body's designee to deny access to the governmental entity's information resources or information resources technologies to an employee or official who is noncompliant with the requirements of Subsection (a).

Deletes existing Subsection (a-2) authorizing the governing body of a local government of the governing body's designee to deny access to the local

government's computer system or database to an individual described by Subsection (a-1)(1) who the governing body or the governing body's designee determines is noncompliant with the requirements of Subsection (a-1)(2).

(c) Redesignates existing Subsection (b) as Subsection (c). Makes conforming changes.

(d) Redesignates existing Subsection (c) as Subsection (d). Authorizes a state agency to select the most appropriate cybersecurity training program certified under Section 2063.102 for employees and officials of the state agency. Makes conforming changes.

(e) Redesignates existing Subsection (d) as Subsection (e) and makes no further changes.

(f) Redesignates existing Subsection (e) as Subsection (f). Requires the command to develop a form for use by governmental entities, rather than state agencies and local governments, in verifying completion of cybersecurity training program requirements under this section. Makes a conforming change.

(g) Redesignates existing Subsection (f) as Subsection (g). Provides that the requirements of Subsection (a), rather than Subsections (a) and (a-1), do not apply to employees and officials who have been:

(1)-(2) makes no changes to these subdivisions;

(3) granted leave related to a sickness or disability covered by workers' compensation benefits, if that employee or official no longer has access to the governmental entity's information resources or information resources technologies, rather than the state agency's or local government's database and systems;

(4) makes conforming changes to this subdivision; or

(5) denied access to a governmental entity's information resources or information resources technologies under Subsection (b) for noncompliance with the requirements of Subsection (a), rather than denied access to a local government's computer system or database by the governing body of the local government or the governing body's designee under Subsection (a-2) for noncompliance with the requirements of Subsection (a-1)(2).

SECTION 6. Transfers Section 2054.5192, Government Code, to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.104, Government Code, and amends it, as follows:

Sec. 2063.104. CYBERSECURITY TRAINING REQUIRED: CERTAIN STATE CONTRACTORS. Redesignates existing Section 2054.5192 as Section 2063.104. (a) Makes no changes to this subsection.

(b) Makes a conforming change to this subsection.

(c)-(d) Makes no changes to these subsections.

(e) Makes a conforming change to this subsection.

SECTION 7. Transfers Section 2054.0594, Government Code, to Subchapter C, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.204, Government Code, and amends it, as follows:

Sec. 2063.204. INFORMATION SHARING AND ANALYSIS ORGANIZATION. Redesignates existing Section 2054.0594 as Section 2063.204. (a) Requires the command to establish at least one, rather than an, information sharing and analysis organization to provide a forum for certain entities to share information regarding cybersecurity threats, best practices, and remediation strategies. Makes a conforming change.

(b) Redesignates existing Subsection (c) as Subsection (b). Deletes text of existing Subsection (b) requiring DIR to provide administrative support to the information sharing and analysis organization.

(c) Redesignates existing Subsection (d) as Subsection (c). Requires the command to establish framework for regional cybersecurity task forces, rather than working groups, to execute mutual aid agreements that allow certain entities, including the regional security operations centers under Subchapter G and the cybersecurity incident response unit under Section 2063.202, rather than including the incident response team established under Subchapter N-2, to assist with responding to a cybersecurity event, rather than incident, in this state. Makes conforming changes.

SECTION 8. Amends Chapter 2063, Government Code, as added by this Act, by adding Subchapter D, and adds a heading to that subchapter, to read as follows:

SUBCHAPTER D. REPORTING

SECTION 9. Transfers Sections 2054.0591, 2054.603, and 2054.077, Government Code, to Subchapter D, Chapter 2063, Government Code, as added by this Act, redesignates them as Sections 2063.301, 2063.302, and 2063.303, Government Code, respectively, and amends them, as follows:

Sec. 2063.301. CYBERSECURITY REPORT. Redesignates existing Section 2054.0591 as Section 2063.301. (a) Deletes existing text requiring that the cybersecurity report include an evaluation of a program that provides an information security officer to assist small state agencies and local governments that are unable to justify hiring a full-time information security officer. Makes conforming and nonsubstantive changes.

(b) Requires the command, not later than October 1 of each even-numbered year, to submit a report to the LBB that prioritizes, for the purpose of receiving funding, state agency cybersecurity projects. Requires each state agency to coordinate with the command to implement this section.

(c) Redesignates existing Subsection (b) as Subsection (c). Provides that the disclosure of information under this section is not a voluntary disclosure for purposes of Section 552.007 (Voluntary Disclosure of Certain Information When Disclosure Not Required). Makes a conforming change.

Sec. 2063.302. New heading: CYBERSECURITY INCIDENT NOTIFICATION BY STATE AGENCY OR LOCAL GOVERNMENT. Redesignates existing Section 2054.603 as Section 2063.302. (a) Redesignates existing Subsection (b) as Subsection (a) and makes conforming changes. Deletes existing definitions of "security incident" and "sensitive personal information."

(b)-(c) Redesignates existing Subsections (c) and (d) as Subsections (b) and (c). Makes conforming changes.

Sec. 2063.303. VULNERABILITY REPORTS. Redesignates existing Section 2054.077 as Section 2063.303. (a)-(c) Makes no changes to these subsections.

(d) Makes a conforming change to this subsection.

(e) Deletes existing text providing that the summary of a state agency's vulnerability test is available to the public on request.

SECTION 10. Transfers Section 2054.136, Government Code, to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2053.401, Government Code, and amends it, as follows:

Sec. 2053.401. DESIGNATED INFORMATION SECURITY OFFICER. Redesignates existing Section 2054.136 as Section 2053.401. Requires each state agency to designate an information security officer who meets certain requirements, including possessing the training and experience required to ensure the agency complies with requirements and policies established by the command, rather than the training and experience required to perform the duties required by DIR rules.

SECTION 11. Transfers Section 2054.518, Government Code, to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.402, Government Code, and amends it, as follows:

Sec. 2063.402. CYBERSECURITY RISKS AND INCIDENTS. Redesignates existing Section 2054.518 as Section 2063.402. (a) Makes conforming changes to this subsection.

(b) Makes conforming changes to this subsection.

(c) Redesignates existing Subsection (d) as Subsection (c). Makes a conforming change to this subsection.

SECTION 12. Transfers Section 2054.133, Government Code, to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.403, Government Code, and amends it, as follows:

Sec. 2063.403. INFORMATION SECURITY PLAN. Redesignates existing Section 2054.133 as Section 1063.403. (a) Makes no changes to this subsection.

(b) Requires each state agency, in developing the information security plan, to take certain actions, including by including the best practices for information security developed by the command or, if best practices are not applied, a written explanation of why the best practices are not sufficient for the agency's security. Makes conforming changes.

(c) Makes conforming changes to this subsection.

(d)-(e) Makes no changes to these subsections.

(f) Requires the command, not later than November 15 of each even-numbered year, to submit a written report to the governor, the lieutenant governor, the speaker of the house of representatives, and each standing committee of the legislature with primary jurisdiction over matters related to the command evaluating information security for this state's information resources. Requires the command to omit from any written copies of the report information that could expose specific vulnerabilities, rather than specific vulnerabilities in the security of this state's information resources. Makes conforming changes.

SECTION 13. Transfers Section 2054.516, Government Code, to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.405, Government Code, and amends it, as follows:

Sec. 2063.405. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. Redesignates existing Section 2054.516 as Section 2063.405. (a)-(b) Makes conforming changes to these subsections.

SECTION 14. Transfers Section 2054.512, Government Code, to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.406, Government Code, and amends it, as follows:

Sec. 2063.406. CYBERSECURITY COUNCIL. Redesignates existing Section 2054.512 as Section 2063.406. (a) Requires the chief or the chief's designee to lead, rather than requires the state cybersecurity coordinator to establish and lead, a cybersecurity council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning this state.

(b) Requires the cybersecurity council to include certain members, including the director of the Elections Division of the Office of the Secretary of State (SOS), rather than one member who is an employee of the Elections Division of the Office of SOS, one member who is an employee of DIR, and additional members appointed by the chief, rather than appointed by the state cybersecurity coordinator.

(c) Provides that members of the cybersecurity council serve staggered six-year terms, with as near as possible to one-third of the members' terms expiring February 1 of each odd-numbered year.

(d) Creates this subsection from existing text and makes a conforming change.

(e) Redesignates existing Subsection (d) as Subsection (e). Requires the cybersecurity council to take certain actions, including consider the costs and benefits of establishing a computer emergency readiness team to address cybersecurity incidents, rather than cyber attacks, occurring in this state during routine and emergency situations.

(f) Redesignates existing Subsection (e) as Subsection (f). Requires the chief, in collaboration with the cybersecurity council, to provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state.

SECTION 15. Transfers Section 2054.514, Government Code, to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignates it as Section 2063.407, Government Code, and amends it, as follows:

Sec. 2063.407. RECOMMENDATIONS. Redesignates existing Section 2054.514 as Section 2063.407. (a) Authorizes the chief, rather than the state cybersecurity coordinator, to implement any portion, of all of the recommendations made by the cybersecurity council under Section 2063.406, rather than made by the Cybersecurity, Education, and Economic Development Council under Subchapter N.

SECTION 16. Transfers Subchapter N-2, Chapter 2054, Government Code, to Chapter 2063, Government Code, as added by this Act, redesignates it as Subchapter F, Government Code, and amends it, as follows:

SUBCHAPTER F. TEXAS VOLUNTEER INCIDENT RESPONSE TEAM

Sec. 2063.501. DEFINITIONS. Redesignates existing Section 2054.52001 as Section 2063.501. Redefines "incident response team," "participating entity," and "volunteer."

Sec. 2063.502. ESTABLISHMENT OF TEXAS VOLUNTEER INCIDENT RESPONSE TEAM. Redesignates existing Section 2054.52002 as Section 2063.502. (a)-(b) Makes conforming changes to these subsections.

Sec. 2063.503. CONTRACT WITH VOLUNTEERS. Redesignates existing Section 2054.52003 as Section 2063.503. Makes conforming changes.

Sec. 2063.504. VOLUNTEER QUALIFICATION. Redesignates existing Section 2054.52004 as Section 2063.504. Makes conforming changes.

Sec. 2063.505. DEPLOYMENT. Redesignates existing Section 2054.52005 as Section 2063.505. (a) Makes conforming changes to this subsection.

(b) Makes no changes to this subsection.

Sec. 2063.506. CYBERSECURITY COUNCIL DUTIES. Redesignates existing Section 2054.52006 as Section 2063.506. Makes conforming changes.

Sec. 2063.507. New heading: COMMAND POWERS AND DUTIES. Redesignates existing Section 2054.52007 as Section 2063.507. (a) Requires the command to take certain actions, including adopting policies, rather than rules, necessary to implement this subchapter. Makes conforming changes.

(b) Deletes existing text requiring that the contract entered into by a participating entity comply with the requirements of Chapters 771 (Interagency Cooperation Act) and 791 (Interlocal Cooperation Contracts). Makes a conforming change.

(c)-(e) Makes conforming changes to these subsections.

Sec. 2063.508. STATUS OF VOLUNTEER; LIABILITY. Redesignates existing Section 2054.52008 as Section 2063.508 and makes no further changes.

Sec. 2063.509. CIVIL LIABILITY. Redesignates existing Section 2054.52009 as Section 2063.509. Makes conforming changes.

Sec. 2063.510. CONFIDENTIAL INFORMATION. Redesignates existing Section 2054.52010 as Section 2063.510. Makes conforming changes.

SECTION 17. Transfers Subchapter E, Chapter 2059, Government Code, to Chapter 2063, Government Code, as added by this Act, redesignates it as Subchapter G, Chapter 2063, and amends it, as follows:

SUBCHAPTER G. REGIONAL SECURITY OPERATIONS CENTERS

Sec. 2063.601. ELIGIBLE PARTICIPATING ENTITIES. Redesignates existing Section 2059.201 as Section 2063.601. Provides that a state agency or entity listed in Section 2059.058 (Agreement to Provide Network Security Services to Entities Other Than State Agencies) is eligible to participate in cybersecurity support and network security provided by a regional security operations center, rather than a regional network security center, under this subchapter.

Sec. 2063.602. New heading: ESTABLISHMENT OF REGIONAL SECURITY OPERATIONS CENTER. Redesignates existing Section 2059.202 as Section 2063.602. (a)-(c) Makes conforming changes to these subsections.

Sec. 2063.603. New heading: REGIONAL NETWORK SECURITY OPERATIONS CENTER LOCATIONS AND PHYSICAL SECURITY. Redesignates existing Section 2059.203 as Section 2063.603. (a) Authorizes, rather than requires, the command, in creating and operating a regional security operations center, rather than a regional network security center, to partner with another university system or institution of higher education as defined by Section 61.003 (Definitions), Education Code, other than a public junior college. Makes conforming and nonsubstantive changes.

(b)-(e) Makes conforming changes to these subsections.

Sec. 2063.604. New heading: REGIONAL SECURITY OPERATIONS CENTERS SERVICES AND SUPPORT. Redesignates existing Section 2059.204 as Section

2063.604. Authorizes the command to offer certain managed security services through a regional security operations center, including immediate response to counter unauthorized activity, rather than network security activity, that exposes this state and the residents of this state to risk, including complete intrusion detection system installation, management, and monitoring for participating entities. Makes conforming changes.

Sec. 2063.605. NETWORK SECURITY GUIDELINES AND STANDARD OPERATING PROCEDURES. Redesignates existing Section 2059.205 as Section 2063.605. Makes conforming changes.

SECTION 18. Amends Section 325.011, Government Code, as follows:

Sec. 325.011. CRITERIA FOR REVIEW. Requires the Sunset Advisory Commission and its staff to consider certain criteria in determining whether a public need exists for the continuation of a state agency or its advisory committees or for the performance of the functions of the agency or its advisory committees, including an assessment of the agency's cybersecurity practices using confidential information available from the command.

SECTION 19. Amends Section 11.175(h-1), Education Code, to make a conforming change.

SECTION 20. Amends Section 38.307(e), Education Code, to make a conforming change.

SECTION 21. Amends Section 61.003(6), Education Code, to redefine "other agency of higher education."

SECTION 22. Amends Section 65.02(a), Education Code, to provide that the UT System is composed of certain institutions and entities, including the Texas Cyber Command (Chapter 2063, Government Code), and to make nonsubstantive changes.

SECTION 23. Amends Sections 772.012(b) and (c), Government Code, to make conforming changes.

SECTION 24. Amends Section 2054.0701(c), Government Code, to make conforming changes.

SECTION 25. Amends Section 2056.002(b), Government Code, to make conforming changes.

SECTION 26. Repealer: Section 2054.5181 (Cyberstar Program; Certificate of Approval), Government Code.

SECTION 27. (a) Defines "department."

(b) Provides that, on the effective date of this Act, the command, organized as provided by Section 2063.002, Government Code, as added by this Act, is created with the powers and duties assigned by Chapter 2063, Government Code, as added by this Act.

(b-1) Requires the governor, as soon as practicable on or after the effective date of this Act, to appoint the chief of the command, as described by Section 2063.0025, Government Code, as added by this Act.

(c) Requires DIR, notwithstanding Subsection (b) of this section, to continue to perform duties and exercise powers under Chapter 2054 (Information Resources), Government Code, as that law existed immediately before the effective date of this Act, until the date provided by the memorandum of understanding entered into under Subsection (e) of this section.

(d) Provides that, not later than December 31, 2026:

(1) all functions and activities performed by DIR that relate to cybersecurity under Chapter 2063, Government Code, as added by this Act, are transferred to the command;

(2) all employees of DIR who primarily perform duties related to cybersecurity, including employees who provide administrative support for those services, under Chapter 2063, Government Code, as added by this Act, become employees of the command, but continue to work in the same physical location unless moved in accordance with the memorandum of understanding entered into under Subsection (e) of this section;

(3) a rule or form adopted by DIR that relates to cybersecurity under Chapter 2063, Government Code, as added by this Act, is a rule or form of the command and remains in effect until changed by the command;

(4) a reference in law to DIR that relates to cybersecurity under Chapter 2063, Government Code, as added by this Act, means the command;

(5) a contract negotiation for a contract specified as provided by Subdivision (7) of this subsection in the memorandum of understanding entered into under Subsection (e) of this section or other proceeding involving DIR that is related to cybersecurity under Chapter 2063, Government Code, as added by this Act, is transferred without change in status to the command, and the command assumes, without a change in status, the position of DIR in a negotiation or proceeding relating to cybersecurity to which DIR is a party;

(6) all money, leases, rights, and obligations of DIR related to cybersecurity under Chapter 2063, Government Code, as added by this Act, are transferred to the command;

(7) contracts specified as necessary to accomplish the goals and duties of the command, as established by Chapter 2063, Government Code, as added by this Act, in the memorandum of understanding entered into under Subsection (e) of this section are transferred to the command;

(8) all property, including records, in the custody of DIR related to cybersecurity under Chapter 2063, Government Code, as added by this Act, becomes property of the command, but stays in the same physical location unless moved in accordance with the specific steps and methods created under Subsection (e) of this section; and

(9) all funds appropriated by the legislature to DIR for purposes related to cybersecurity, including funds for providing administrative support, under Chapter 2063, Government Code, as added by this Act, are transferred to the command.

(e) Requires DIR, in collaboration with the chief and the board of regents of the UT system, not later than January 1, 2026, to enter into a memorandum of understanding relating to the transfer of powers and duties from DIR to the command as provided by this Act. Requires that the memorandum include:

(1) a timetable and specific steps and methods for the transfer of all powers, duties, obligations, rights, contracts, leases, records, real or personal property, and unspent and unobligated appropriations and other funds relating to the administration of the powers and duties as provided by this Act;

(2) measures to ensure against any unnecessary disruption to cybersecurity operations during the transfer process; and

(3) a provision that the terms of any memorandum of understanding entered into related to the transfer remain in effect until the transfer is completed.

SECTION 28. Effective date: September 1, 2025.