# SENATE AMENDMENTS

**2nd Printing**

By: Capriglione, Bonnen, Hefner, Lujan, Lopez of Bexar, et al. H.B. No. 150

A BILL TO BE ENTITLED

AN ACT

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.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2063 to read as follows:

CHAPTER 2063. TEXAS CYBER COMMAND

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 2063.001. DEFINITIONS. In this chapter:

(1) "Chief" means the chief of the Texas Cyber Command.

(2) "Command" means the Texas Cyber Command established under this chapter.

(3) "Covered entity" means a private entity operating critical infrastructure or a local government that the command contracts with in order to provide cybersecurity services under this chapter.

(4) "Critical infrastructure" means infrastructure in this state vital to the security, governance, public health and safety, economy, or morale of the state or the nation, including:

(A) chemical facilities;

(B) commercial facilities;

(C) communication facilities;

(D) manufacturing facilities;

(E) dams;

(F) defense industrial bases;

(G) emergency services systems;

(H) energy facilities;

(I) financial services systems;

(J) food and agriculture facilities;

(K) government facilities;

(L) health care and public health facilities;

(M) information technology and information technology systems;

(N) nuclear reactors, materials, and waste;

(O) transportation systems; or

(P) water and wastewater systems.

(5) "Cybersecurity" means the measures taken for a computer, computer network, computer system, or other technology infrastructure to protect against, respond to, and recover from unauthorized:

(A) use, access, disruption, modification, or destruction; or

(B) disclosure, modification, or destruction of information.

(6) "Cybersecurity incident" includes:

(A) a breach or suspected breach of system security as defined by Section 521.053, Business & Commerce Code;

(B) the introduction of ransomware, as defined by

Section 33.023, Penal Code, into a computer, computer network, or computer system; or

(C) any other cybersecurity-related occurrence that jeopardizes information or an information system designated by command policy adopted under this chapter.

(7) "Department" means the Department of Information Resources.

(8) "Governmental entity" means a state agency.

(9) "Information resources" has the meaning assigned by Section 2054.003, Government Code.

(10) "Information resources technologies" has the meaning assigned by Section 2054.003.

(11) "Local government" has the meaning assigned by Section 2054.003.

(12) "Sensitive personal information" has the meaning assigned by Section 521.002, Business & Commerce Code.

(13) "State agency" means:

(A) a department, commission, board, office, or other agency that is in the executive branch of state government and that was created by the constitution or a statute;

(B) the supreme court, the court of criminal appeals, a court of appeals, a district court, or the Texas Judicial Council or another agency in the judicial branch of state government; or

(C) a university system or an institution of higher education as defined by Section 61.003, Education Code.

Sec. 2063.002. ORGANIZATION. (a) The Texas Cyber Command

is a component of The University of Texas System and administratively attached to The University of Texas at San Antonio.

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

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

(d) Under an agreement with the command, The University of Texas at San Antonio shall provide administrative support services for the command as necessary to carry out the purposes of this chapter.

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

(b) The command is responsible for cybersecurity for this state, including:

(1) developing tools to enhance cybersecurity defenses;

(2) facilitating education and training of a cybersecurity workforce;

(3) developing cyber threat intelligence, monitoring information systems to detect and warn entities of cyber attacks,

proactively searching for cyber threats to critical infrastructure and state systems, developing and executing cybersecurity incident responses, and conducting digital forensics of cybersecurity incidents to support law enforcement and attribute the incidents;

(4) creating partnerships needed to effectively carry out the command's functions; and

(5) receiving all cybersecurity incident reports from state agencies and covered entities.

Sec. 2063.004. GENERAL POWERS AND DUTIES. (a) The command shall:

(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 to ensure information resources and information resources technologies obtained by the department 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) The command may:

(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) Except as otherwise provided by this chapter, the command shall 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. The command shall 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. 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, 2155.083, and 2155.132(c) in making the purchase.

Sec. 2063.008. RULES. The chief may adopt rules necessary for carrying out the purposes of this chapter.

Sec. 2063.009. APPLICATION OF SUNSET ACT. The command is subject to Chapter 325 (Texas Sunset Act). 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) The command shall 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) The command shall establish and periodically assess mandatory cybersecurity training that must be completed by all information resources employees of state agencies. The command shall consult with the Information Technology Council for Higher Education established under Section 2054.121 regarding applying the training requirements to employees of institutions of higher education.

(c) Except as otherwise provided by this subsection, the command shall adopt policies to ensure governmental entities are complying with the requirements of this section. The command shall adopt policies that ensure that a person who is not a citizen of the United States may not be 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) In this section, "center" means the cybersecurity threat intelligence center established under this section.

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

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

(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) The chief shall employ a director for the center.

Sec. 2063.202. CYBERSECURITY INCIDENT RESPONSE UNIT. (a) The command shall 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) The chief shall employ a director for the cybersecurity incident response unit.

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

(1) in collaboration with the cybersecurity incident

response unit under Section 2063.202, develop procedures to:

(A) preserve evidence of a cybersecurity incident, including logs and communication;

(B) document chains of custody; and

(C) timely notify and maintain contact with the appropriate law enforcement agencies investigating a cybersecurity incident;

(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 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) The chief shall employ a director for the digital forensics laboratory.

Sec. 2063.205. POLICIES. The command shall 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. Information received from state agencies by the department under Section 2054.069 shall be transmitted by the department to the command on an ongoing basis.

SECTION 2. Section 2054.510, Government Code, is transferred to Subchapter A, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.0025, Government Code, and amended to read as follows:

Sec. 2063.0025 [~~2054.510~~]. COMMAND CHIEF [~~INFORMATION SECURITY OFFICER~~]. (a) In this section, "state cybersecurity [~~information security~~] program" means the policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish the cybersecurity [~~information resources security~~] function for this state.

(b) 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. [~~The executive director, using existing funds, shall employ a chief information security officer.~~]

(c) The chief [~~information security officer~~] shall oversee cybersecurity matters for this state including:

(1) implementing the duties described by Section 2063.004 [~~2054.059~~];

(2) [~~responding to reports received under Section 2054.1125,~~

[~~(3)~~] developing a statewide cybersecurity [~~information security~~] framework;

(3) [~~(4)~~] overseeing the development of cybersecurity [~~statewide information security~~] policies and standards;

(4) [~~(5)~~] collaborating with [~~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) [~~(6)~~] overseeing the implementation of the policies, standards, and requirements [~~guidelines~~] developed under this chapter [~~Subdivisions (3) and (4)~~];

(6) [~~(7)~~] providing cybersecurity [~~information security~~] leadership, strategic direction, and coordination for the state cybersecurity [~~information security~~] program;

(7) [~~(8)~~] providing strategic direction to:

(A) the network security center established under Section 2059.101; and

(B) regional security operations [~~statewide technology~~] centers operated under Subchapter G [~~I~~]; and

(8) [~~(9)~~] overseeing the preparation and submission of the report described by Section 2063.301 [~~2054.0591~~].

SECTION 3. Section 2054.0592, Government Code, is transferred to Subchapter A, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.006, Government Code, and amended to read as follows:

Sec. 2063.006 [~~2054.0592~~]. CYBERSECURITY EMERGENCY FUNDING. If a cybersecurity event creates a need for emergency funding, the command [~~department~~] may request that the governor or Legislative Budget Board make a proposal under Chapter 317 to provide funding to manage the operational and financial impacts from the cybersecurity event.

SECTION 4. Section 2054.519, Government Code, is transferred to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.102, Government Code, and amended to read as follows:

Sec. 2063.102 [~~2054.519~~]. STATE CERTIFIED CYBERSECURITY TRAINING PROGRAMS. (a) The command [~~department~~], in consultation with the cybersecurity council established under Section 2063.406 [~~2054.512~~] and industry stakeholders, shall annually:

(1) certify at least five cybersecurity training programs for state and local government employees; and

(2) update standards for maintenance of certification by the cybersecurity training programs under this section.

(b) To be certified under Subsection (a), a cybersecurity training program must:

(1) focus on forming appropriate cybersecurity

[~~information security~~] habits and procedures that protect information resources; and

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

(c) The command [~~department~~] may identify and certify under Subsection (a) training programs provided by state agencies and local governments that satisfy the training requirements described by Subsection (b).

(d) The command [~~department~~] may contract with an independent third party to certify cybersecurity training programs under this section.

(e) The command [~~department~~] shall annually publish on the command's [~~department's~~] Internet website the list of cybersecurity training programs certified under this section.

SECTION 5. Section 2054.5191, Government Code, is transferred to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.103, Government Code, and amended to read as follows:

Sec. 2063.103 [~~2054.5191~~]. CYBERSECURITY TRAINING REQUIRED [~~: CERTAIN EMPLOYEES AND OFFICIALS~~]. (a) Each elected or appointed official and employee of a governmental entity who has access to the entity's information resources or information resources technologies [~~state agency shall identify state employees who use a computer to complete at least 25 percent of the employee's required duties. At least once each year, an employee identified by the state agency and each elected or appointed officer of the agency~~]

shall annually complete a cybersecurity training program certified under Section 2063.102 [~~2054.519~~].

(b) [~~(a-1) At least once each year, a local government shall:~~

[~~(1) 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; and~~

[~~(2) require the employees and officials identified under Subdivision (1) to complete a cybersecurity training program certified under Section 2054.519.~~

[~~(a-2)~~] The governing body of a governmental entity [~~local government~~] or the governing body's designee may deny access to the governmental entity's information resources or information resources technologies [~~local government's computer system or database~~] to an employee or official [~~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) [~~(a-1)(2)~~].

(c) [~~(b)~~] The governing body of a local government may select the most appropriate cybersecurity training program certified under Section 2063.102 [~~2054.519~~] for employees and officials of the local government to complete. The governing body shall:

(1) verify and report on the completion of a cybersecurity training program by employees and officials of the local government to the command [~~department~~]; and

(2) require periodic audits to ensure compliance with this section.

(d) [~~(c)~~] A state agency may select the most appropriate cybersecurity training program certified under Section 2063.102 [~~2054.519~~] for employees and officials of the state agency. The executive head of each state agency shall verify completion of a cybersecurity training program by employees and officials of the state agency in a manner specified by the command [~~department~~].

(e) [~~(d)~~] The executive head of each state agency shall periodically require an internal review of the agency to ensure compliance with this section.

(f) [~~(e)~~] The command [~~department~~] shall develop a form for use by governmental entities [~~state agencies and local governments~~] in verifying completion of cybersecurity training program requirements under this section. The form must allow the state agency and local government to indicate the percentage of employee and official completion.

(g) [~~(f)~~] The requirements of Subsection [~~Subsections~~] (a) [~~and (a-1)~~] do not apply to employees and officials who have been:

(1) granted military leave;

(2) granted leave under the federal Family and Medical Leave Act of 1993 (29 U.S.C. Section 2601 et seq.);

(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 [~~state agency's or local government's database and systems~~];

(4) granted any other type of extended leave or authorization to work from an alternative work site if that employee or official no longer has access to the governmental entity's information resources or information resources technologies [~~state agency's or local government's database and systems~~]; or

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

SECTION 6. Section 2054.5192, Government Code, is transferred to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.104, Government Code, and amended to read as follows:

Sec. 2063.104 [~~2054.5192~~]. CYBERSECURITY TRAINING REQUIRED: CERTAIN STATE CONTRACTORS. (a) In this section, "contractor" includes a subcontractor, officer, or employee of the contractor.

(b) A state agency shall require any contractor who has access to a state computer system or database to complete a cybersecurity training program certified under Section 2063.102 [~~2054.519~~] as selected by the agency.

(c) The cybersecurity training program must be completed by a contractor during the term of the contract and during any renewal period.

(d) Required completion of a cybersecurity training program must be included in the terms of a contract awarded by a state agency to a contractor.

(e) A contractor required to complete a cybersecurity training program under this section shall verify completion of the program to the contracting state agency. The person who oversees contract management for the agency shall:

(1) not later than August 31 of each year, report the contractor's completion to the command [~~department~~]; and

(2) periodically review agency contracts to ensure compliance with this section.

SECTION 7. Section 2054.0594, Government Code, is transferred to Subchapter C, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.204, Government Code, and amended to read as follows:

Sec. 2063.204 [~~2054.0594~~]. INFORMATION SHARING AND ANALYSIS ORGANIZATION. (a) The command [~~department~~] shall establish at least one [~~an~~] information sharing and analysis organization to provide a forum for state agencies, local governments, public and private institutions of higher education, and the private sector to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) [~~The department shall provide administrative support to the information sharing and analysis organization.~~

[~~(c)~~] A participant in the information sharing and analysis organization shall assert any exception available under state or federal law, including Section 552.139, in response to a request

for public disclosure of information shared through the organization. Section 552.007 does not apply to information described by this subsection.

(c) [~~(d)~~] The command [~~department~~] shall establish a framework for regional cybersecurity task forces [~~working groups~~] to execute mutual aid agreements that allow state agencies, local governments, regional planning commissions, public and private institutions of higher education, the private sector, the regional security operations centers under Subchapter G, and the cybersecurity incident response unit under Section 2063.202 [~~and the incident response team established under Subchapter N-2~~] to assist with responding to a cybersecurity incident [~~event~~] in this state. A task force [~~working group~~] may be established within the geographic area of a regional planning commission established under Chapter 391, Local Government Code. The task force [~~working group~~] may establish a list of available cybersecurity experts and share resources to assist in responding to the cybersecurity incident [~~event~~] and recovery from the incident [~~event~~].

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

SUBCHAPTER D. REPORTING

SECTION 9. Sections 2054.0591, 2054.603, and 2054.077, Government Code, are transferred to Subchapter D, Chapter 2063, Government Code, as added by this Act, redesignated as Sections 2063.301, 2063.302, and 2063.303, Government Code, respectively, and amended to read as follows:

Sec. 2063.301 [~~2054.0591~~]. CYBERSECURITY REPORT. (a) Not later than November 15 of each even-numbered year, the command [~~department~~] shall submit to the governor, the lieutenant governor, the speaker of the house of representatives, and the standing committee of each house of the legislature with primary jurisdiction over state government operations a report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in this state. The report must include:

(1) an assessment of the resources available to address the operational and financial impacts of a cybersecurity event;

(2) a review of existing statutes regarding cybersecurity and information resources technologies; and

(3) recommendations for legislative action to increase the state's cybersecurity and protect against adverse impacts from a cybersecurity incident [~~event; and~~

[~~(4) 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~~].

(b) Not later than October 1 of each even-numbered year, the command shall submit a report to the Legislative Budget Board that prioritizes, for the purpose of receiving funding, state agency cybersecurity projects. Each state agency shall coordinate with the command to implement this subsection.

(c) [~~(b)~~] The command [~~department~~] or a recipient of a report under this section may redact or withhold information

confidential under Chapter 552, including Section 552.139, or other state or federal law that is contained in the report in response to a request under Chapter 552 without the necessity of requesting a decision from the attorney general under Subchapter G, Chapter 552. The disclosure of information under this section is not a voluntary disclosure for purposes of Section 552.007.

Sec. 2063.302 [~~2054.603~~]. CYBERSECURITY [~~SECURITY~~] INCIDENT NOTIFICATION BY STATE AGENCY OR LOCAL GOVERNMENT. (a) [~~In this section:~~

[~~(1) "Security incident" means:~~

[~~(A) a breach or suspected breach of system security as defined by Section 521.053, Business & Commerce Code; and~~

[~~(B) the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or computer system.~~

[~~(2) "Sensitive personal information" has the meaning assigned by Section 521.002, Business & Commerce Code.~~

[~~(b)~~] A state agency or local government that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a cybersecurity [~~security~~] incident:

(1) comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state;

(2) not later than 48 hours after the discovery of the

cybersecurity [~~security~~] incident, notify:

(A) the command [~~department~~], including the chief [~~information security officer~~]; or

(B) if the cybersecurity [~~security~~] incident involves election data, the secretary of state; and

(3) comply with all command [~~department~~] rules relating to reporting cybersecurity [~~security~~] incidents as required by this section.

(b) [~~(c)~~] Not later than the 10th business day after the date of the eradication, closure, and recovery from a cybersecurity [~~security~~] incident, a state agency or local government shall notify the command [~~department~~], including the chief [~~information security officer~~], of the details of the cybersecurity [~~security~~] incident and include in the notification an analysis of the cause of the cybersecurity [~~security~~] incident.

(c) [~~(d)~~] This section does not apply to a cybersecurity [~~security~~] incident that a local government is required to report to an independent organization certified by the Public Utility Commission of Texas under Section 39.151, Utilities Code.

Sec. 2063.303 [~~2054.077~~]. VULNERABILITY REPORTS. (a) In this section, a term defined by Section 33.01, Penal Code, has the meaning assigned by that section.

(b) The information security officer of a state agency shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than June 1 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a

printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

(c) Except as provided by this section, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential and is not subject to disclosure under Chapter 552.

(d) The information security officer shall provide an electronic copy of the vulnerability report on its completion to:

(1) the command [~~department~~];

(2) the state auditor;

(3) the agency's executive director;

(4) the agency's designated information resources manager; and

(5) any other information technology security oversight group specifically authorized by the legislature to receive the report.

(e) Separate from the executive summary described by Subsection (b), a state agency shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices,

computer software, data processing, or electronically stored information. [~~The summary is available to the public on request.~~]

SECTION 10. Section 2054.136, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.401, Government Code, and amended to read as follows:

Sec. 2063.401 [~~2054.136~~]. DESIGNATED INFORMATION SECURITY OFFICER. Each state agency shall designate an information security officer who:

(1) reports to the agency's executive-level management;

(2) has authority over information security for the entire agency;

(3) possesses the training and experience required to ensure the agency complies with requirements and policies established by the command [~~perform the duties required by department rules~~]; and

(4) to the extent feasible, has information security duties as the officer's primary duties.

SECTION 11. Section 2054.518, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.402, Government Code, and amended to read as follows:

Sec. 2063.402 [~~2054.518~~]. CYBERSECURITY RISKS AND INCIDENTS. (a) The command [~~department~~] shall develop a plan to address cybersecurity risks and incidents in this state. The command [~~department~~] may enter into an agreement with a national

organization, including the National Cybersecurity Preparedness Consortium, to support the command's [~~department's~~] efforts in implementing the components of the plan for which the command [~~department~~] lacks resources to address internally. The agreement may include provisions for:

(1) providing technical assistance services to support preparedness for and response to cybersecurity risks and incidents;

(2) conducting cybersecurity simulation exercises for state agencies to encourage coordination in defending against and responding to cybersecurity risks and incidents;

(3) assisting state agencies in developing cybersecurity information-sharing programs to disseminate information related to cybersecurity risks and incidents; and

(4) incorporating cybersecurity risk and incident prevention and response methods into existing state emergency plans, including continuity of operation plans and incident response plans.

(b) In implementing the provisions of the agreement prescribed by Subsection (a), the command [~~department~~] shall seek to prevent unnecessary duplication of existing programs or efforts of the command [~~department~~] or another state agency.

(c) [~~(d)~~] The command [~~department~~] shall consult with institutions of higher education in this state when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.

SECTION 12. Section 2054.133, Government Code, is

transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.403, Government Code, and amended to read as follows:

Sec. 2063.403 [~~2054.133~~]. INFORMATION SECURITY PLAN. (a) Each state agency shall develop, and periodically update, an information security plan for protecting the security of the agency's information.

(b) In developing the plan, the state agency shall:

(1) consider any vulnerability report prepared under Section 2063.303 [~~2054.077~~] for the agency;

(2) incorporate the network security services provided by the department to the agency under Chapter 2059;

(3) identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;

(4) identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction;

(5) include:

(A) the best practices for information security developed by the command [~~department~~]; or

(B) if best practices are not applied, a written explanation of why the best practices are not sufficient for the agency's security; and

(6) omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems.

(c) Not later than June 1 of each even-numbered year, each state agency shall submit a copy of the agency's information security plan to the command [~~department~~]. Subject to available resources, the command [~~department~~] may select a portion of the submitted security plans to be assessed by the command [~~department~~] in accordance with command policies [~~department rules~~].

(d) Each state agency's information security plan is confidential and exempt from disclosure under Chapter 552.

(e) Each state agency shall include in the agency's information security plan a written document that is signed by the head of the agency, the chief financial officer, and each executive manager designated by the state agency and states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan.

(f) Not later than November 15 of each even-numbered year, the command [~~department~~] shall 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 [~~department~~] evaluating information security for this state's information resources. In preparing the report, the command [~~department~~] shall consider the information security plans submitted by state agencies under this section, any vulnerability reports submitted under Section 2063.303 [~~2054.077~~], and other available information regarding the security of this state's information resources. The command [~~department~~] shall omit from any written copies of the report information that could expose

specific vulnerabilities [~~in the security of this state's information resources~~].

SECTION 13. Section 2054.516, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.405, Government Code, and amended to read as follows:

Sec. 2063.405 [~~2054.516~~]. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. (a) Each state agency implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must:

(1) submit a biennial data security plan to the command [~~department~~] not later than June 1 of each even-numbered year to establish planned beta testing for the website or application; and

(2) subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

(b) The command [~~department~~] shall review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan to the state agency as soon as practicable after the command [~~department~~] reviews the plan.

SECTION 14. Section 2054.512, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.406, Government Code, and amended to read as follows:

Sec. 2063.406 [~~2054.512~~]. CYBERSECURITY COUNCIL. (a) The

chief or the chief's designee [~~state cybersecurity coordinator~~] shall [~~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) The cybersecurity council must include:

(1) one member who is an employee of the office of the governor;

(2) one member of the senate appointed by the lieutenant governor;

(3) one member of the house of representatives appointed by the speaker of the house of representatives;

(4) the director of [~~one member who is an employee of~~] the Elections Division of the Office of the Secretary of State; [~~and~~]

(5) one member who is an employee of the department; and

(6) additional members appointed by the chief [~~state cybersecurity coordinator~~], including representatives of institutions of higher education and private sector leaders.

(c) 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) In appointing representatives from institutions of higher education to the cybersecurity council, the chief [~~state cybersecurity coordinator~~] shall consider appointing members of the Information Technology Council for Higher Education.

(e) [~~(d)~~] The cybersecurity council shall:

(1) consider the costs and benefits of establishing a computer emergency readiness team to address cybersecurity incidents [~~cyber attacks~~] occurring in this state during routine and emergency situations;

(2) establish criteria and priorities for addressing cybersecurity threats to critical state installations;

(3) consolidate and synthesize best practices to assist state agencies in understanding and implementing cybersecurity measures that are most beneficial to this state; and

(4) assess the knowledge, skills, and capabilities of the existing information technology and cybersecurity workforce to mitigate and respond to cyber threats and develop recommendations for addressing immediate workforce deficiencies and ensuring a long-term pool of qualified applicants.

(f) [~~(e)~~] The chief, in collaboration with the cybersecurity council, shall provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state.

SECTION 15. Section 2054.514, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.407, Government Code, and amended to read as follows:

Sec. 2063.407 [~~2054.514~~]. RECOMMENDATIONS. The chief [~~state cybersecurity coordinator~~] may implement any portion, or all of the recommendations made by the cybersecurity council under Section 2063.406 [~~Cybersecurity, Education, and Economic~~

~~Development Council under Subchapter N~~].

SECTION 16. Subchapter N-2, Chapter 2054, Government Code, is transferred to Chapter 2063, Government Code, as added by this Act, redesignated as Subchapter F, Chapter 2063, Government Code, and amended to read as follows:

SUBCHAPTER F [~~N-2~~]. TEXAS VOLUNTEER INCIDENT RESPONSE TEAM

Sec. 2063.501 [~~2054.52001~~]. DEFINITIONS. In this subchapter:

(1) "Incident response team" means the Texas volunteer incident response team established under Section 2063.502 [~~2054.52002~~].

(2) "Participating entity" means a state agency, including an institution of higher education, or a local government that receives assistance under this subchapter during a cybersecurity incident [~~event~~].

(3) "Volunteer" means an individual who provides rapid response assistance during a cybersecurity incident [~~event~~] under this subchapter.

Sec. 2063.502 [~~2054.52002~~]. ESTABLISHMENT OF TEXAS VOLUNTEER INCIDENT RESPONSE TEAM. (a) The command [~~department~~] shall establish the Texas volunteer incident response team to provide rapid response assistance to a participating entity under the command's [~~department's~~] direction during a cybersecurity incident [~~event~~].

(b) The command [~~department~~] shall prescribe eligibility criteria for participation as a volunteer member of the incident response team, including a requirement that each volunteer have

expertise in addressing cybersecurity incidents [~~events~~].

Sec. 2063.503 [~~2054.52003~~]. CONTRACT WITH VOLUNTEERS. The command [~~department~~] shall enter into a contract with each volunteer the command [~~department~~] approves to provide rapid response assistance under this subchapter. The contract must require the volunteer to:

(1) acknowledge the confidentiality of information required by Section 2063.510 [~~2054.52010~~];

(2) protect all confidential information from disclosure;

(3) avoid conflicts of interest that might arise in a deployment under this subchapter;

(4) comply with command [~~department~~] security policies and procedures regarding information resources technologies;

(5) consent to background screening required by the command [~~department~~]; and

(6) attest to the volunteer's satisfaction of any eligibility criteria established by the command [~~department~~].

Sec. 2063.504 [~~2054.52004~~]. VOLUNTEER QUALIFICATION. (a) The command [~~department~~] shall require criminal history record information for each individual who accepts an invitation to become a volunteer.

(b) The command [~~department~~] may request other information relevant to the individual's qualification and fitness to serve as a volunteer.

(c) The command [~~department~~] has sole discretion to

determine whether an individual is qualified to serve as a volunteer.

Sec. 2063.505 [~~2054.52005~~]. DEPLOYMENT. (a) In response to a cybersecurity incident [~~event~~] that affects multiple participating entities or a declaration by the governor of a state of disaster caused by a cybersecurity event, the command [~~department~~] on request of a participating entity may deploy volunteers and provide rapid response assistance under the command's [~~department's~~] direction and the managed security services framework established under Section 2063.204(c) [~~2054.0594(d)~~] to assist with the incident [~~event~~].

(b) A volunteer may only accept a deployment under this subchapter in writing. A volunteer may decline to accept a deployment for any reason.

Sec. 2063.506 [~~2054.52006~~]. CYBERSECURITY COUNCIL DUTIES. The cybersecurity council established under Section 2063.406 [~~2054.512~~] shall review and make recommendations to the command [~~department~~] regarding the policies and procedures used by the command [~~department~~] to implement this subchapter. The command [~~department~~] may consult with the council to implement and administer this subchapter.

Sec. 2063.507 [~~2054.52007~~]. COMMAND [~~DEPARTMENT~~] POWERS AND DUTIES. (a) The command [~~department~~] shall:

(1) approve the incident response tools the incident response team may use in responding to a cybersecurity incident [~~event~~];

(2) establish the eligibility criteria an individual

must meet to become a volunteer;

(3) develop and publish guidelines for operation of the incident response team, including the:

(A) standards and procedures the command [~~department~~] uses to determine whether an individual is eligible to serve as a volunteer;

(B) process for an individual to apply for and accept incident response team membership;

(C) requirements for a participating entity to receive assistance from the incident response team; and

(D) process for a participating entity to request and obtain the assistance of the incident response team; and

(4) adopt policies [~~rules~~] necessary to implement this subchapter.

(b) The command [~~department~~] may require a participating entity to enter into a contract as a condition for obtaining assistance from the incident response team. [~~The contract must comply with the requirements of Chapters 771 and 791.~~]

(c) The command [~~department~~] may provide appropriate training to prospective and approved volunteers.

(d) In accordance with state law, the command [~~department~~] may provide compensation for actual and necessary travel and living expenses incurred by a volunteer on a deployment using money available for that purpose.

(e) The command [~~department~~] may establish a fee schedule for participating entities receiving incident response team assistance. The amount of fees collected may not exceed the

command's [~~department's~~] costs to operate the incident response team.

Sec. 2063.508 [~~2054.52008~~]. STATUS OF VOLUNTEER; LIABILITY. (a) A volunteer is not an agent, employee, or independent contractor of this state for any purpose and has no authority to obligate this state to a third party.

(b) This state is not liable to a volunteer for personal injury or property damage sustained by the volunteer that arises from participation in the incident response team.

Sec. 2063.509 [~~2054.52009~~]. CIVIL LIABILITY. A volunteer who in good faith provides professional services in response to a cybersecurity incident [~~event~~] is not liable for civil damages as a result of the volunteer's acts or omissions in providing the services, except for wilful and wanton misconduct. This immunity is limited to services provided during the time of deployment for a cybersecurity incident [~~event~~].

Sec. 2063.510 [~~2054.52010~~]. CONFIDENTIAL INFORMATION. Information written, produced, collected, assembled, or maintained by the command [~~department~~], a participating entity, the cybersecurity council, or a volunteer in the implementation of this subchapter is confidential and not subject to disclosure under Chapter 552 if the information:

(1) contains the contact information for a volunteer;

(2) identifies or provides a means of identifying a person who may, as a result of disclosure of the information, become a victim of a cybersecurity incident [~~event~~];

(3) consists of a participating entity's cybersecurity

plans or cybersecurity-related practices; or

(4) is obtained from a participating entity or from a participating entity's computer system in the course of providing assistance under this subchapter.

SECTION 17. Subchapter E, Chapter 2059, Government Code, is transferred to Chapter 2063, Government Code, as added by this Act, redesignated as Subchapter G, Chapter 2063, Government Code, and amended to read as follows:

SUBCHAPTER G [~~E~~]. REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTERS

Sec. 2063.601 [~~2059.201~~]. ELIGIBLE PARTICIPATING ENTITIES. A state agency or an entity listed in Section 2059.058 is eligible to participate in cybersecurity support and network security provided by a regional [~~network~~] security operations center under this subchapter.

Sec. 2063.602 [~~2059.202~~]. ESTABLISHMENT OF REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTERS. (a) Subject to Subsection (b), the command [~~department~~] may establish regional [~~network~~] security operations centers, under the command's [~~department's~~] managed security services framework established by Section 2063.204(c) [~~2054.0594(d)~~], to assist in providing cybersecurity support and network security to regional offices or locations for state agencies and other eligible entities that elect to participate in and receive services through the center.

(b) The command [~~department~~] may establish more than one regional [~~network~~] security operations center only if the command [~~department~~] determines the first center established by the command [~~department~~] successfully provides to state agencies and other

eligible entities the services the center has contracted to provide.

(c) The command [~~department~~] shall enter into an interagency contract in accordance with Chapter 771 or an interlocal contract in accordance with Chapter 791, as appropriate, with an eligible participating entity that elects to participate in and receive services through a regional [~~network~~] security operations center.

Sec. 2063.603 [~~2059.203~~]. REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTER LOCATIONS AND PHYSICAL SECURITY. (a) In creating and operating a regional [~~network~~] security operations center, the command may [~~department shall~~] partner with another [~~a~~] university system or institution of higher education as defined by Section 61.003, Education Code, other than a public junior college. The system or institution shall:

(1) serve as an education partner with the command [~~department~~] for the regional [~~network~~] security operations center; and

(2) enter into an interagency contract with the command [~~department~~] in accordance with Chapter 771.

(b) In selecting the location for a regional [~~network~~] security operations center, the command [~~department~~] shall select a university system or institution of higher education that has supportive educational capabilities.

(c) A university system or institution of higher education selected to serve as a regional [~~network~~] security operations center shall control and monitor all entrances to and critical

areas of the center to prevent unauthorized entry. The system or institution shall restrict access to the center to only authorized individuals.

(d) A local law enforcement entity or any entity providing security for a regional [~~network~~] security operations center shall monitor security alarms at the regional [~~network~~] security operations center subject to the availability of that service.

(e) The command [~~department~~] and a university system or institution of higher education selected to serve as a regional [~~network~~] security operations center shall restrict operational information to only center personnel, except as provided by Chapter 321.

Sec. 2063.604 [~~2059.204~~]. REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTERS SERVICES AND SUPPORT. The command [~~department~~] may offer the following managed security services through a regional [~~network~~] security operations center:

(1) real-time cybersecurity [~~network security~~] monitoring to detect and respond to cybersecurity incidents [~~network security events~~] that may jeopardize this state and the residents of this state;

(2) alerts and guidance for defeating cybersecurity [~~network security~~] threats, including firewall configuration, installation, management, and monitoring, intelligence gathering, and protocol analysis;

(3) immediate response to counter unauthorized [~~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;

(4) development, coordination, and execution of statewide cybersecurity operations to isolate, contain, and mitigate the impact of cybersecurity [~~network security~~] incidents for participating entities; and

(5) cybersecurity educational services.

Sec. 2063.605 [~~2059.205~~]. NETWORK SECURITY GUIDELINES AND STANDARD OPERATING PROCEDURES. (a) The command [~~department~~] shall adopt and provide to each regional [~~network~~] security operations center appropriate network security guidelines and standard operating procedures to ensure efficient operation of the center with a maximum return on the state's investment.

(b) The command [~~department~~] shall revise the standard operating procedures as necessary to confirm network security.

(c) Each eligible participating entity that elects to participate in a regional [~~network~~] security operations center shall comply with the network security guidelines and standard operating procedures.

SECTION 18. Section 325.011, Government Code, is amended to read as follows:

Sec. 325.011. CRITERIA FOR REVIEW. The commission and its staff shall consider the following 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:

(1) the efficiency and effectiveness with which the

agency or the advisory committee operates;

(2)(A) an identification of the mission, goals, and objectives intended for the agency or advisory committee and of the problem or need that the agency or advisory committee was intended to address; and

(B) the extent to which the mission, goals, and objectives have been achieved and the problem or need has been addressed;

(3)(A) an identification of any activities of the agency in addition to those granted by statute and of the authority for those activities; and

(B) the extent to which those activities are needed;

(4) an assessment of authority of the agency relating to fees, inspections, enforcement, and penalties;

(5) whether less restrictive or alternative methods of performing any function that the agency performs could adequately protect or provide service to the public;

(6) the extent to which the jurisdiction of the agency and the programs administered by the agency overlap or duplicate those of other agencies, the extent to which the agency coordinates with those agencies, and the extent to which the programs administered by the agency can be consolidated with the programs of other state agencies;

(7) the promptness and effectiveness with which the agency addresses complaints concerning entities or other persons affected by the agency, including an assessment of the agency's

administrative hearings process;

(8) an assessment of the agency's rulemaking process and the extent to which the agency has encouraged participation by the public in making its rules and decisions and the extent to which the public participation has resulted in rules that benefit the public;

(9) the extent to which the agency has complied with:

(A) federal and state laws and applicable rules regarding equality of employment opportunity and the rights and privacy of individuals; and

(B) state law and applicable rules of any state agency regarding purchasing guidelines and programs for historically underutilized businesses;

(10) the extent to which the agency issues and enforces rules relating to potential conflicts of interest of its employees;

(11) the extent to which the agency complies with Chapters 551 and 552 and follows records management practices that enable the agency to respond efficiently to requests for public information;

(12) the effect of federal intervention or loss of federal funds if the agency is abolished;

(13) the extent to which the purpose and effectiveness of reporting requirements imposed on the agency justifies the continuation of the requirement; and

(14) an assessment of the agency's cybersecurity practices using confidential information available from the

Department of Information Resources, the Texas Cyber Command, or any other appropriate state agency.

SECTION 19. Section 11.175(h-1), Education Code, is amended to read as follows:

(h-1) Notwithstanding Section 2063.103 [~~2054.5191~~], Government Code, only the district's cybersecurity coordinator is required to complete the cybersecurity training under that section on an annual basis. Any other school district employee required to complete the cybersecurity training shall complete the training as determined by the district, in consultation with the district's cybersecurity coordinator.

SECTION 20. Section 38.307(e), Education Code, is amended to read as follows:

(e) The agency shall maintain the data collected by the task force and the work product of the task force in accordance with:

(1) the agency's information security plan under Section 2063.403 [~~2054.133~~], Government Code; and

(2) the agency's records retention schedule under Section 441.185, Government Code.

SECTION 21. Section 61.003(6), Education Code, is amended to read as follows:

(6) "Other agency of higher education" means The University of Texas System, System Administration; The University of Texas at El Paso Museum; Texas Epidemic Public Health Institute at The University of Texas Health Science Center at Houston; the Texas Cyber Command; The Texas A&M University System, Administrative and General Offices; Texas A&M AgriLife Research;

Texas A&M AgriLife Extension Service; Rodent and Predatory Animal Control Service (a part of the Texas A&M AgriLife Extension Service); Texas A&M Engineering Experiment Station (including the Texas A&M Transportation Institute); Texas A&M Engineering Extension Service; Texas A&M Forest Service; Texas Division of Emergency Management; Texas Tech University Museum; Texas State University System, System Administration; Sam Houston Memorial Museum; Panhandle-Plains Historical Museum; Cotton Research Committee of Texas; Texas Water Resources Institute; Texas A&M Veterinary Medical Diagnostic Laboratory; and any other unit, division, institution, or agency which shall be so designated by statute or which may be established to operate as a component part of any public senior college or university, or which may be so classified as provided in this chapter.

SECTION 22. Section 65.02(a), Education Code, is amended to read as follows:

(a) The University of Texas System is composed of the following institutions and entities:

(1) The University of Texas at Arlington;

(2) The University of Texas at Austin;

(3) The University of Texas at Dallas;

(4) The University of Texas at El Paso;

(5) The University of Texas Permian Basin;

(6) The University of Texas at San Antonio;

(7) The University of Texas Southwestern Medical Center;

(8) The University of Texas Medical Branch at

Galveston;

(9) The University of Texas Health Science Center at Houston;

(10) The University of Texas Health Science Center at San Antonio;

(11) The University of Texas M. D. Anderson Cancer Center;

(12) Stephen F. Austin State University, a member of The University of Texas System;

(13) The University of Texas at Tyler; [~~and~~]

(14) The University of Texas Rio Grande Valley; and

(15) the Texas Cyber Command (Chapter 2063, Government Code).

SECTION 23. Sections 772.012(b) and (c), Government Code, are amended to read as follows:

(b) To apply for a grant under this chapter, a local government must submit with the grant application a written certification of the local government's compliance with the cybersecurity training required by Section 2063.103 [~~2054.5191~~].

(c) On a determination by the criminal justice division established under Section 772.006 that a local government awarded a grant under this chapter has not complied with the cybersecurity training required by Section 2063.103 [~~2054.5191~~], the local government shall pay to this state an amount equal to the amount of the grant award. A local government that is the subject of a determination described by this subsection is ineligible for another grant under this chapter until the second anniversary of

the date the local government is determined ineligible.

SECTION 24. Section 2054.0701(c), Government Code, is amended to read as follows:

(c) A program offered under this section must:

(1) be approved by the Texas Higher Education Coordinating Board in accordance with Section 61.0512, Education Code;

(2) develop the knowledge and skills necessary for an entry-level information technology position in a state agency; and

(3) include a one-year apprenticeship with:

(A) the department;

(B) another relevant state agency;

(C) an organization working on a major information resources project; or

(D) a regional [~~network~~] security operations center established under Section 2063.602 [~~2059.202~~].

SECTION 25. Section 2056.002(b), Government Code, is amended to read as follows:

(b) The Legislative Budget Board and the governor's office shall determine the elements required to be included in each agency's strategic plan. Unless modified by the Legislative Budget Board and the governor's office, and except as provided by Subsection (c), a plan must include:

(1) a statement of the mission and goals of the state agency;

(2) a description of the indicators developed under this chapter and used to measure the output and outcome of the

agency;

(3) identification of the groups of people served by the agency, including those having service priorities, or other service measures established by law, and estimates of changes in those groups expected during the term of the plan;

(4) an analysis of the use of the agency's resources to meet the agency's needs, including future needs, and an estimate of additional resources that may be necessary to meet future needs;

(5) an analysis of expected changes in the services provided by the agency because of changes in state or federal law;

(6) a description of the means and strategies for meeting the agency's needs, including future needs, and achieving the goals established under Section 2056.006 for each area of state government for which the agency provides services;

(7) a description of the capital improvement needs of the agency during the term of the plan and a statement, if appropriate, of the priority of those needs;

(8) identification of each geographic region of this state, including the Texas-Louisiana border region and the Texas-Mexico border region, served by the agency, and if appropriate the agency's means and strategies for serving each region;

(9) a description of the training of the agency's contract managers under Section 656.052;

(10) an analysis of the agency's expected expenditures that relate to federally owned or operated military installations or facilities, or communities where a federally owned or operated

military installation or facility is located;

(11) an analysis of the strategic use of information resources as provided by the instructions prepared under Section 2054.095;

(12) a written certification of the agency's compliance with the cybersecurity training required under Sections 2063.103 [~~2054.5191~~] and 2063.104 [~~2054.5192~~]; and

(13) other information that may be required.

SECTION 26. Section 2054.5181, Government Code, is repealed.

SECTION 27. (a) In this section, "department" means the Department of Information Resources.

(b) On the effective date of this Act, the Texas Cyber 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) As soon as practicable on or after the effective date of this Act, the governor shall appoint the chief of the Texas Cyber Command, as described by Section 2063.0025, Government Code, as added by this Act.

(c) Notwithstanding Subsection (b) of this section, the department shall continue to perform duties and exercise powers under Chapter 2054, 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) Not later than December 31, 2026:

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

(2) all employees of the department 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 Texas Cyber 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 the department that relates to cybersecurity under Chapter 2063, Government Code, as added by this Act, is a rule or form of the Texas Cyber Command and remains in effect until changed by the command;

(4) a reference in law to the department that relates to cybersecurity under Chapter 2063, Government Code, as added by this Act, means the Texas Cyber 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 the department that is related to cybersecurity under Chapter 2063, Government Code, as added by this Act, is transferred without change in status to the Texas Cyber Command, and the Texas Cyber Command assumes, without a change in status, the position of the department in a negotiation or proceeding relating to cybersecurity to which the department is a

party;

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

(7) contracts specified as necessary to accomplish the goals and duties of the Texas Cyber 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 Texas Cyber Command;

(8) all property, including records, in the custody of the department related to cybersecurity under Chapter 2063, Government Code, as added by this Act, becomes property of the Texas Cyber 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 the department 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 Texas Cyber Command.

(e) Not later than January 1, 2026, the department, in collaboration with the chief of the Texas Cyber Command, and the board of regents of The University of Texas System shall enter into a memorandum of understanding relating to the transfer of powers and duties from the department to the Texas Cyber Command as provided by this Act. The memorandum must 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. This Act takes effect September 1, 2025.

ADOPTED

MAY 28 2023

Secretary of the Senate

By: Tan Parker H.B. No. 150

Substitute the following for H.B. No. 150:

By: Phil King C.S.H.B. No. 150

A BILL TO BE ENTITLED

AN ACT

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.

BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

SECTION 1. Subtitle B, Title 10, Government Code, is amended by adding Chapter 2063 to read as follows:

CHAPTER 2063. TEXAS CYBER COMMAND

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 2063.001. DEFINITIONS. In this chapter:

(1) "Chief" means the chief of the Texas Cyber Command.

(2) "Command" means the Texas Cyber Command established under this chapter.

(3) "Covered entity" means a private entity operating critical infrastructure or a local government that the command contracts with in order to provide cybersecurity services under this chapter.

(4) "Critical infrastructure" means infrastructure in this state vital to the security, governance, public health and safety, economy, or morale of the state or the nation, including:

(A) chemical facilities;

(B) commercial facilities;

(C) communication facilities;

(D) manufacturing facilities;

(E) dams;

(F) defense industrial bases;

(G) emergency services systems;

(H) energy facilities;

(I) financial services systems;

(J) food and agriculture facilities;

(K) government facilities;

(L) health care and public health facilities;

(M) information technology and information technology systems;

(N) nuclear reactors, materials, and waste;

(O) transportation systems; or

(P) water and wastewater systems.

(5) "Cybersecurity" means the measures taken for a computer, computer network, computer system, or other technology infrastructure to protect against, respond to, and recover from unauthorized:

(A) use, access, disruption, modification, or destruction; or

(B) disclosure, modification, or destruction of information.

(6) "Cybersecurity incident" includes:

(A) a breach or suspected breach of system security as defined by Section 521.053, Business & Commerce Code;

(B) the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or

computer system; or

(C) any other cybersecurity-related occurrence that jeopardizes information or an information system designated by command policy adopted under this chapter.

(7) "Department" means the Department of Information Resources.

(8) "Governmental entity" means a state agency or a local government.

(9) "Information resources" has the meaning assigned by Section 2054.003.

(10) "Information resources technologies" has the meaning assigned by Section 2054.003.

(11) "Local government" has the meaning assigned by Section 2054.003.

(12) "Sensitive personal information" has the meaning assigned by Section 521.002, Business & Commerce Code.

(13) "State agency" means:

(A) a department, commission, board, office, or other agency that is in the executive branch of state government and that was created by the constitution or a statute;

(B) the supreme court, the court of criminal appeals, a court of appeals, a district court, or the Texas Judicial Council or another agency in the judicial branch of state government; or

(C) a university system or an institution of higher education as defined by Section 61.003, Education Code.

Sec. 2063.002. ORGANIZATION. (a) The Texas Cyber Command

is a state agency.

(b) The command is governed by a chief appointed by the governor and confirmed with the advice and consent of the senate. The chief serves for a two-year term expiring February 1 of each odd-numbered year and must possess professional training and knowledge relevant to the functions and duties of the command.

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

(d) The command may enter into an interagency agreement with another state agency for the purpose of providing:

(1) administrative support services to the command as necessary to carry out the purposes of this chapter and Chapter 2059; and

(2) a facility to the command located in San Antonio that has a sensitive compartmented information facility for use in carrying out the purposes of this chapter and Chapter 2059.

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

(b) The command is responsible for cybersecurity for this state, including:

(1) providing leadership, guidance, and tools to enhance cybersecurity defenses;

(2) facilitating education and training of a cybersecurity workforce;

(3) monitoring and coordinating cyber threat intelligence and information systems to detect and warn entities of cyber attacks, identifying cyber threats to critical infrastructure and state systems, planning and executing cybersecurity incident responses, and conducting digital forensics of cybersecurity incidents to support law enforcement and attribute the incidents;

(4) creating partnerships needed to effectively carry out the command's functions; and

(5) receiving all cybersecurity incident reports from state agencies and covered entities.

Sec. 2063.004. GENERAL POWERS AND DUTIES. (a) The command shall:

(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 to ensure information resources and information resources technologies obtained by the department 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) The command may:

(1) adopt and use an official seal;

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

(3) acquire and convey property or an interest in

property;

(4) 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;

(5) 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

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

(c) Except as otherwise provided by this chapter, the command shall 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. The command may 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 IN RESPONSE TO CYBERSECURITY INCIDENT. (a) 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, 2155.083, and 2155.132(c) in making the purchase.

(b) The command shall, as soon as practicable after an emergency purchase is made under this section:

(1) provide written notice to the Legislative Budget

Board and the governor describing the nature of the emergency, the purchase made, and the vendor selected;

(2) ensure that documentation of the purchase, including the justification for bypassing standard procedures and the terms of the contract, is maintained and made available for post-incident audit; and

(3) submit a report to the State Auditor's Office not later than the 90th day after the date of the purchase describing:

(A) the necessity for making the purchase;

(B) the cost and duration of the contract; and

(C) any competitive processes used, if applicable.

Sec. 2063.008. PURCHASING OF CYBERSECURITY RESOURCES BY GOVERNMENTAL ENTITIES. (a) The command may not require, including by rule, governmental entities to purchase specific cybersecurity systems or resources.

(b) The command may adopt guidelines designating the purchasing method that attains the best value for the state for cybersecurity systems and resources.

Sec. 2063.009. RULES. The chief, with advice from the department, may adopt rules necessary for carrying out the purposes of this chapter.

Sec. 2063.010. APPLICATION OF SUNSET ACT. The command is subject to Chapter 325 (Texas Sunset Act). Unless continued in existence as provided by that chapter, the command is abolished September 1, 2031.

Sec. 2063.011. LAWS NOT AFFECTED. (a) Except as

specifically provided by this chapter, this chapter does not affect laws, rules, or decisions relating to the confidentiality or privileged status of categories of information or communications.

(b) This chapter does not enlarge the right of state government to require information, records, or communications from the people.

SUBCHAPTER B. MINIMUM STANDARDS AND TRAINING

Sec. 2063.101. BEST PRACTICES AND MINIMUM STANDARDS FOR CYBERSECURITY AND TRAINING. (a) The command shall 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) The command shall establish and periodically assess mandatory cybersecurity training that must be completed by all information resources employees of state agencies. The command shall consult with the Information Technology Council for Higher Education established under Section 2054.121 regarding applying the training requirements to employees of institutions of higher education.

(c) Except as otherwise provided by this subsection, the command shall adopt policies to ensure governmental entities are complying with the requirements of this section. The command shall adopt policies that ensure that a person who is not a citizen of the United States may not be 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) In this section, "center" means the cybersecurity threat intelligence center established under this section.

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

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

(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) The chief shall employ a director for the center.

Sec. 2063.202. CYBERSECURITY INCIDENT RESPONSE UNIT. (a) The command shall 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) The chief shall employ a director for the cybersecurity

incident response unit.

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

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

(A) preserve evidence of a cybersecurity incident, including logs and communication;

(B) document chains of custody; and

(C) timely notify and maintain contact with the appropriate law enforcement agencies investigating a cybersecurity incident;

(2) develop and share with relevant state agencies and covered entities, subject to a contractual agreement, 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;

(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 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) The chief shall employ a director for the digital forensics laboratory.

Sec. 2063.205. POLICIES. The command shall 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. Information received from state agencies by the department under Section 2054.069 shall be transmitted by the department to the command on an ongoing basis.

Sec. 2063.409. INFORMATION SECURITY ASSESSMENT AND PENETRATION TEST REQUIRED. (a) This section does not apply to a university system or institution of higher education as defined by Section 61.003, Education Code.

(b) At least once every two years, the command shall require each state agency to complete an information security assessment and a penetration test to be performed by the command or, at the command's discretion, a vendor selected by the command.

(c) The chief shall adopt rules as necessary to implement this section, including rules for the procurement of a vendor under Subsection (b).

SECTION 2. Section 2054.510, Government Code, is transferred to Subchapter A, Chapter 2063, Government Code, as

added by this Act, redesignated as Section 2063.0025, Government Code, and amended to read as follows:

Sec. 2063.0025 [~~2054.510~~]. COMMAND CHIEF [~~INFORMATION SECURITY OFFICER~~]. (a) In this section, "state cybersecurity [~~information security~~] program" means the policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish the cybersecurity [~~information resources security~~] function for this state.

(b) 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. [~~The executive director, using existing funds, shall employ a chief information security officer.~~]

(c) The chief [~~information security officer~~] shall oversee cybersecurity matters for this state including:

(1) implementing the duties described by Section 2063.004 [~~2054.059~~];

(2) [~~responding to reports received under Section 2054.1125,~~

[~~(3)~~] developing a statewide cybersecurity [~~information security~~] framework;

(3) [~~(4)~~] overseeing the development of cybersecurity [~~statewide information security~~] policies and standards;

(4) [~~(5)~~] collaborating with [~~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) [~~(6)~~] overseeing the implementation of the policies, standards, and requirements [~~guidelines~~] developed under this chapter [~~Subdivisions (3) and (4)~~];

(6) [~~(7)~~] providing cybersecurity [~~information security~~] leadership, strategic direction, and coordination for the state cybersecurity [~~information security~~] program;

(7) [~~(8)~~] providing strategic direction to:

(A) the network security center established under Section 2059.101; and

(B) regional security operations [~~statewide technology~~] centers operated under Subchapter G [~~L~~]; and

(8) [~~(9)~~] overseeing the preparation and submission of the report described by Section 2063.301 [~~2054.0591~~].

SECTION 3. Section 2054.0592, Government Code, is transferred to Subchapter A, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.006, Government Code, and amended to read as follows:

Sec. 2063.006 [~~2054.0592~~]. CYBERSECURITY EMERGENCY FUNDING. If a cybersecurity incident [~~event~~] creates a need for emergency funding, the command [~~department~~] may request that the governor or Legislative Budget Board make a proposal under Chapter 317 to provide funding to manage the operational and financial impacts from the cybersecurity incident [~~event~~].

SECTION 4. Section 2054.519, Government Code, is

transferred to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.102, Government Code, and amended to read as follows:

Sec. 2063.102 [~~2054.519~~]. STATE CERTIFIED CYBERSECURITY TRAINING PROGRAMS. (a) The command [~~department~~], in consultation with the cybersecurity council established under Section 2063.406 [~~2054.512~~] and industry stakeholders, shall annually:

(1) certify at least five cybersecurity training programs for state and local government employees; and

(2) update standards for maintenance of certification by the cybersecurity training programs under this section.

(b) To be certified under Subsection (a), a cybersecurity training program must:

(1) focus on forming appropriate cybersecurity [~~information security~~] habits and procedures that protect information resources; and

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

(c) The command [~~department~~] may identify and certify under Subsection (a) training programs provided by state agencies and local governments that satisfy the training requirements described by Subsection (b).

(d) The command [~~department~~] may contract with an independent third party to certify cybersecurity training programs under this section.

(e) The command [~~department~~] shall annually publish on the

command's [~~department's~~] Internet website the list of cybersecurity training programs certified under this section.

SECTION 5. Section 2054.5191, Government Code, is transferred to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.103, Government Code, and amended to read as follows:

Sec. 2063.103 [~~2054.5191~~]. CYBERSECURITY TRAINING REQUIRED [~~: CERTAIN EMPLOYEES AND OFFICIALS~~]. (a) Each elected or appointed official and employee of a governmental entity who has access to the entity's information resources or information resources technologies [~~state agency shall identify state employees who use a computer to complete at least 25 percent of the employee's required duties. At least once each year, an employee identified by the state agency and each elected or appointed officer of the agency~~] shall annually complete a cybersecurity training program certified under Section 2063.102 [~~2054.519~~].

(b) [~~(a-1) At least once each year, a local government shall:~~

[~~(1) 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; and~~

[~~(2) require the employees and officials identified under Subdivision (1) to complete a cybersecurity training program certified under Section 2054.519.~~

[~~(a-2)~~] The governing body of a governmental entity [~~local government~~] or the governing body's designee may deny access to the

governmental entity's information resources or information resources technologies [~~local government's computer system or database~~] to an employee or official [~~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) [~~(a-1)(2)~~].

(c) [~~(b)~~] The governing body of a local government may select the most appropriate cybersecurity training program certified under Section 2063.102 [~~2054.519~~] for employees and officials of the local government to complete. The governing body shall:

(1) verify and report on the completion of a cybersecurity training program by employees and officials of the local government to the command [~~department~~]; and

(2) require periodic audits to ensure compliance with this section.

(d) [~~(c)~~] A state agency may select the most appropriate cybersecurity training program certified under Section 2063.102 [~~2054.519~~] for employees and officials of the state agency. The executive head of each state agency shall verify completion of a cybersecurity training program by employees and officials of the state agency in a manner specified by the command [~~department~~].

(e) [~~(d)~~] The executive head of each state agency shall periodically require an internal review of the agency to ensure compliance with this section.

(f) [~~(e)~~] The command [~~department~~] shall develop a form for use by governmental entities [~~state agencies and local governments~~]

in verifying completion of cybersecurity training program requirements under this section. The form must allow the state agency and local government to indicate the percentage of employee and official completion.

(g) [~~(f)~~] The requirements of Subsection [~~Subsections~~] (a) [~~and (a-1)~~] do not apply to employees and officials who have been:

(1) granted military leave;

(2) granted leave under the federal Family and Medical Leave Act of 1993 (29 U.S.C. Section 2601 et seq.);

(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 [~~state agency's or local government's database and systems~~];

(4) granted any other type of extended leave or authorization to work from an alternative work site if that employee or official no longer has access to the governmental entity's information resources or information resources technologies [~~state agency's or local government's database and systems~~]; or

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

SECTION 6. Section 2054.5192, Government Code, is

transferred to Subchapter B, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.104, Government Code, and amended to read as follows:

Sec. 2063.104 [~~2054.5192~~]. CYBERSECURITY TRAINING REQUIRED: CERTAIN STATE CONTRACTORS. (a) In this section, "contractor" includes a subcontractor, officer, or employee of the contractor.

(b) A state agency shall require any contractor who has access to a state computer system or database to complete a cybersecurity training program certified under Section 2063.102 [~~2054.519~~] as selected by the agency.

(c) The cybersecurity training program must be completed by a contractor during the term of the contract and during any renewal period.

(d) Required completion of a cybersecurity training program must be included in the terms of a contract awarded by a state agency to a contractor.

(e) A contractor required to complete a cybersecurity training program under this section shall verify completion of the program to the contracting state agency. The person who oversees contract management for the agency shall:

(1) not later than August 31 of each year, report the contractor's completion to the command [~~department~~]; and

(2) periodically review agency contracts to ensure compliance with this section.

SECTION 7. Section 2054.0594, Government Code, is transferred to Subchapter C, Chapter 2063, Government Code, as

added by this Act, redesignated as Section 2063.204, Government Code, and amended to read as follows:

Sec. 2063.204 [~~2054.0594~~]. INFORMATION SHARING AND ANALYSIS ORGANIZATION. (a) The command [~~department~~] shall establish at least one [~~an~~] information sharing and analysis organization to provide a forum for state agencies, local governments, public and private institutions of higher education, and the private sector to share information regarding cybersecurity threats, best practices, and remediation strategies.

(b) [~~The department shall provide administrative support to the information sharing and analysis organization.~~

[~~(c)~~] A participant in the information sharing and analysis organization shall assert any exception available under state or federal law, including Section 552.139, in response to a request for public disclosure of information shared through the organization. Section 552.007 does not apply to information described by this subsection.

(c) [~~(d)~~] The command [~~department~~] shall establish a framework for regional cybersecurity task forces [~~working groups~~] to execute mutual aid agreements that allow state agencies, local governments, regional planning commissions, public and private institutions of higher education, the private sector, the regional security operations centers under Subchapter G, and the cybersecurity incident response unit under Section 2063.202 [~~and the incident response team established under Subchapter N-2~~] to assist with responding to a cybersecurity incident [~~event~~] in this state. A task force [~~working group~~] may be established within the

geographic area of a regional planning commission established under Chapter 391, Local Government Code. The task force [~~working group~~] may establish a list of available cybersecurity experts and share resources to assist in responding to the cybersecurity incident [~~event~~] and recovery from the incident [~~event~~].

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

SUBCHAPTER D. REPORTING

SECTION 9. Sections 2054.0591, 2054.603, and 2054.077, Government Code, are transferred to Subchapter D, Chapter 2063, Government Code, as added by this Act, redesignated as Sections 2063.301, 2063.302, and 2063.303, Government Code, respectively, and amended to read as follows:

Sec. 2063.301 [~~2054.0591~~]. CYBERSECURITY REPORT. (a) Not later than November 15 of each even-numbered year, the command [~~department~~] shall submit to the governor, the lieutenant governor, the speaker of the house of representatives, and the standing committee of each house of the legislature with primary jurisdiction over state government operations a report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in this state. The report must include:

(1) an assessment of the resources available to address the operational and financial impacts of a cybersecurity incident [~~event~~];

(2) a review of existing statutes regarding cybersecurity and information resources technologies; and

(3) recommendations for legislative action to increase the state's cybersecurity and protect against adverse impacts from a cybersecurity incident [~~event; and~~

[~~(4) 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~~].

(b) Not later than October 1 of each even-numbered year, the command shall submit a report to the Legislative Budget Board that prioritizes, for the purpose of receiving funding, state agency cybersecurity projects. Each state agency shall coordinate with the command to implement this subsection.

(c) [~~(b)~~] The command [~~department~~] or a recipient of a report under this section may redact or withhold information confidential under Chapter 552, including Section 552.139, or other state or federal law that is contained in the report in response to a request under Chapter 552 without the necessity of requesting a decision from the attorney general under Subchapter G, Chapter 552. The disclosure of information under this section is not a voluntary disclosure for purposes of Section 552.007.

Sec. 2063.302 [~~2054.603~~]. CYBERSECURITY [~~SECURITY~~] INCIDENT NOTIFICATION BY STATE AGENCY OR LOCAL GOVERNMENT. (a) [~~In this section:~~

[~~(1) "Security incident" means:~~

[~~(A) a breach or suspected breach of system security as defined by Section 521.053, Business & Commerce Code; and~~

[~~(B) the introduction of ransomware, as defined by Section 33.023, Penal Code, into a computer, computer network, or computer system.~~

[~~(2) "Sensitive personal information" has the meaning assigned by Section 521.002, Business & Commerce Code.~~

[~~(b)~~] A state agency or local government that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a cybersecurity [~~security~~] incident:

(1) comply with the notification requirements of Section 521.053, Business & Commerce Code, to the same extent as a person who conducts business in this state;

(2) not later than 48 hours after the discovery of the cybersecurity [~~security~~] incident, notify:

(A) the command [~~department~~], including the chief [~~information security officer~~]; or

(B) if the cybersecurity [~~security~~] incident involves election data, the secretary of state; and

(3) comply with all command [~~department~~] rules relating to reporting cybersecurity [~~security~~] incidents as required by this section.

(b) [~~(c)~~] Not later than the 10th business day after the date of the eradication, closure, and recovery from a cybersecurity [~~security~~] incident, a state agency or local government shall notify the command [~~department~~], including the chief [~~information security officer~~], of the details of the cybersecurity [~~security~~]

incident and include in the notification an analysis of the cause of the cybersecurity [~~security~~] incident.

(c) [~~(d)~~] This section does not apply to a cybersecurity [~~security~~] incident that a local government is required to report to an independent organization certified by the Public Utility Commission of Texas under Section 39.151, Utilities Code.

Sec. 2063.303 [~~2054.077~~]. VULNERABILITY REPORTS. (a) In this section, a term defined by Section 33.01, Penal Code, has the meaning assigned by that section.

(b) The information security officer of a state agency shall prepare or have prepared a report, including an executive summary of the findings of the biennial report, not later than June 1 of each even-numbered year, assessing the extent to which a computer, a computer program, a computer network, a computer system, a printer, an interface to a computer system, including mobile and peripheral devices, computer software, or data processing of the agency or of a contractor of the agency is vulnerable to unauthorized access or harm, including the extent to which the agency's or contractor's electronically stored information is vulnerable to alteration, damage, erasure, or inappropriate use.

(c) Except as provided by this section, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is confidential and is not subject to disclosure under Chapter 552.

(d) The information security officer shall provide an electronic copy of the vulnerability report on its completion to:

(1) the command [~~department~~];

(2) the state auditor;

(3) the agency's executive director;

(4) the agency's designated information resources manager; and

(5) any other information technology security oversight group specifically authorized by the legislature to receive the report.

(e) Separate from the executive summary described by Subsection (b), a state agency shall prepare a summary of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. [~~The summary is available to the public on request.~~]

SECTION 10. Section 2054.515, Government Code, as amended by Chapters 567 (S.B. 475) and 856 (S.B. 800), Acts of the 87th Legislature, Regular Session, 2021, is transferred to Subchapter D, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.304, Government Code, reenacted, and amended to read as follows:

Sec. 2063.304 [~~2054.515~~]. AGENCY DATA GOVERNANCE [~~INFORMATION SECURITY~~] ASSESSMENT AND REPORT. (a) At least once every two years, each state agency shall conduct an [~~information security~~] assessment of the agency's[~~:~~

[~~(1) information resources systems, network systems,~~

~~digital data storage systems, digital data security measures, and information resources vulnerabilities; and~~

[~~(2)~~] data governance program with participation from the agency's data management officer, if applicable, and in accordance with requirements established by command [~~department~~] rule.

(b) Not later than June 1 of each even-numbered year, each state agency shall report the results of the assessment conducted under Subsection (a) to:

(1) the command; and

(2) on request, the governor, the lieutenant governor, and the speaker of the house of representatives.

[~~(b) Not later than November 15 of each even-numbered year, the agency shall report the results of the assessment to:~~

[~~(1) the department; and~~

[~~(2) on request, the governor, the lieutenant governor, and the speaker of the house of representatives.~~

[~~(b) Not later than December 1 of the year in which a state agency conducts the assessment under Subsection (a) or the 60th day after the date the agency completes the assessment, whichever occurs first, the agency shall report the results of the assessment to:~~

[~~(1) the department; and~~

[~~(2) on request, the governor, the lieutenant governor, and the speaker of the house of representatives.~~]

(c) The chief [~~department~~] by rule shall establish the requirements for the [~~information security~~] assessment and report

required by this section.

(d) The report and all documentation related to the [~~information security~~] assessment and report are confidential and not subject to disclosure under Chapter 552. The state agency or command [~~department~~] may redact or withhold the information as confidential under Chapter 552 without requesting a decision from the attorney general under Subchapter G, Chapter 552.

SECTION 11. Section 2054.136, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.401, Government Code, and amended to read as follows:

Sec. 2063.401 [~~2054.136~~]. DESIGNATED INFORMATION SECURITY OFFICER. Each state agency shall designate an information security officer who:

(1) reports to the agency's executive-level management;

(2) has authority over information security for the entire agency;

(3) possesses the training and experience required to ensure the agency complies with requirements and policies established by the command [~~perform the duties required by department rules~~]; and

(4) to the extent feasible, has information security duties as the officer's primary duties.

SECTION 12. Section 2054.518, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.402, Government

Code, and amended to read as follows:

Sec. 2063.402 [~~2054.518~~]. CYBERSECURITY RISKS AND INCIDENTS. (a) The command [~~department~~] shall develop a plan to address cybersecurity risks and incidents in this state. The command [~~department~~] may enter into an agreement with a national organization, including the National Cybersecurity Preparedness Consortium, to support the command's [~~department's~~] efforts in implementing the components of the plan for which the command [~~department~~] lacks resources to address internally. The agreement may include provisions for:

(1) providing technical assistance services to support preparedness for and response to cybersecurity risks and incidents;

(2) conducting cybersecurity simulation exercises for state agencies to encourage coordination in defending against and responding to cybersecurity risks and incidents;

(3) assisting state agencies in developing cybersecurity information-sharing programs to disseminate information related to cybersecurity risks and incidents; and

(4) incorporating cybersecurity risk and incident prevention and response methods into existing state emergency plans, including continuity of operation plans and incident response plans.

(b) In implementing the provisions of the agreement prescribed by Subsection (a), the command [~~department~~] shall seek to prevent unnecessary duplication of existing programs or efforts of the command [~~department~~] or another state agency.

(c) [~~(d)~~] The command [~~department~~] shall consult with institutions of higher education in this state when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.

SECTION 13. Section 2054.133, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.403, Government Code, and amended to read as follows:

Sec. 2063.403 [~~2054.133~~]. INFORMATION SECURITY PLAN. (a) Each state agency shall develop, and periodically update, an information security plan for protecting the security of the agency's information.

(b) In developing the plan, the state agency shall:

(1) consider any vulnerability report prepared under Section 2063.303 [~~2054.077~~] for the agency;

(2) incorporate the network security services provided by the department to the agency under Chapter 2059;

(3) identify and define the responsibilities of agency staff who produce, access, use, or serve as custodians of the agency's information;

(4) identify risk management and other measures taken to protect the agency's information from unauthorized access, disclosure, modification, or destruction;

(5) include:

(A) the best practices for information security developed by the command [~~department~~]; or

(B) if best practices are not applied, a written

explanation of why the best practices are not sufficient for the agency's security; and

(6) omit from any written copies of the plan information that could expose vulnerabilities in the agency's network or online systems.

(c) Not later than June 1 of each even-numbered year, each state agency shall submit a copy of the agency's information security plan to the command [~~department~~]. Subject to available resources, the command [~~department~~] may select a portion of the submitted security plans to be assessed by the command [~~department~~] in accordance with command policies [~~department rules~~].

(d) Each state agency's information security plan is confidential and exempt from disclosure under Chapter 552.

(e) Each state agency shall include in the agency's information security plan a written document that is signed by the head of the agency, the chief financial officer, and each executive manager designated by the state agency and states that those persons have been made aware of the risks revealed during the preparation of the agency's information security plan.

(f) Not later than November 15 of each even-numbered year, the command [~~department~~] shall 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 [~~department~~] evaluating information security for this state's information resources. In preparing the report, the command [~~department~~] shall consider the information security plans

submitted by state agencies under this section, any vulnerability reports submitted under Section 2063.303 [~~2054.077~~], and other available information regarding the security of this state's information resources. The command [~~department~~] shall omit from any written copies of the report information that could expose specific vulnerabilities [~~in the security of this state's information resources~~].

SECTION 14. Section 2054.516, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.405, Government Code, and amended to read as follows:

Sec. 2063.405 [~~2054.516~~]. DATA SECURITY PLAN FOR ONLINE AND MOBILE APPLICATIONS. (a) Each state agency implementing an Internet website or mobile application that processes any sensitive personal or personally identifiable information or confidential information must:

(1) submit a biennial data security plan to the command [~~department~~] not later than June 1 of each even-numbered year to establish planned beta testing for the website or application; and

(2) subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test.

(b) The command [~~department~~] shall review each data security plan submitted under Subsection (a) and make any recommendations for changes to the plan to the state agency as soon as practicable after the command [~~department~~] reviews the plan.

SECTION 15. Section 2054.512, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.406, Government Code, and amended to read as follows:

Sec. 2063.406 [~~2054.512~~]. CYBERSECURITY COUNCIL. (a) The chief or the chief's designee [~~state cybersecurity coordinator~~] shall [~~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) The cybersecurity council must include:

(1) one member who is an employee of the office of the governor;

(2) one member of the senate appointed by the lieutenant governor;

(3) one member of the house of representatives appointed by the speaker of the house of representatives;

(4) the director [~~one member who is an employee~~] of the Elections Division of the Office of the Secretary of State; [~~and~~]

(5) one member who is an employee of the department; and

(6) additional members appointed by the chief [~~state cybersecurity coordinator~~], including representatives of institutions of higher education and private sector leaders.

(c) 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) In appointing representatives from institutions of

higher education to the cybersecurity council, the chief [~~state cybersecurity coordinator~~] shall consider appointing members of the Information Technology Council for Higher Education.

(e) [~~(d)~~] The cybersecurity council shall:

(1) consider the costs and benefits of establishing a computer emergency readiness team to address cybersecurity incidents [~~cyber attacks~~] occurring in this state during routine and emergency situations;

(2) establish criteria and priorities for addressing cybersecurity threats to critical state installations;

(3) consolidate and synthesize best practices to assist state agencies in understanding and implementing cybersecurity measures that are most beneficial to this state; and

(4) assess the knowledge, skills, and capabilities of the existing information technology and cybersecurity workforce to mitigate and respond to cyber threats and develop recommendations for addressing immediate workforce deficiencies and ensuring a long-term pool of qualified applicants.

(f) [~~(e)~~] The chief, in collaboration with the cybersecurity council, shall provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for this state.

SECTION 16. Section 2054.514, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.407, Government Code, and amended to read as follows:

Sec. 2063.407 [~~2054.514~~]. RECOMMENDATIONS. The chief [~~state cybersecurity coordinator~~] may implement any portion, or all of the recommendations made by the cybersecurity council under Section 2063.406 [~~Cybersecurity, Education, and Economic Development Council under Subchapter N~~].

SECTION 17. Section 2054.0593, Government Code, is transferred to Subchapter E, Chapter 2063, Government Code, as added by this Act, redesignated as Section 2063.408, Government Code, and amended to read as follows:

Sec. 2063.408 [~~2054.0593~~]. CLOUD COMPUTING STATE RISK AND AUTHORIZATION MANAGEMENT PROGRAM. (a) In this section, "cloud computing service" has the meaning assigned by Section 2157.007.

(b) The command [~~department~~] shall establish a state risk and authorization management program to provide a standardized approach for security assessment, authorization, and continuous monitoring of cloud computing services that process the data of a state agency. The program must allow a vendor to demonstrate compliance by submitting documentation that shows the vendor's compliance with a risk and authorization management program of:

(1) the federal government; or

(2) another state that the command [~~department~~] approves.

(c) The command [~~department~~] by rule shall prescribe:

(1) the categories and characteristics of cloud computing services subject to the state risk and authorization management program; and

(2) the requirements for certification through the

program of vendors that provide cloud computing services.

(d) A state agency shall require each vendor contracting with the agency to provide cloud computing services for the agency to comply with the requirements of the state risk and authorization management program. The command [~~department~~] shall evaluate vendors to determine whether a vendor qualifies for a certification issued by the department reflecting compliance with program requirements.

(e) A state agency may not enter or renew a contract with a vendor to purchase cloud computing services for the agency that are subject to the state risk and authorization management program unless the vendor demonstrates compliance with program requirements.

(f) A state agency shall require a vendor contracting with the agency to provide cloud computing services for the agency that are subject to the state risk and authorization management program to maintain program compliance and certification throughout the term of the contract.

SECTION 18. Subchapter N-2, Chapter 2054, Government Code, is transferred to Chapter 2063, Government Code, as added by this Act, redesignated as Subchapter F, Chapter 2063, Government Code, and amended to read as follows:

SUBCHAPTER F [~~N-2~~]. TEXAS VOLUNTEER INCIDENT RESPONSE TEAM

Sec. 2063.501 [~~2054.52001~~]. DEFINITIONS. In this subchapter:

(1) "Incident response team" means the Texas volunteer incident response team established under Section 2063.502

[~~2054.52002~~].

(2) "Participating entity" means a state agency, including an institution of higher education, or a local government that receives assistance under this subchapter during a cybersecurity incident [~~event~~].

(3) "Volunteer" means an individual who provides rapid response assistance during a cybersecurity incident [~~event~~] under this subchapter.

Sec. 2063.502 [~~2054.52002~~]. ESTABLISHMENT OF TEXAS VOLUNTEER INCIDENT RESPONSE TEAM. (a) The command [~~department~~] shall establish the Texas volunteer incident response team to provide rapid response assistance to a participating entity under the command's [~~department's~~] direction during a cybersecurity incident [~~event~~].

(b) The command [~~department~~] shall prescribe eligibility criteria for participation as a volunteer member of the incident response team, including a requirement that each volunteer have expertise in addressing cybersecurity incidents [~~events~~].

Sec. 2063.503 [~~2054.52003~~]. CONTRACT WITH VOLUNTEERS. The command [~~department~~] shall enter into a contract with each volunteer the command [~~department~~] approves to provide rapid response assistance under this subchapter. The contract must require the volunteer to:

(1) acknowledge the confidentiality of information required by Section 2063.510 [~~2054.52010~~];

(2) protect all confidential information from disclosure;

(3) avoid conflicts of interest that might arise in a deployment under this subchapter;

(4) comply with command [~~department~~] security policies and procedures regarding information resources technologies;

(5) consent to background screening required by the command [~~department~~]; and

(6) attest to the volunteer's satisfaction of any eligibility criteria established by the command [~~department~~].

Sec. 2063.504 [~~2054.52004~~]. VOLUNTEER QUALIFICATION. (a) The command [~~department~~] shall require criminal history record information for each individual who accepts an invitation to become a volunteer.

(b) The command [~~department~~] may request other information relevant to the individual's qualification and fitness to serve as a volunteer.

(c) The command [~~department~~] has sole discretion to determine whether an individual is qualified to serve as a volunteer.

Sec. 2063.505 [~~2054.52005~~]. DEPLOYMENT. (a) In response to a cybersecurity incident [~~event~~] that affects multiple participating entities or a declaration by the governor of a state of disaster caused by a cybersecurity event, the command [~~department~~] on request of a participating entity may deploy volunteers and provide rapid response assistance under the command's [~~department's~~] direction and the managed security services framework established under Section 2063.204(c)

[~~2054.0594(d)~~] to assist with the incident [~~event~~].

(b) A volunteer may only accept a deployment under this subchapter in writing. A volunteer may decline to accept a deployment for any reason.

Sec. 2063.506 [~~2054.52006~~]. CYBERSECURITY COUNCIL DUTIES. The cybersecurity council established under Section 2063.406 [~~2054.512~~] shall review and make recommendations to the command [~~department~~] regarding the policies and procedures used by the command [~~department~~] to implement this subchapter. The command [~~department~~] may consult with the council to implement and administer this subchapter.

Sec. 2063.507 [~~2054.52007~~]. COMMAND [~~DEPARTMENT~~] POWERS AND DUTIES. (a) The command [~~department~~] shall:

(1) approve the incident response tools the incident response team may use in responding to a cybersecurity incident [~~event~~];

(2) establish the eligibility criteria an individual must meet to become a volunteer;

(3) develop and publish guidelines for operation of the incident response team, including the:

(A) standards and procedures the command [~~department~~] uses to determine whether an individual is eligible to serve as a volunteer;

(B) process for an individual to apply for and accept incident response team membership;

(C) requirements for a participating entity to receive assistance from the incident response team; and

(D) process for a participating entity to request and obtain the assistance of the incident response team; and

(4) adopt rules necessary to implement this subchapter.

(b) The command [~~department~~] may require a participating entity to enter into a contract as a condition for obtaining assistance from the incident response team. [~~The contract must comply with the requirements of Chapters 771 and 791.~~]

(c) The command [~~department~~] may provide appropriate training to prospective and approved volunteers.

(d) In accordance with state law, the command [~~department~~] may provide compensation for actual and necessary travel and living expenses incurred by a volunteer on a deployment using money available for that purpose.

(e) The command [~~department~~] may establish a fee schedule for participating entities receiving incident response team assistance. The amount of fees collected may not exceed the command's [~~department's~~] costs to operate the incident response team.

Sec. 2063.508 [~~2054.52008~~]. STATUS OF VOLUNTEER; LIABILITY. (a) A volunteer is not an agent, employee, or independent contractor of this state for any purpose and has no authority to obligate this state to a third party.

(b) This state is not liable to a volunteer for personal injury or property damage sustained by the volunteer that arises from participation in the incident response team.

Sec. 2063.509 [~~2054.52009~~]. CIVIL LIABILITY. A volunteer

who in good faith provides professional services in response to a cybersecurity incident [~~event~~] is not liable for civil damages as a result of the volunteer's acts or omissions in providing the services, except for wilful and wanton misconduct. This immunity is limited to services provided during the time of deployment for a cybersecurity incident [~~event~~].

Sec. 2063.510 [~~2054.52010~~]. CONFIDENTIAL INFORMATION. Information written, produced, collected, assembled, or maintained by the command [~~department~~], a participating entity, the cybersecurity council, or a volunteer in the implementation of this subchapter is confidential and not subject to disclosure under Chapter 552 if the information:

(1) contains the contact information for a volunteer;

(2) identifies or provides a means of identifying a person who may, as a result of disclosure of the information, become a victim of a cybersecurity incident [~~event~~];

(3) consists of a participating entity's cybersecurity plans or cybersecurity-related practices; or

(4) is obtained from a participating entity or from a participating entity's computer system in the course of providing assistance under this subchapter.

SECTION 19. Subchapter E, Chapter 2059, Government Code, is transferred to Chapter 2063, Government Code, as added by this Act, redesignated as Subchapter G, Chapter 2063, Government Code, and amended to read as follows:

SUBCHAPTER G [~~E~~]. REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTERS

Sec. 2063.601 [~~2059.201~~]. ELIGIBLE PARTICIPATING ENTITIES.

A state agency or an entity listed in Section 2059.058 is eligible to participate in cybersecurity support and network security provided by a regional [~~network~~] security operations center under this subchapter.

Sec. 2063.602 [~~2059.202~~]. ESTABLISHMENT OF REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTERS. (a) Subject to Subsection (b), the command [~~department~~] may establish regional [~~network~~] security operations centers, under the command's [~~department's~~] managed security services framework established by Section 2063.204(c) [~~2054.0594(d)~~], to assist in providing cybersecurity support and network security to regional offices or locations for state agencies and other eligible entities that elect to participate in and receive services through the center.

(b) The command [~~department~~] may establish more than one regional [~~network~~] security operations center only if the command [~~department~~] determines the first center established by the command [~~department~~] successfully provides to state agencies and other eligible entities the services the center has contracted to provide.

(c) The command [~~department~~] shall enter into an interagency contract in accordance with Chapter 771 or an interlocal contract in accordance with Chapter 791, as appropriate, with an eligible participating entity that elects to participate in and receive services through a regional [~~network~~] security operations center.

Sec. 2063.603 [~~2059.203~~]. REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTER LOCATIONS AND PHYSICAL SECURITY. (a) In

creating and operating a regional [~~network~~] security operations center, the command may [~~department shall~~] partner with a university system or institution of higher education as defined by Section 61.003, Education Code, other than a public junior college. The system or institution shall:

(1) serve as an education partner with the command [~~department~~] for the regional [~~network~~] security operations center; and

(2) enter into an interagency contract with the command [~~department~~] in accordance with Chapter 771.

(b) In selecting the location for a regional [~~network~~] security operations center, the command [~~department~~] shall select a university system or institution of higher education that has supportive educational capabilities.

(c) A university system or institution of higher education selected to serve as a regional [~~network~~] security operations center shall control and monitor all entrances to and critical areas of the center to prevent unauthorized entry. The system or institution shall restrict access to the center to only authorized individuals.

(d) A local law enforcement entity or any entity providing security for a regional [~~network~~] security operations center shall monitor security alarms at the regional [~~network~~] security operations center subject to the availability of that service.

(e) The command [~~department~~] and a university system or institution of higher education selected to serve as a regional [~~network~~] security operations center shall restrict operational

information to only center personnel, except as provided by Chapter 321.

Sec. 2063.604 [~~2059.204~~]. REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTERS SERVICES AND SUPPORT. The command [~~department~~] may offer the following managed security services through a regional [~~network~~] security operations center:

(1) real-time cybersecurity [~~network security~~] monitoring to detect and respond to cybersecurity incidents [~~network security events~~] that may jeopardize this state and the residents of this state;

(2) alerts and guidance for defeating cybersecurity [~~network security~~] threats, including firewall configuration, installation, management, and monitoring, intelligence gathering, and protocol analysis;

(3) immediate response to counter unauthorized [~~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;

(4) development, coordination, and execution of statewide cybersecurity operations to isolate, contain, and mitigate the impact of cybersecurity [~~network security~~] incidents for participating entities; and

(5) cybersecurity educational services.

Sec. 2063.605 [~~2059.205~~]. NETWORK SECURITY GUIDELINES AND STANDARD OPERATING PROCEDURES. (a) The command [~~department~~] shall adopt and provide to each regional [~~network~~] security operations

center appropriate network security guidelines and standard operating procedures to ensure efficient operation of the center with a maximum return on the state's investment.

(b) The command [~~department~~] shall revise the standard operating procedures as necessary to confirm network security.

(c) Each eligible participating entity that elects to participate in a regional [~~network~~] security operations center shall comply with the network security guidelines and standard operating procedures.

SECTION 20. Sections 11.175(c) and (h-1), Education Code, are amended to read as follows:

(c) A school district's cybersecurity policy may not conflict with the information security standards for institutions of higher education adopted by the Texas Cyber Command [~~Department of Information Resources~~] under Chapters [~~2054 and~~] 2059 and 2063, Government Code.

(h-1) Notwithstanding Section 2063.103 [~~2054.5191~~], Government Code, only the district's cybersecurity coordinator is required to complete the cybersecurity training under that section on an annual basis. Any other school district employee required to complete the cybersecurity training shall complete the training as determined by the district, in consultation with the district's cybersecurity coordinator.

SECTION 21. Section 38.307(e), Education Code, is amended to read as follows:

(e) The agency shall maintain the data collected by the task force and the work product of the task force in accordance with:

(1) the agency's information security plan under Section 2063.403 [~~2054.133~~], Government Code; and

(2) the agency's records retention schedule under Section 441.185, Government Code.

SECTION 22. Section 325.011, Government Code, is amended to read as follows:

Sec. 325.011. CRITERIA FOR REVIEW. The commission and its staff shall consider the following 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:

(1) the efficiency and effectiveness with which the agency or the advisory committee operates;

(2)(A) an identification of the mission, goals, and objectives intended for the agency or advisory committee and of the problem or need that the agency or advisory committee was intended to address; and

(B) the extent to which the mission, goals, and objectives have been achieved and the problem or need has been addressed;

(3)(A) an identification of any activities of the agency in addition to those granted by statute and of the authority for those activities; and

(B) the extent to which those activities are needed;

(4) an assessment of authority of the agency relating to fees, inspections, enforcement, and penalties;

(5) whether less restrictive or alternative methods of performing any function that the agency performs could adequately protect or provide service to the public;

(6) the extent to which the jurisdiction of the agency and the programs administered by the agency overlap or duplicate those of other agencies, the extent to which the agency coordinates with those agencies, and the extent to which the programs administered by the agency can be consolidated with the programs of other state agencies;

(7) the promptness and effectiveness with which the agency addresses complaints concerning entities or other persons affected by the agency, including an assessment of the agency's administrative hearings process;

(8) an assessment of the agency's rulemaking process and the extent to which the agency has encouraged participation by the public in making its rules and decisions and the extent to which the public participation has resulted in rules that benefit the public;

(9) the extent to which the agency has complied with:

(A) federal and state laws and applicable rules regarding equality of employment opportunity and the rights and privacy of individuals; and

(B) state law and applicable rules of any state agency regarding purchasing guidelines and programs for historically underutilized businesses;

(10) the extent to which the agency issues and enforces rules relating to potential conflicts of interest of its

employees;

(11) the extent to which the agency complies with Chapters 551 and 552 and follows records management practices that enable the agency to respond efficiently to requests for public information;

(12) the effect of federal intervention or loss of federal funds if the agency is abolished;

(13) the extent to which the purpose and effectiveness of reporting requirements imposed on the agency justifies the continuation of the requirement; and

(14) an assessment of the agency's cybersecurity practices using confidential information available from the Department of Information Resources, the Texas Cyber Command, or any other appropriate state agency.

SECTION 23. Section 411.0765(b), Government Code, is amended to read as follows:

(b) A criminal justice agency may disclose criminal history record information that is the subject of an order of nondisclosure of criminal history record information under this subchapter to the following noncriminal justice agencies or entities only:

(1) the State Board for Educator Certification;

(2) a school district, charter school, private school, regional education service center, commercial transportation company, or education shared services arrangement;

(3) the Texas Medical Board;

(4) the Texas School for the Blind and Visually Impaired;

(5) the Board of Law Examiners;

(6) the State Bar of Texas;

(7) a district court regarding a petition for name change under Subchapter B, Chapter 45, Family Code;

(8) the Texas School for the Deaf;

(9) the Department of Family and Protective Services;

(10) the Texas Juvenile Justice Department;

(11) the Department of Assistive and Rehabilitative Services;

(12) the Department of State Health Services, a local mental health service, a local intellectual and developmental disability authority, or a community center providing services to persons with mental illness or intellectual or developmental disabilities;

(13) the Texas Private Security Board;

(14) a municipal or volunteer fire department;

(15) the Texas Board of Nursing;

(16) a safe house providing shelter to children in harmful situations;

(17) a public or nonprofit hospital or hospital district, or a facility as defined by Section 250.001, Health and Safety Code;

(18) the securities commissioner, the banking commissioner, the savings and mortgage lending commissioner, the consumer credit commissioner, or the credit union commissioner;

(19) the Texas State Board of Public Accountancy;

(20) the Texas Department of Licensing and Regulation;

(21) the Health and Human Services Commission;

(22) the Department of Aging and Disability Services;

(23) the Texas Education Agency;

(24) the Judicial Branch Certification Commission;

(25) a county clerk's office in relation to a proceeding for the appointment of a guardian under Title 3, Estates Code;

(26) the Texas Cyber Command [~~Department of Information Resources~~] but only regarding an employee, applicant for employment, contractor, subcontractor, intern, or volunteer who provides network security services under Chapter 2059 to:

(A) the Texas Cyber Command [~~Department of Information Resources~~]; or

(B) a contractor or subcontractor of the Texas Cyber Command [~~Department of Information Resources~~];

(27) the Texas Department of Insurance;

(28) the Teacher Retirement System of Texas;

(29) the Texas State Board of Pharmacy;

(30) the Texas Civil Commitment Office;

(31) a bank, savings bank, savings and loan association, credit union, or mortgage banker, a subsidiary or affiliate of those entities, or another financial institution regulated by a state regulatory entity listed in Subdivision (18) or by a corresponding federal regulatory entity, but only regarding an employee, contractor, subcontractor, intern, or volunteer of or an applicant for employment by that bank, savings bank, savings and loan association, credit union, mortgage banker, subsidiary or

affiliate, or financial institution; and

(32) an employer that has a facility that handles or has the capability of handling, transporting, storing, processing, manufacturing, or controlling hazardous, explosive, combustible, or flammable materials, if:

(A) the facility is critical infrastructure, as defined by 42 U.S.C. Section 5195c(e), or the employer is required to submit to a risk management plan under Section 112(r) of the federal Clean Air Act (42 U.S.C. Section 7412) for the facility; and

(B) the information concerns an employee, applicant for employment, contractor, or subcontractor whose duties involve or will involve the handling, transporting, storing, processing, manufacturing, or controlling hazardous, explosive, combustible, or flammable materials and whose background is required to be screened under a federal provision described by Paragraph (A).

SECTION 24. Section 418.0195(a), Government Code, is amended to read as follows:

(a) This section applies only to a computer network used by:

(1) a state agency; or

(2) an entity other than a state agency receiving network security services from the Texas Cyber Command [~~Department of Information Resources~~] under Section 2059.058.

SECTION 25. Sections 772.012(b) and (c), Government Code, are amended to read as follows:

(b) To apply for a grant under this chapter, a local government must submit with the grant application a written

certification of the local government's compliance with the cybersecurity training required by Section 2063.103 [~~2054.5191~~].

(c) On a determination by the criminal justice division established under Section 772.006 that a local government awarded a grant under this chapter has not complied with the cybersecurity training required by Section 2063.103 [~~2054.5191~~], the local government shall pay to this state an amount equal to the amount of the grant award. A local government that is the subject of a determination described by this subsection is ineligible for another grant under this chapter until the second anniversary of the date the local government is determined ineligible.

SECTION 26. Section 2054.380(b), Government Code, is amended to read as follows:

(b) Revenue derived from the collection of fees imposed under Subsection (a) may be appropriated to the department for:

(1) developing statewide information resources technology policies and planning under this chapter [~~and Chapter 2059~~]; and

(2) providing shared information resources technology services under this chapter.

SECTION 27. Section 2054.0701(c), Government Code, is amended to read as follows:

(c) A program offered under this section must:

(1) be approved by the Texas Higher Education Coordinating Board in accordance with Section 61.0512, Education Code;

(2) develop the knowledge and skills necessary for an

entry-level information technology position in a state agency; and

(3) include a one-year apprenticeship with:

(A) the department;

(B) another relevant state agency;

(C) an organization working on a major information resources project; or

(D) a regional [~~network~~] security operations center established under Section 2063.602 [~~2059.202~~].

SECTION 28. Section 2056.002(b), Government Code, is amended to read as follows:

(b) The Legislative Budget Board and the governor's office shall determine the elements required to be included in each agency's strategic plan. Unless modified by the Legislative Budget Board and the governor's office, and except as provided by Subsection (c), a plan must include:

(1) a statement of the mission and goals of the state agency;

(2) a description of the indicators developed under this chapter and used to measure the output and outcome of the agency;

(3) identification of the groups of people served by the agency, including those having service priorities, or other service measures established by law, and estimates of changes in those groups expected during the term of the plan;

(4) an analysis of the use of the agency's resources to meet the agency's needs, including future needs, and an estimate of additional resources that may be necessary to meet future needs;

(5) an analysis of expected changes in the services provided by the agency because of changes in state or federal law;

(6) a description of the means and strategies for meeting the agency's needs, including future needs, and achieving the goals established under Section 2056.006 for each area of state government for which the agency provides services;

(7) a description of the capital improvement needs of the agency during the term of the plan and a statement, if appropriate, of the priority of those needs;

(8) identification of each geographic region of this state, including the Texas-Louisiana border region and the Texas-Mexico border region, served by the agency, and if appropriate the agency's means and strategies for serving each region;

(9) a description of the training of the agency's contract managers under Section 656.052;

(10) an analysis of the agency's expected expenditures that relate to federally owned or operated military installations or facilities, or communities where a federally owned or operated military installation or facility is located;

(11) an analysis of the strategic use of information resources as provided by the instructions prepared under Section 2054.095;

(12) a written certification of the agency's compliance with the cybersecurity training required under Sections 2063.103 [~~2054.5191~~] and 2063.104 [~~2054.5192~~]; and

(13) other information that may be required.

SECTION 29. Section 2059.001, Government Code, is amended by adding Subdivision (1-a) to read as follows:

(1-a) "Command" means the Texas Cyber Command.

SECTION 30. Section 2059.051, Government Code, is amended to read as follows:

Sec. 2059.051. COMMAND [~~DEPARTMENT~~] RESPONSIBLE FOR PROVIDING COMPUTER NETWORK SECURITY SERVICES. The command [~~department~~] shall provide network security services to:

(1) state agencies; and

(2) other entities by agreement as provided by Section 2059.058.

SECTION 31. Section 2059.052, Government Code, is amended to read as follows:

Sec. 2059.052. SERVICES PROVIDED TO INSTITUTIONS OF HIGHER EDUCATION. The command [~~department~~] may provide network security services to an institution of higher education, and may include an institution of higher education in a center, only if and to the extent approved by the Information Technology Council for Higher Education.

SECTION 32. Section 2059.053, Government Code, is amended to read as follows:

Sec. 2059.053. RULES. The command [~~department~~] may adopt rules necessary to implement this chapter.

SECTION 33. Section 2059.054, Government Code, is amended to read as follows:

Sec. 2059.054. OWNERSHIP OR LEASE OF NECESSARY EQUIPMENT. The command [~~department~~] may purchase in accordance

with Chapters 2155, 2156, 2157, and 2158 any facilities or equipment necessary to provide network security services to state agencies.

SECTION 34. Section 2059.055(a), Government Code, is amended to read as follows:

(a) Confidential network security information may be released only to officials responsible for the network, law enforcement, the state auditor's office, and agency or elected officials designated by the command [~~department~~].

SECTION 35. Section 2059.056, Government Code, is amended to read as follows:

Sec. 2059.056. RESPONSIBILITY FOR EXTERNAL AND INTERNAL SECURITY THREATS. If the command [~~department~~] provides network security services for a state agency or other entity under this chapter, the command [~~department~~] is responsible for network security from external threats for that agency or entity. Network security management for that state agency or entity regarding internal threats remains the responsibility of that state agency or entity.

SECTION 36. Section 2059.057, Government Code, is amended to read as follows:

Sec. 2059.057. BIENNIAL REPORT. (a) The command [~~department~~] shall biennially prepare a report on:

(1) the command's [~~department's~~] accomplishment of service objectives and other performance measures under this chapter; and

(2) the status, including the financial performance,

of the consolidated network security system provided through the center.

(b) The command [~~department~~] shall submit the report to:

(1) the governor;

(2) the lieutenant governor;

(3) the speaker of the house of representatives; and

(4) the state auditor's office.

SECTION 37. Section 2059.058, Government Code, is amended to read as follows:

Sec. 2059.058. AGREEMENT TO PROVIDE NETWORK SECURITY SERVICES TO ENTITIES OTHER THAN STATE AGENCIES. In addition to the command's [~~department's~~] duty to provide network security services to state agencies under this chapter, the command [~~department~~] by agreement may provide network security services to:

(1) each house of the legislature and a legislative agency;

(2) a local government;

(3) the supreme court, the court of criminal appeals, or a court of appeals;

(4) a public hospital owned or operated by this state or a political subdivision or municipal corporation of this state, including a hospital district or hospital authority;

(5) the Texas Permanent School Fund Corporation;

(6) an open-enrollment charter school, as defined by Section 5.001, Education Code;

(7) a private school, as defined by Section 5.001, Education Code;

(8) a private or independent institution of higher education, as defined by Section 61.003, Education Code;

(9) a volunteer fire department, as defined by Section 152.001, Tax Code; and

(10) an independent organization certified under Section 39.151, Utilities Code, for the ERCOT power region.

SECTION 38. Section 2059.101, Government Code, is amended to read as follows:

Sec. 2059.101. NETWORK SECURITY CENTER. The command [~~department~~] shall establish a network security center to provide network security services to state agencies.

SECTION 39. Sections 2059.102(a), (b), and (d), Government Code, are amended to read as follows:

(a) The command [~~department~~] shall manage the operation of network security system services for all state agencies at the center.

(b) The command [~~department~~] shall fulfill the network security requirements of each state agency to the extent practicable. However, the command [~~department~~] shall protect criminal justice and homeland security networks of this state to the fullest extent possible in accordance with federal criminal justice and homeland security network standards.

(d) A state agency may not purchase network security services unless the command [~~department~~] determines that the agency's requirement for network security services cannot be met at a comparable cost through the center. The command [~~department~~] shall develop an efficient process for this determination.

SECTION 40. Sections 2059.103(a), (b), and (d), Government Code, are amended to read as follows:

(a) The command [~~department~~] shall locate the center at a location that has an existing secure and restricted facility, cyber-security infrastructure, available trained workforce, and supportive educational capabilities.

(b) The command [~~department~~] shall control and monitor all entrances and critical areas to prevent unauthorized entry. The command [~~department~~] shall limit access to authorized individuals.

(d) The command [~~department~~] shall restrict operational information to personnel at the center, except as provided by Chapter 321.

SECTION 41. Section 2059.104, Government Code, is amended to read as follows:

Sec. 2059.104. CENTER SERVICES AND SUPPORT. (a) The command [~~department~~] shall provide the following managed security services through the center:

(1) real-time network security monitoring to detect and respond to network security events that may jeopardize this state and the residents of this state, including vulnerability assessment services consisting of a comprehensive security posture assessment, external and internal threat analysis, and penetration testing;

(2) continuous, 24-hour alerts and guidance for defeating network security threats, including firewall preconfiguration, installation, management and monitoring, intelligence gathering, protocol analysis, and user

authentication;

(3) immediate incident response to counter network security activity that exposes this state and the residents of this state to risk, including complete intrusion detection systems installation, management, and monitoring and a network operations call center;

(4) development, coordination, and execution of statewide cyber-security operations to isolate, contain, and mitigate the impact of network security incidents at state agencies;

(5) operation of a central authority for all statewide information assurance programs; and

(6) the provision of educational services regarding network security.

(b) The command [~~department~~] may provide:

(1) implementation of best-of-breed information security architecture engineering services, including public key infrastructure development, design, engineering, custom software development, and secure web design; or

(2) certification and accreditation to ensure compliance with the applicable regulatory requirements for cyber-security and information technology risk management, including the use of proprietary tools to automate the assessment and enforcement of compliance.

SECTION 42. Sections 2059.105(a) and (b), Government Code, are amended to read as follows:

(a) The command [~~department~~] shall adopt and provide to all

state agencies appropriate network security guidelines and standard operating procedures to ensure efficient operation of the center with a maximum return on investment for the state.

(b) The command [~~department~~] shall revise the standard operating procedures as necessary to confirm network security.

SECTION 43. Section 2059.1055, Government Code, is amended to read as follows:

Sec. 2059.1055. NETWORK SECURITY IN A STATE OF DISASTER. The command [~~department~~] shall disconnect the computer network of an entity receiving security services under this chapter from the Internet if the governor issues an order under Section 418.0195 to disconnect the network because of a substantial external threat to the entity's computer network.

SECTION 44. Section 2059.106, Government Code, is amended to read as follows:

Sec. 2059.106. PRIVATE VENDOR. The command [~~department~~] may contract with a private vendor to build and operate the center and act as an authorized agent to acquire, install, integrate, maintain, configure, and monitor the network security services and security infrastructure elements.

SECTION 45. Section 2059.151, Government Code, is amended to read as follows:

Sec. 2059.151. PAYMENT FOR SERVICES. The department shall develop a system of billings and charges for services provided by the command in operating and administering the network security system that allocates the total state cost to each state agency or other entity served by the system based on proportionate usage.

SECTION 46. Section 2059.152, Government Code, is amended by adding Subsection (d) to read as follows:

(d) The department shall enter into an agreement with the command to transfer funds as necessary for the performance of functions under this chapter.

SECTION 47. Section 2059.153, Government Code, is amended to read as follows:

Sec. 2059.153. GRANTS. The command [~~department~~] may apply for and use for purposes of this chapter the proceeds from grants offered by any federal agency or other source.

SECTION 48. Section 2157.068(d), Government Code, is amended to read as follows:

(d) The department may charge a reasonable administrative fee to a state agency, local government, or governmental entity of another state that purchases commodity items through the department in an amount that is sufficient to recover costs associated with the administration of this section. Revenue derived from the collection of fees imposed under this subsection may be appropriated to the department for:

(1) developing statewide information resources technology policies and planning under Chapter [~~Chapters~~] 2054 [~~and 2059~~]; and

(2) providing shared information resources technology services under Chapter 2054.

SECTION 49. Section 2170.057(a), Government Code, is amended to read as follows:

(a) The department shall develop a system of billings and

charges for services provided in operating and administering the consolidated telecommunications system that allocates the total state cost to each entity served by the system based on proportionate usage. The department shall set and charge a fee to each entity that receives services provided under this chapter in an amount sufficient to cover the direct and indirect costs of providing the service. Revenue derived from the collection of fees imposed under this subsection may be appropriated to the department for:

(1) developing statewide information resources technology policies and planning under Chapter [~~Chapters~~] 2054 [~~and 2059~~]; and

(2) providing[~~+~~

[~~(A)~~] shared information resources technology services under Chapter 2054[~~; and~~

[~~(B) network security services under Chapter 2059~~].

SECTION 50. The following provisions of the Government Code are repealed:

(1) Section 2054.059;

(2) Section 2054.076(b-1);

(3) Section 2054.511; and

(4) Section 2054.5181.

SECTION 51. (a) In this section, "department" means the Department of Information Resources.

(b) On the effective date of this Act, the Texas Cyber 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, and Chapter 2059, Government Code, as amended by this Act.

(b-1) As soon as practicable on or after the effective date of this Act, the governor shall appoint the chief of the Texas Cyber Command, as described by Section 2063.0025, Government Code, as added by this Act, to a term expiring February 1, 2027.

(c) Notwithstanding Subsection (b) of this section, the department shall continue to perform duties and exercise powers under Chapters 2054 and 2059, 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) Not later than December 31, 2026:

(1) all functions and activities performed by the department 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;

(2) all employees of the department 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 Texas Cyber 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 the department that relates 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, is a rule or form of the Texas Cyber Command and remains in effect until changed by the command;

(4) a reference in law to the department that relates 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, means the Texas Cyber 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 the department that is 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, is transferred without change in status to the Texas Cyber Command, and the Texas Cyber Command assumes, without a change in status, the position of the department in a negotiation or proceeding relating to cybersecurity or network security to which the department is a party;

(6) all money, leases, rights, and obligations of the department 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, are transferred to the Texas Cyber Command;

(7) contracts specified as necessary to accomplish the

goals and duties of the Texas Cyber 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 Texas Cyber Command;

(8) all property, including records, in the custody of the department 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, becomes property of the Texas Cyber 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 the department for purposes 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, are transferred to the Texas Cyber Command.

(e) Not later than January 1, 2026, the department and Texas Cyber Command shall enter into a memorandum of understanding relating to the transfer of powers and duties from the department to the Texas Cyber Command as provided by this Act. The memorandum must 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 or network security 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 52. This Act takes effect September 1, 2025.

ADOPTED

MAY 27 2025

Secretary of the Senate

FLOOR AMENDMENT NO. 1 BY: Tom Parker

Amend C.S.H.B. No. 150 (89R 33580) as follows:

(1) In SECTION 1 of the bill, in added Section 2063.009, Government Code (page 8, lines 20 and 21), strike ", with advice from the department,".

(2) Strike SECTION 10 of the bill (page 26, line 17, through page 28, line 7), and renumber subsequent SECTIONS of the bill accordingly.

(3) In SECTION 43 of the bill, in Section 2059.1055, Government Code (page 61, lines 8 though 13) amend to read as follows:

Sec.2059.1055.NETWORK SECURITY IN A STATE OF DISASTER. The department, in coordination with the command, shall disconnect the computer network of an entity receiving security services under this chapter from the Internet if the governor issues an order under Section 418.0195 to disconnect the network because of a substantial external threat to the entity 's computer network.

(4) In SECTION 51 of the bill, in Subsection (b-1) (page 64, line 6), strike "2063.0025" and substitute "2063.002".

**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

**LEGISLATIVE BUDGET BOARD**
**Austin, Texas**

**FISCAL NOTE, 89TH LEGISLATIVE REGULAR SESSION**

**May 27, 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 and the transfer to it of certain powers and duties of the Department of Information Resources.), **Committee Report 2nd House, Substituted**

**Estimated Two-year Net Impact to General Revenue Related Funds** for HB150, Committee Report 2nd House, Substituted: 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. Additionally, each state agency would be required to, at least once every two years, assess the agency's data governance program and report the results to the Command, and upon request, to the Governor, Lieutenant Governor, and Speaker of the House.

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

**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

**LEGISLATIVE BUDGET BOARD**
**Austin, Texas**

**FISCAL NOTE, 89TH LEGISLATIVE REGULAR SESSION**

**March 30, 2025**

**TO:** Honorable Giovanni Capriglione, Chair, House Committee on Delivery of Government Efficiency

**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.), **Committee Report 1st House, Substituted**

**Estimated Two-year Net Impact to General Revenue Related Funds** for HB150, Committee Report 1st House, Substituted: 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

**LEGISLATIVE BUDGET BOARD**
**Austin, Texas**

**FISCAL NOTE, 89TH LEGISLATIVE REGULAR SESSION**

**March 18, 2025**

**TO:** Honorable Giovanni Capriglione, Chair, House Committee on Delivery of Government Efficiency

**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 Introduced**

**Estimated Two-year Net Impact to General Revenue Related Funds** for HB150, As Introduced: a negative impact of ($196,936,455) 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 | ($88,715,399) |
| 2027 | ($108,221,056) |
| 2028 | ($69,311,249) |
| 2029 | ($71,187,923) |
| 2030 | ($76,415,652) |

**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 | ($88,715,399) | 50.0 |
| 2027 | ($108,221,056) | 143.0 |
| 2028 | ($69,311,249) | 143.0 |
| 2029 | ($71,187,923) | 143.0 |
| 2030 | ($76,415,652) | 143.0 |

**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; (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; and (13) 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 26.0 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 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 as well as estimated annual costs beginning in fiscal year 2026 of $4.4 million increasing to $5.2 million by FY 2030. There would also be other operating expenses, primarily rent of an office in Austin, of $1.8 million, beginning in fiscal year 2026.

Beginning in fiscal year 2026, it is estimated that 50.0 FTEs would need to be hired to implement provisions of the bill. Beginning in fiscal year 2027, it is estimated that approximately 143.0 full-time equivalents would be required to fulfill all the responsibilities and duties of the Command as articulated in the bill: 24.0 for the Cyber Threat Intelligence Center; 68.0 for the Cybersecurity Incident Response Unit; 24.0 for the Digital Forensics Laboratory; 10.0 for training, compliance, and reporting; and 17.0 for the office of the director. 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 50.0 FTEs in fiscal year 2026 is estimated at $8.3 million. The total costs for the 143.0 FTEs in fiscal year 2027 is estimated at $23.7 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 $0.5 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 $40.5 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