

1-1 By: Capriglione, et al. (Senate Sponsor - Parker) H.B. No. 150
 1-2 (In the Senate - Received from the House April 16, 2025;
 1-3 April 28, 2025, read first time and referred to Committee on
 1-4 Business & Commerce; May 27, 2025, reported adversely, with
 1-5 favorable Committee Substitute by the following vote: Yeas 11,
 1-6 Nays 0; May 27, 2025, sent to printer.)

1-7 COMMITTEE VOTE

	Yea	Nay	Absent	PNV
1-8				
1-9	X			
1-10	X			
1-11	X			
1-12	X			
1-13	X			
1-14	X			
1-15	X			
1-16	X			
1-17	X			
1-18	X			
1-19	X			

1-20 COMMITTEE SUBSTITUTE FOR H.B. No. 150 By: King

1-21 A BILL TO BE ENTITLED
 1-22 AN ACT

1-23 relating to the establishment of the Texas Cyber Command and the
 1-24 transfer to it of certain powers and duties of the Department of
 1-25 Information Resources.

1-26 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

1-27 SECTION 1. Subtitle B, Title 10, Government Code, is
 1-28 amended by adding Chapter 2063 to read as follows:

1-29 CHAPTER 2063. TEXAS CYBER COMMAND

1-30 SUBCHAPTER A. GENERAL PROVISIONS

1-31 Sec. 2063.001. DEFINITIONS. In this chapter:

1-32 (1) "Chief" means the chief of the Texas Cyber
 1-33 Command.

1-34 (2) "Command" means the Texas Cyber Command
 1-35 established under this chapter.

1-36 (3) "Covered entity" means a private entity operating
 1-37 critical infrastructure or a local government that the command
 1-38 contracts with in order to provide cybersecurity services under
 1-39 this chapter.

1-40 (4) "Critical infrastructure" means infrastructure in
 1-41 this state vital to the security, governance, public health and
 1-42 safety, economy, or morale of the state or the nation, including:

1-43 (A) chemical facilities;

1-44 (B) commercial facilities;

1-45 (C) communication facilities;

1-46 (D) manufacturing facilities;

1-47 (E) dams;

1-48 (F) defense industrial bases;

1-49 (G) emergency services systems;

1-50 (H) energy facilities;

1-51 (I) financial services systems;

1-52 (J) food and agriculture facilities;

1-53 (K) government facilities;

1-54 (L) health care and public health facilities;

1-55 (M) information technology and information
 1-56 technology systems;

1-57 (N) nuclear reactors, materials, and waste;

1-58 (O) transportation systems; or

1-59 (P) water and wastewater systems.

1-60 (5) "Cybersecurity" means the measures taken for a

2-1 computer, computer network, computer system, or other technology
2-2 infrastructure to protect against, respond to, and recover from
2-3 unauthorized:
2-4 (A) use, access, disruption, modification, or
2-5 destruction; or
2-6 (B) disclosure, modification, or destruction of
2-7 information.
2-8 (6) "Cybersecurity incident" includes:
2-9 (A) a breach or suspected breach of system
2-10 security as defined by Section 521.053, Business & Commerce Code;
2-11 (B) the introduction of ransomware, as defined by
2-12 Section 33.023, Penal Code, into a computer, computer network, or
2-13 computer system; or
2-14 (C) any other cybersecurity-related occurrence
2-15 that jeopardizes information or an information system designated by
2-16 command policy adopted under this chapter.
2-17 (7) "Department" means the Department of Information
2-18 Resources.
2-19 (8) "Governmental entity" means a state agency or a
2-20 local government.
2-21 (9) "Information resources" has the meaning assigned
2-22 by Section 2054.003.
2-23 (10) "Information resources technologies" has the
2-24 meaning assigned by Section 2054.003.
2-25 (11) "Local government" has the meaning assigned by
2-26 Section 2054.003.
2-27 (12) "Sensitive personal information" has the meaning
2-28 assigned by Section 521.002, Business & Commerce Code.
2-29 (13) "State agency" means:
2-30 (A) a department, commission, board, office, or
2-31 other agency that is in the executive branch of state government and
2-32 that was created by the constitution or a statute;
2-33 (B) the supreme court, the court of criminal
2-34 appeals, a court of appeals, a district court, or the Texas Judicial
2-35 Council or another agency in the judicial branch of state
2-36 government; or
2-37 (C) a university system or an institution of
2-38 higher education as defined by Section 61.003, Education Code.
2-39 Sec. 2063.002. ORGANIZATION. (a) The Texas Cyber Command
2-40 is a state agency.
2-41 (b) The command is governed by a chief appointed by the
2-42 governor and confirmed with the advice and consent of the senate.
2-43 The chief serves for a two-year term expiring February 1 of each
2-44 odd-numbered year and must possess professional training and
2-45 knowledge relevant to the functions and duties of the command.
2-46 (c) The command shall employ other coordinating and
2-47 planning officers and other personnel necessary to the performance
2-48 of its functions.
2-49 (d) The command may enter into an interagency agreement with
2-50 another state agency for the purpose of providing:
2-51 (1) administrative support services to the command as
2-52 necessary to carry out the purposes of this chapter and Chapter
2-53 2059; and
2-54 (2) a facility to the command located in San Antonio
2-55 that has a sensitive compartmented information facility for use in
2-56 carrying out the purposes of this chapter and Chapter 2059.
2-57 Sec. 2063.003. ESTABLISHMENT AND PURPOSE. (a) The command
2-58 is established to prevent and respond to cybersecurity incidents
2-59 that affect governmental entities and critical infrastructure in
2-60 this state.
2-61 (b) The command is responsible for cybersecurity for this
2-62 state, including:
2-63 (1) providing leadership, guidance, and tools to
2-64 enhance cybersecurity defenses;
2-65 (2) facilitating education and training of a
2-66 cybersecurity workforce;
2-67 (3) monitoring and coordinating cyber threat
2-68 intelligence and information systems to detect and warn entities of
2-69 cyber attacks, identifying cyber threats to critical

3-1 infrastructure and state systems, planning and executing
3-2 cybersecurity incident responses, and conducting digital forensics
3-3 of cybersecurity incidents to support law enforcement and attribute
3-4 the incidents;
3-5 (4) creating partnerships needed to effectively carry
3-6 out the command's functions; and
3-7 (5) receiving all cybersecurity incident reports from
3-8 state agencies and covered entities.
3-9 Sec. 2063.004. GENERAL POWERS AND DUTIES. (a) The command
3-10 shall:
3-11 (1) promote public awareness of cybersecurity issues;
3-12 (2) develop cybersecurity best practices and minimum
3-13 standards for governmental entities;
3-14 (3) develop and provide training to state agencies and
3-15 covered entities on cybersecurity measures and awareness;
3-16 (4) administer the cybersecurity threat intelligence
3-17 center under Section 2063.201;
3-18 (5) provide support to state agencies and covered
3-19 entities experiencing a cybersecurity incident and respond to
3-20 cybersecurity reports received under Subchapter D and other reports
3-21 as appropriate;
3-22 (6) administer the digital forensics laboratory under
3-23 Section 2063.203;
3-24 (7) administer a statewide portal for enterprise
3-25 cybersecurity threat, risk, and incident management, and operate a
3-26 cybersecurity hotline available for state agencies and covered
3-27 entities 24 hours a day, seven days a week;
3-28 (8) collaborate with law enforcement agencies to
3-29 provide training and support related to cybersecurity incidents;
3-30 (9) serve as a clearinghouse for information relating
3-31 to all aspects of protecting the cybersecurity of governmental
3-32 entities, including sharing appropriate intelligence and
3-33 information with governmental entities, federal agencies, and
3-34 covered entities;
3-35 (10) collaborate with the department to ensure
3-36 information resources and information resources technologies
3-37 obtained by the department meet the cybersecurity standards and
3-38 requirements established under this chapter;
3-39 (11) offer cybersecurity resources to state agencies
3-40 and covered entities as determined by the command;
3-41 (12) adopt policies to ensure state agencies implement
3-42 sufficient cybersecurity measures to defend information resources,
3-43 information resources technologies, and sensitive personal
3-44 information maintained by the agencies; and
3-45 (13) collaborate with federal agencies to protect
3-46 against, respond to, and recover from cybersecurity incidents.
3-47 (b) The command may:
3-48 (1) adopt and use an official seal;
3-49 (2) establish ad hoc advisory committees as necessary
3-50 to carry out the command's duties under this chapter;
3-51 (3) acquire and convey property or an interest in
3-52 property;
3-53 (4) procure insurance and pay premiums on insurance of
3-54 any type, in accounts, and from insurers as the command considers
3-55 necessary and advisable to accomplish any of the command's duties;
3-56 (5) hold patents, copyrights, trademarks, or other
3-57 evidence of protection or exclusivity issued under the laws of the
3-58 United States, any state, or any nation and may enter into license
3-59 agreements with any third parties for the receipt of fees,
3-60 royalties, or other monetary or nonmonetary value; and
3-61 (6) solicit and accept gifts, grants, donations, or
3-62 loans from and contract with any entity to accomplish the command's
3-63 duties.
3-64 (c) Except as otherwise provided by this chapter, the
3-65 command shall deposit money paid to the command under this chapter
3-66 in the state treasury to the credit of the general revenue fund.
3-67 Sec. 2063.005. COST RECOVERY. The command may recover the
3-68 cost of providing direct technical assistance, training services,
3-69 and other services to covered entities when reasonable and

4-1 practical.

4-2 Sec. 2063.007. EMERGENCY PURCHASING IN RESPONSE TO
 4-3 CYBERSECURITY INCIDENT. (a) In the event the emergency response to
 4-4 a cybersecurity incident requires the command to purchase an item,
 4-5 the command is exempt from the requirements of Sections [2155.0755](#),
 4-6 [2155.083](#), and [2155.132](#)(c) in making the purchase.

4-7 (b) The command shall, as soon as practicable after an
 4-8 emergency purchase is made under this section:

4-9 (1) provide written notice to the Legislative Budget
 4-10 Board and the governor describing the nature of the emergency, the
 4-11 purchase made, and the vendor selected;

4-12 (2) ensure that documentation of the purchase,
 4-13 including the justification for bypassing standard procedures and
 4-14 the terms of the contract, is maintained and made available for
 4-15 post-incident audit; and

4-16 (3) submit a report to the State Auditor's Office not
 4-17 later than the 90th day after the date of the purchase describing:

4-18 (A) the necessity for making the purchase;

4-19 (B) the cost and duration of the contract; and

4-20 (C) any competitive processes used, if
 4-21 applicable.

4-22 Sec. 2063.008. PURCHASING OF CYBERSECURITY RESOURCES BY
 4-23 GOVERNMENTAL ENTITIES. (a) The command may not require, including
 4-24 by rule, governmental entities to purchase specific cybersecurity
 4-25 systems or resources.

4-26 (b) The command may adopt guidelines designating the
 4-27 purchasing method that attains the best value for the state for
 4-28 cybersecurity systems and resources.

4-29 Sec. 2063.009. RULES. The chief, with advice from the
 4-30 department, may adopt rules necessary for carrying out the purposes
 4-31 of this chapter.

4-32 Sec. 2063.010. APPLICATION OF SUNSET ACT. The command is
 4-33 subject to Chapter 325 (Texas Sunset Act). Unless continued in
 4-34 existence as provided by that chapter, the command is abolished
 4-35 September 1, 2031.

4-36 Sec. 2063.011. LAWS NOT AFFECTED. (a) Except as
 4-37 specifically provided by this chapter, this chapter does not affect
 4-38 laws, rules, or decisions relating to the confidentiality or
 4-39 privileged status of categories of information or communications.

4-40 (b) This chapter does not enlarge the right of state
 4-41 government to require information, records, or communications from
 4-42 the people.

4-43 SUBCHAPTER B. MINIMUM STANDARDS AND TRAINING

4-44 Sec. 2063.101. BEST PRACTICES AND MINIMUM STANDARDS FOR
 4-45 CYBERSECURITY AND TRAINING. (a) The command shall develop and
 4-46 annually assess best practices and minimum standards for use by
 4-47 governmental entities to enhance the security of information
 4-48 resources in this state.

4-49 (b) The command shall establish and periodically assess
 4-50 mandatory cybersecurity training that must be completed by all
 4-51 information resources employees of state agencies. The command
 4-52 shall consult with the Information Technology Council for Higher
 4-53 Education established under Section [2054.121](#) regarding applying
 4-54 the training requirements to employees of institutions of higher
 4-55 education.

4-56 (c) Except as otherwise provided by this subsection, the
 4-57 command shall adopt policies to ensure governmental entities are
 4-58 complying with the requirements of this section. The command shall
 4-59 adopt policies that ensure that a person who is not a citizen of the
 4-60 United States may not be a member, employee, contractor, volunteer,
 4-61 or otherwise affiliated with the command or any entity or
 4-62 organization established or operated by the command under this
 4-63 chapter.

4-64 SUBCHAPTER C. CYBERSECURITY PREVENTION, RESPONSE, AND RECOVERY

4-65 Sec. 2063.201. CYBERSECURITY THREAT INTELLIGENCE CENTER.
 4-66 (a) In this section, "center" means the cybersecurity threat
 4-67 intelligence center established under this section.

4-68 (b) The command shall establish a cybersecurity threat
 4-69 intelligence center. The center shall collaborate with federal

5-1 cybersecurity intelligence and law enforcement agencies to achieve
 5-2 the purposes of this section.

5-3 (c) The center, in coordination with the digital forensics
 5-4 laboratory under Section 2063.203, shall:

5-5 (1) operate the information sharing and analysis
 5-6 organization established under Section 2063.204; and

5-7 (2) provide strategic guidance to regional security
 5-8 operations centers established under Subchapter G and the
 5-9 cybersecurity incident response unit under Section 2063.202 to
 5-10 assist governmental entities in responding to a cybersecurity
 5-11 incident.

5-12 (d) The chief shall employ a director for the center.

5-13 Sec. 2063.202. CYBERSECURITY INCIDENT RESPONSE UNIT. (a)
 5-14 The command shall establish a dedicated cybersecurity incident
 5-15 response unit to:

5-16 (1) detect and contain cybersecurity incidents in
 5-17 collaboration with the cybersecurity threat intelligence center
 5-18 under Section 2063.201;

5-19 (2) engage in threat neutralization as necessary and
 5-20 appropriate, including removing malware, disallowing unauthorized
 5-21 access, and patching vulnerabilities in information resources
 5-22 technologies;

5-23 (3) in collaboration with the digital forensics
 5-24 laboratory under Section 2063.203, undertake mitigation efforts if
 5-25 sensitive personal information is breached during a cybersecurity
 5-26 incident;

5-27 (4) loan resources to state agencies and covered
 5-28 entities to promote continuity of operations while the agency or
 5-29 entity restores the systems affected by a cybersecurity incident;

5-30 (5) assist in the restoration of information resources
 5-31 and information resources technologies after a cybersecurity
 5-32 incident and conduct post-incident monitoring;

5-33 (6) in collaboration with the cybersecurity threat
 5-34 intelligence center under Section 2063.201 and digital forensics
 5-35 laboratory under Section 2063.203, identify weaknesses, establish
 5-36 risk mitigation options and effective vulnerability-reduction
 5-37 strategies, and make recommendations to state agencies and covered
 5-38 entities that have been the target of a cybersecurity attack or have
 5-39 experienced a cybersecurity incident in order to remediate
 5-40 identified cybersecurity vulnerabilities;

5-41 (7) in collaboration with the cybersecurity threat
 5-42 intelligence center under Section 2063.201, the digital forensics
 5-43 laboratory under Section 2063.203, the Texas Division of Emergency
 5-44 Management, and other state agencies, conduct, support, and
 5-45 participate in cyber-related exercises; and

5-46 (8) undertake any other activities necessary to carry
 5-47 out the duties described by this subsection.

5-48 (b) The chief shall employ a director for the cybersecurity
 5-49 incident response unit.

5-50 Sec. 2063.203. DIGITAL FORENSICS LABORATORY. (a) The
 5-51 command shall establish a digital forensics laboratory to:

5-52 (1) in collaboration with the cybersecurity incident
 5-53 response unit under Section 2063.202, develop procedures to:

5-54 (A) preserve evidence of a cybersecurity
 5-55 incident, including logs and communication;

5-56 (B) document chains of custody; and

5-57 (C) timely notify and maintain contact with the
 5-58 appropriate law enforcement agencies investigating a cybersecurity
 5-59 incident;

5-60 (2) develop and share with relevant state agencies and
 5-61 covered entities, subject to a contractual agreement, cyber threat
 5-62 hunting tools and procedures to assist in identifying indicators of
 5-63 a compromise in the cybersecurity of state information systems and
 5-64 non-state information systems, as appropriate;

5-65 (3) conduct analyses of causes of cybersecurity
 5-66 incidents and of remediation options;

5-67 (4) conduct assessments of the scope of harm caused by
 5-68 cybersecurity incidents, including data loss, compromised systems,
 5-69 and system disruptions;

6-1 (5) provide information and training to state agencies
6-2 and covered entities on producing reports required by regulatory
6-3 and auditing bodies;
6-4 (6) in collaboration with the Department of Public
6-5 Safety, the Texas Military Department, the office of the attorney
6-6 general, and other state agencies, provide forensic analysis of a
6-7 cybersecurity incident to support an investigation, attribution
6-8 process, or other law enforcement or judicial action; and
6-9 (7) undertake any other activities necessary to carry
6-10 out the duties described by this subsection.
6-11 (b) The chief shall employ a director for the digital
6-12 forensics laboratory.
6-13 Sec. 2063.205. POLICIES. The command shall adopt policies
6-14 and procedures necessary to enable the entities established in this
6-15 subchapter to carry out their respective duties and purposes.
6-16 SUBCHAPTER E. CYBERSECURITY PREPARATION AND PLANNING
6-17 Sec. 2063.404. ONGOING INFORMATION TRANSMISSIONS.
6-18 Information received from state agencies by the department under
6-19 Section 2054.069 shall be transmitted by the department to the
6-20 command on an ongoing basis.
6-21 Sec. 2063.409. INFORMATION SECURITY ASSESSMENT AND
6-22 PENETRATION TEST REQUIRED. (a) This section does not apply to a
6-23 university system or institution of higher education as defined by
6-24 Section 61.003, Education Code.
6-25 (b) At least once every two years, the command shall require
6-26 each state agency to complete an information security assessment
6-27 and a penetration test to be performed by the command or, at the
6-28 command's discretion, a vendor selected by the command.
6-29 (c) The chief shall adopt rules as necessary to implement
6-30 this section, including rules for the procurement of a vendor under
6-31 Subsection (b).
6-32 SECTION 2. Section 2054.510, Government Code, is
6-33 transferred to Subchapter A, Chapter 2063, Government Code, as
6-34 added by this Act, redesignated as Section 2063.0025, Government
6-35 Code, and amended to read as follows:
6-36 Sec. 2063.0025 [2054.510]. COMMAND CHIEF [INFORMATION
6-37 SECURITY OFFICER]. (a) In this section, "state cybersecurity
6-38 [information security] program" means the policies, standards,
6-39 procedures, elements, structure, strategies, objectives, plans,
6-40 metrics, reports, services, and resources that establish the
6-41 cybersecurity [information resources security] function for this
6-42 state.
6-43 (b) The chief directs the day-to-day operations and
6-44 policies of the command and oversees and is responsible for all
6-45 functions and duties of the command. [The executive director,
6-46 using existing funds, shall employ a chief information security
6-47 officer.]
6-48 (c) The chief [information security officer] shall oversee
6-49 cybersecurity matters for this state including:
6-50 (1) implementing the duties described by Section
6-51 2063.004 [2054.059];
6-52 (2) [responding to reports received under Section
6-53 2054.1125,
6-54 ~~[(3)]~~ developing a statewide cybersecurity
6-55 [information security] framework;
6-56 (3) ~~[(4)]~~ overseeing the development of cybersecurity
6-57 [statewide information security] policies and standards;
6-58 (4) ~~[(5)]~~ collaborating with [state agencies, local]
6-59 governmental entities[7] and other entities operating or
6-60 exercising control over state information systems or
6-61 state-controlled data critical to strengthen this state's
6-62 cybersecurity and information security policies, standards, and
6-63 guidelines;
6-64 (5) ~~[(6)]~~ overseeing the implementation of the
6-65 policies, standards, and requirements [guidelines] developed under
6-66 this chapter [Subdivisions (3) and (4)];
6-67 (6) ~~[(7)]~~ providing cybersecurity [information
6-68 security] leadership, strategic direction, and coordination for
6-69 the state cybersecurity [information security] program;

7-1 (7) ~~[(8)]~~ providing strategic direction to:
7-2 (A) the network security center established
7-3 under Section 2059.101; and

7-4 (B) regional security operations ~~[statewide~~
7-5 ~~technology]~~ centers operated under Subchapter G ~~[H]~~; and

7-6 (8) ~~[(9)]~~ overseeing the preparation and submission
7-7 of the report described by Section 2063.301 ~~[2054.0591]~~.

7-8 SECTION 3. Section 2054.0592, Government Code, is
7-9 transferred to Subchapter A, Chapter 2063, Government Code, as
7-10 added by this Act, redesignated as Section 2063.006, Government
7-11 Code, and amended to read as follows:

7-12 Sec. 2063.006 ~~[2054.0592]~~. CYBERSECURITY EMERGENCY
7-13 FUNDING. If a cybersecurity incident ~~[event]~~ creates a need for
7-14 emergency funding, the command ~~[department]~~ may request that the
7-15 governor or Legislative Budget Board make a proposal under Chapter
7-16 317 to provide funding to manage the operational and financial
7-17 impacts from the cybersecurity incident ~~[event]~~.

7-18 SECTION 4. Section 2054.519, Government Code, is
7-19 transferred to Subchapter B, Chapter 2063, Government Code, as
7-20 added by this Act, redesignated as Section 2063.102, Government
7-21 Code, and amended to read as follows:

7-22 Sec. 2063.102 ~~[2054.519]~~. STATE CERTIFIED CYBERSECURITY
7-23 TRAINING PROGRAMS. (a) The command ~~[department]~~, in consultation
7-24 with the cybersecurity council established under Section 2063.406
7-25 ~~[2054.512]~~ and industry stakeholders, shall annually:

7-26 (1) certify at least five cybersecurity training
7-27 programs for state and local government employees; and

7-28 (2) update standards for maintenance of certification
7-29 by the cybersecurity training programs under this section.

7-30 (b) To be certified under Subsection (a), a cybersecurity
7-31 training program must:

7-32 (1) focus on forming appropriate cybersecurity
7-33 ~~[information security]~~ habits and procedures that protect
7-34 information resources; and

7-35 (2) teach best practices and minimum standards
7-36 established under this subchapter ~~[for detecting, assessing,~~
7-37 ~~reporting, and addressing information security threats]~~.

7-38 (c) The command ~~[department]~~ may identify and certify under
7-39 Subsection (a) training programs provided by state agencies and
7-40 local governments that satisfy the training requirements described
7-41 by Subsection (b).

7-42 (d) The command ~~[department]~~ may contract with an
7-43 independent third party to certify cybersecurity training programs
7-44 under this section.

7-45 (e) The command ~~[department]~~ shall annually publish on the
7-46 command's ~~[department's]~~ Internet website the list of cybersecurity
7-47 training programs certified under this section.

7-48 SECTION 5. Section 2054.5191, Government Code, is
7-49 transferred to Subchapter B, Chapter 2063, Government Code, as
7-50 added by this Act, redesignated as Section 2063.103, Government
7-51 Code, and amended to read as follows:

7-52 Sec. 2063.103 ~~[2054.5191]~~. CYBERSECURITY TRAINING REQUIRED
7-53 ~~[. CERTAIN EMPLOYEES AND OFFICIALS]~~. (a) Each elected or appointed
7-54 official and employee of a governmental entity who has access to the
7-55 entity's information resources or information resources
7-56 technologies ~~[state agency shall identify state employees who use a~~
7-57 ~~computer to complete at least 25 percent of the employee's required~~
7-58 ~~duties. At least once each year, an employee identified by the~~
7-59 ~~state agency and each elected or appointed officer of the agency]~~
7-60 shall annually complete a cybersecurity training program certified
7-61 under Section 2063.102 ~~[2054.519]~~.

7-62 (b) ~~[(a-1) At least once each year, a local government~~
7-63 ~~shall:~~

7-64 ~~[(1) identify local government employees and elected~~
7-65 ~~and appointed officials who have access to a local government~~
7-66 ~~computer system or database and use a computer to perform at least~~
7-67 ~~25 percent of the employee's or official's required duties; and~~

7-68 ~~[(2) require the employees and officials identified~~
7-69 ~~under Subdivision (1) to complete a cybersecurity training program~~

8-1 ~~certified under Section 2054.519.~~

8-2 ~~[(a-2)]~~ The governing body of a governmental entity [~~local~~
8-3 ~~government]~~ or the governing body's designee may deny access to the
8-4 governmental entity's information resources or information
8-5 resources technologies [~~local government's computer system or~~
8-6 ~~database]~~ to an employee or official [~~individual described by~~
8-7 ~~Subsection (a-1)(1)]~~ who [~~the governing body or the governing~~
8-8 ~~body's designee determines]~~ is noncompliant with the requirements
8-9 of Subsection (a) [~~(a-1)(2)]~~.

8-10 (c) [~~(b)~~] The governing body of a local government may
8-11 select the most appropriate cybersecurity training program
8-12 certified under Section 2063.102 [~~2054.519~~] for employees and
8-13 officials of the local government to complete. The governing body
8-14 shall:

8-15 (1) verify and report on the completion of a
8-16 cybersecurity training program by employees and officials of the
8-17 local government to the command [~~department~~]; and

8-18 (2) require periodic audits to ensure compliance with
8-19 this section.

8-20 (d) [~~(c)~~] A state agency may select the most appropriate
8-21 cybersecurity training program certified under Section 2063.102
8-22 [~~2054.519~~] for employees and officials of the state agency. The
8-23 executive head of each state agency shall verify completion of a
8-24 cybersecurity training program by employees and officials of the
8-25 state agency in a manner specified by the command [~~department~~].

8-26 (e) [~~(d)~~] The executive head of each state agency shall
8-27 periodically require an internal review of the agency to ensure
8-28 compliance with this section.

8-29 (f) [~~(e)~~] The command [~~department~~] shall develop a form for
8-30 use by governmental entities [~~state agencies and local governments]~~
8-31 in verifying completion of cybersecurity training program
8-32 requirements under this section. The form must allow the state
8-33 agency and local government to indicate the percentage of employee
8-34 and official completion.

8-35 (g) [~~(f)~~] The requirements of Subsection [~~Subsections~~] (a)
8-36 [~~and (a-1)]~~ do not apply to employees and officials who have been:

8-37 (1) granted military leave;

8-38 (2) granted leave under the federal Family and Medical
8-39 Leave Act of 1993 (29 U.S.C. Section 2601 et seq.);

8-40 (3) granted leave related to a sickness or disability
8-41 covered by workers' compensation benefits, if that employee or
8-42 official no longer has access to the governmental entity's
8-43 information resources or information resources technologies [~~state~~
8-44 ~~agency's or local government's database and systems]~~;

8-45 (4) granted any other type of extended leave or
8-46 authorization to work from an alternative work site if that
8-47 employee or official no longer has access to the governmental
8-48 entity's information resources or information resources
8-49 technologies [~~state agency's or local government's database and~~
8-50 ~~systems]~~; or

8-51 (5) denied access to a governmental entity's
8-52 information resources or information resources technologies [~~local~~
8-53 ~~government's computer system or database by the governing body of~~
8-54 ~~the local government or the governing body's designee]~~ under
8-55 Subsection (b) [~~(a-2)]~~ for noncompliance with the requirements of
8-56 Subsection (a) [~~(a-1)(2)]~~.

8-57 SECTION 6. Section 2054.5192, Government Code, is
8-58 transferred to Subchapter B, Chapter 2063, Government Code, as
8-59 added by this Act, redesignated as Section 2063.104, Government
8-60 Code, and amended to read as follows:

8-61 Sec. 2063.104 [~~2054.5192~~]. CYBERSECURITY TRAINING
8-62 REQUIRED: CERTAIN STATE CONTRACTORS. (a) In this section,
8-63 "contractor" includes a subcontractor, officer, or employee of the
8-64 contractor.

8-65 (b) A state agency shall require any contractor who has
8-66 access to a state computer system or database to complete a
8-67 cybersecurity training program certified under Section 2063.102
8-68 [~~2054.519~~] as selected by the agency.

8-69 (c) The cybersecurity training program must be completed by

9-1 a contractor during the term of the contract and during any renewal
9-2 period.

9-3 (d) Required completion of a cybersecurity training program
9-4 must be included in the terms of a contract awarded by a state
9-5 agency to a contractor.

9-6 (e) A contractor required to complete a cybersecurity
9-7 training program under this section shall verify completion of the
9-8 program to the contracting state agency. The person who oversees
9-9 contract management for the agency shall:

9-10 (1) not later than August 31 of each year, report the
9-11 contractor's completion to the command [~~department~~]; and

9-12 (2) periodically review agency contracts to ensure
9-13 compliance with this section.

9-14 SECTION 7. Section 2054.0594, Government Code, is
9-15 transferred to Subchapter C, Chapter 2063, Government Code, as
9-16 added by this Act, redesignated as Section 2063.204, Government
9-17 Code, and amended to read as follows:

9-18 Sec. 2063.204 [2054.0594]. INFORMATION SHARING AND
9-19 ANALYSIS ORGANIZATION. (a) The command [~~department~~] shall
9-20 establish at least one [~~an~~] information sharing and analysis
9-21 organization to provide a forum for state agencies, local
9-22 governments, public and private institutions of higher education,
9-23 and the private sector to share information regarding cybersecurity
9-24 threats, best practices, and remediation strategies.

9-25 (b) [~~The department shall provide administrative support to~~
9-26 ~~the information sharing and analysis organization.~~

9-27 [~~(c)~~] A participant in the information sharing and analysis
9-28 organization shall assert any exception available under state or
9-29 federal law, including Section 552.139, in response to a request
9-30 for public disclosure of information shared through the
9-31 organization. Section 552.007 does not apply to information
9-32 described by this subsection.

9-33 (c) [~~(d)~~] The command [~~department~~] shall establish a
9-34 framework for regional cybersecurity task forces [~~working groups~~]
9-35 to execute mutual aid agreements that allow state agencies, local
9-36 governments, regional planning commissions, public and private
9-37 institutions of higher education, the private sector, the regional
9-38 security operations centers under Subchapter G, and the
9-39 cybersecurity incident response unit under Section 2063.202 [~~and~~
9-40 ~~the incident response team established under Subchapter N-2~~] to
9-41 assist with responding to a cybersecurity incident [~~event~~] in this
9-42 state. A task force [~~working group~~] may be established within the
9-43 geographic area of a regional planning commission established under
9-44 Chapter 391, Local Government Code. The task force [~~working group~~]
9-45 may establish a list of available cybersecurity experts and share
9-46 resources to assist in responding to the cybersecurity incident
9-47 [~~event~~] and recovery from the incident [~~event~~].

9-48 SECTION 8. Chapter 2063, Government Code, as added by this
9-49 Act, is amended by adding Subchapter D, and a heading is added to
9-50 that subchapter to read as follows:

9-51 SUBCHAPTER D. REPORTING

9-52 SECTION 9. Sections 2054.0591, 2054.603, and 2054.077,
9-53 Government Code, are transferred to Subchapter D, Chapter 2063,
9-54 Government Code, as added by this Act, redesignated as Sections
9-55 2063.301, 2063.302, and 2063.303, Government Code, respectively,
9-56 and amended to read as follows:

9-57 Sec. 2063.301 [2054.0591]. CYBERSECURITY REPORT. (a) Not
9-58 later than November 15 of each even-numbered year, the command
9-59 [~~department~~] shall submit to the governor, the lieutenant governor,
9-60 the speaker of the house of representatives, and the standing
9-61 committee of each house of the legislature with primary
9-62 jurisdiction over state government operations a report identifying
9-63 preventive and recovery efforts the state can undertake to improve
9-64 cybersecurity in this state. The report must include:

9-65 (1) an assessment of the resources available to
9-66 address the operational and financial impacts of a cybersecurity
9-67 incident [~~event~~];

9-68 (2) a review of existing statutes regarding
9-69 cybersecurity and information resources technologies; and

10-1 (3) recommendations for legislative action to
 10-2 increase the state's cybersecurity and protect against adverse
 10-3 impacts from a cybersecurity incident ~~[event, and~~

10-4 ~~[(4) an evaluation of a program that provides an~~
 10-5 ~~information security officer to assist small state agencies and~~
 10-6 ~~local governments that are unable to justify hiring a full-time~~
 10-7 ~~information security officer].~~

10-8 (b) Not later than October 1 of each even-numbered year, the
 10-9 command shall submit a report to the Legislative Budget Board that
 10-10 prioritizes, for the purpose of receiving funding, state agency
 10-11 cybersecurity projects. Each state agency shall coordinate with the
 10-12 command to implement this subsection.

10-13 (c) ~~[(b)]~~ The command ~~[department]~~ or a recipient of a
 10-14 report under this section may redact or withhold information
 10-15 confidential under Chapter 552, including Section 552.139, or other
 10-16 state or federal law that is contained in the report in response to
 10-17 a request under Chapter 552 without the necessity of requesting a
 10-18 decision from the attorney general under Subchapter G, Chapter 552.
 10-19 The disclosure of information under this section is not a voluntary
 10-20 disclosure for purposes of Section 552.007.

10-21 Sec. 2063.302 ~~[2054.603]~~. CYBERSECURITY ~~[SECURITY]~~
 10-22 INCIDENT NOTIFICATION BY STATE AGENCY OR LOCAL GOVERNMENT. (a) ~~[In~~
 10-23 ~~this section.~~

10-24 ~~[(1) "Security incident" means:~~
 10-25 ~~[(A) a breach or suspected breach of system~~
 10-26 ~~security as defined by Section 521.053, Business & Commerce Code,~~
 10-27 ~~and~~

10-28 ~~[(B) the introduction of ransomware, as defined~~
 10-29 ~~by Section 33.023, Penal Code, into a computer, computer network,~~
 10-30 ~~or computer system.~~

10-31 ~~[(2) "Sensitive personal information" has the meaning~~
 10-32 ~~assigned by Section 521.002, Business & Commerce Code.~~

10-33 ~~[(b)]~~ A state agency or local government that owns,
 10-34 licenses, or maintains computerized data that includes sensitive
 10-35 personal information, confidential information, or information the
 10-36 disclosure of which is regulated by law shall, in the event of a
 10-37 cybersecurity ~~[security]~~ incident:

10-38 (1) comply with the notification requirements of
 10-39 Section 521.053, Business & Commerce Code, to the same extent as a
 10-40 person who conducts business in this state;

10-41 (2) not later than 48 hours after the discovery of the
 10-42 cybersecurity ~~[security]~~ incident, notify:

10-43 (A) the command ~~[department]~~, including the
 10-44 chief ~~[information security officer]~~; or

10-45 (B) if the cybersecurity ~~[security]~~ incident
 10-46 involves election data, the secretary of state; and

10-47 (3) comply with all command ~~[department]~~ rules
 10-48 relating to reporting cybersecurity ~~[security]~~ incidents as
 10-49 required by this section.

10-50 (b) ~~[(c)]~~ Not later than the 10th business day after the
 10-51 date of the eradication, closure, and recovery from a cybersecurity
 10-52 ~~[security]~~ incident, a state agency or local government shall
 10-53 notify the command ~~[department]~~, including the chief ~~[information~~
 10-54 ~~security officer]~~, of the details of the cybersecurity ~~[security]~~
 10-55 incident and include in the notification an analysis of the cause of
 10-56 the cybersecurity ~~[security]~~ incident.

10-57 (c) ~~[(d)]~~ This section does not apply to a cybersecurity
 10-58 ~~[security]~~ incident that a local government is required to report
 10-59 to an independent organization certified by the Public Utility
 10-60 Commission of Texas under Section 39.151, Utilities Code.

10-61 Sec. 2063.303 ~~[2054.077]~~. VULNERABILITY REPORTS. (a) In
 10-62 this section, a term defined by Section 33.01, Penal Code, has the
 10-63 meaning assigned by that section.

10-64 (b) The information security officer of a state agency shall
 10-65 prepare or have prepared a report, including an executive summary
 10-66 of the findings of the biennial report, not later than June 1 of
 10-67 each even-numbered year, assessing the extent to which a computer,
 10-68 a computer program, a computer network, a computer system, a
 10-69 printer, an interface to a computer system, including mobile and

11-1 peripheral devices, computer software, or data processing of the
 11-2 agency or of a contractor of the agency is vulnerable to
 11-3 unauthorized access or harm, including the extent to which the
 11-4 agency's or contractor's electronically stored information is
 11-5 vulnerable to alteration, damage, erasure, or inappropriate use.

11-6 (c) Except as provided by this section, a vulnerability
 11-7 report and any information or communication prepared or maintained
 11-8 for use in the preparation of a vulnerability report is
 11-9 confidential and is not subject to disclosure under Chapter 552.

11-10 (d) The information security officer shall provide an
 11-11 electronic copy of the vulnerability report on its completion to:

- 11-12 (1) the command [~~department~~];
- 11-13 (2) the state auditor;
- 11-14 (3) the agency's executive director;
- 11-15 (4) the agency's designated information resources
 11-16 manager; and

11-17 (5) any other information technology security
 11-18 oversight group specifically authorized by the legislature to
 11-19 receive the report.

11-20 (e) Separate from the executive summary described by
 11-21 Subsection (b), a state agency shall prepare a summary of the
 11-22 agency's vulnerability report that does not contain any information
 11-23 the release of which might compromise the security of the state
 11-24 agency's or state agency contractor's computers, computer programs,
 11-25 computer networks, computer systems, printers, interfaces to
 11-26 computer systems, including mobile and peripheral devices,
 11-27 computer software, data processing, or electronically stored
 11-28 information. [~~The summary is available to the public on request.~~]

11-29 SECTION 10. Section 2054.515, Government Code, as amended
 11-30 by Chapters 567 (S.B. 475) and 856 (S.B. 800), Acts of the 87th
 11-31 Legislature, Regular Session, 2021, is transferred to Subchapter D,
 11-32 Chapter 2063, Government Code, as added by this Act, redesignated
 11-33 as Section 2063.304, Government Code, reenacted, and amended to
 11-34 read as follows:

11-35 Sec. 2063.304 [~~2054.515~~]. AGENCY DATA GOVERNANCE
 11-36 [~~INFORMATION SECURITY~~] ASSESSMENT AND REPORT. (a) At least once
 11-37 every two years, each state agency shall conduct an [~~information~~
 11-38 ~~security~~] assessment of the agency's[+]

11-39 [~~(1) information resources systems, network systems,~~
 11-40 ~~digital data storage systems, digital data security measures, and~~
 11-41 ~~information resources vulnerabilities; and~~

11-42 [~~(2)~~] data governance program with participation from
 11-43 the agency's data management officer, if applicable, and in
 11-44 accordance with requirements established by command [~~department~~]
 11-45 rule.

11-46 (b) Not later than June 1 of each even-numbered year, each
 11-47 state agency shall report the results of the assessment conducted
 11-48 under Subsection (a) to:

- 11-49 (1) the command; and
- 11-50 (2) on request, the governor, the lieutenant governor,
 11-51 and the speaker of the house of representatives.

11-52 [~~(b) Not later than November 15 of each even-numbered year,~~
 11-53 ~~the agency shall report the results of the assessment to:~~

- 11-54 (1) the department; and
- 11-55 (2) on request, the governor, the lieutenant
 11-56 governor, and the speaker of the house of representatives.

11-57 [~~(b) Not later than December 1 of the year in which a state~~
 11-58 ~~agency conducts the assessment under Subsection (a) or the 60th day~~
 11-59 ~~after the date the agency completes the assessment, whichever~~
 11-60 ~~occurs first, the agency shall report the results of the assessment~~
 11-61 ~~to:~~

- 11-62 (1) the department; and
- 11-63 (2) on request, the governor, the lieutenant
 11-64 governor, and the speaker of the house of representatives.]

11-65 (c) The chief [~~department~~] by rule shall establish the
 11-66 requirements for the [~~information security~~] assessment and report
 11-67 required by this section.

11-68 (d) The report and all documentation related to the
 11-69 [~~information security~~] assessment and report are confidential and

12-1 not subject to disclosure under Chapter 552. The state agency or
 12-2 command [~~department~~] may redact or withhold the information as
 12-3 confidential under Chapter 552 without requesting a decision from
 12-4 the attorney general under Subchapter G, Chapter 552.

12-5 SECTION 11. Section 2054.136, Government Code, is
 12-6 transferred to Subchapter E, Chapter 2063, Government Code, as
 12-7 added by this Act, redesignated as Section 2063.401, Government
 12-8 Code, and amended to read as follows:

12-9 Sec. 2063.401 [~~2054.136~~]. DESIGNATED INFORMATION SECURITY
 12-10 OFFICER. Each state agency shall designate an information security
 12-11 officer who:

12-12 (1) reports to the agency's executive-level
 12-13 management;

12-14 (2) has authority over information security for the
 12-15 entire agency;

12-16 (3) possesses the training and experience required to
 12-17 ensure the agency complies with requirements and policies
 12-18 established by the command [~~perform the duties required by~~
 12-19 ~~department rules~~]; and

12-20 (4) to the extent feasible, has information security
 12-21 duties as the officer's primary duties.

12-22 SECTION 12. Section 2054.518, Government Code, is
 12-23 transferred to Subchapter E, Chapter 2063, Government Code, as
 12-24 added by this Act, redesignated as Section 2063.402, Government
 12-25 Code, and amended to read as follows:

12-26 Sec. 2063.402 [~~2054.518~~]. CYBERSECURITY RISKS AND
 12-27 INCIDENTS. (a) The command [~~department~~] shall develop a plan to
 12-28 address cybersecurity risks and incidents in this state. The
 12-29 command [~~department~~] may enter into an agreement with a national
 12-30 organization, including the National Cybersecurity Preparedness
 12-31 Consortium, to support the command's [~~department's~~] efforts in
 12-32 implementing the components of the plan for which the command
 12-33 [~~department~~] lacks resources to address internally. The agreement
 12-34 may include provisions for:

12-35 (1) providing technical assistance services to
 12-36 support preparedness for and response to cybersecurity risks and
 12-37 incidents;

12-38 (2) conducting cybersecurity simulation exercises for
 12-39 state agencies to encourage coordination in defending against and
 12-40 responding to cybersecurity risks and incidents;

12-41 (3) assisting state agencies in developing
 12-42 cybersecurity information-sharing programs to disseminate
 12-43 information related to cybersecurity risks and incidents; and

12-44 (4) incorporating cybersecurity risk and incident
 12-45 prevention and response methods into existing state emergency
 12-46 plans, including continuity of operation plans and incident
 12-47 response plans.

12-48 (b) In implementing the provisions of the agreement
 12-49 prescribed by Subsection (a), the command [~~department~~] shall seek
 12-50 to prevent unnecessary duplication of existing programs or efforts
 12-51 of the command [~~department~~] or another state agency.

12-52 (c) [~~(a)~~] The command [~~department~~] shall consult with
 12-53 institutions of higher education in this state when appropriate
 12-54 based on an institution's expertise in addressing specific
 12-55 cybersecurity risks and incidents.

12-56 SECTION 13. Section 2054.133, Government Code, is
 12-57 transferred to Subchapter E, Chapter 2063, Government Code, as
 12-58 added by this Act, redesignated as Section 2063.403, Government
 12-59 Code, and amended to read as follows:

12-60 Sec. 2063.403 [~~2054.133~~]. INFORMATION SECURITY PLAN. (a)
 12-61 Each state agency shall develop, and periodically update, an
 12-62 information security plan for protecting the security of the
 12-63 agency's information.

12-64 (b) In developing the plan, the state agency shall:

12-65 (1) consider any vulnerability report prepared under
 12-66 Section 2063.303 [~~2054.077~~] for the agency;

12-67 (2) incorporate the network security services
 12-68 provided by the department to the agency under Chapter 2059;

12-69 (3) identify and define the responsibilities of agency

13-1 staff who produce, access, use, or serve as custodians of the
13-2 agency's information;

13-3 (4) identify risk management and other measures taken
13-4 to protect the agency's information from unauthorized access,
13-5 disclosure, modification, or destruction;

13-6 (5) include:

13-7 (A) the best practices for information security
13-8 developed by the command [~~department~~]; or

13-9 (B) if best practices are not applied, a written
13-10 explanation of why the best practices are not sufficient for the
13-11 agency's security; and

13-12 (6) omit from any written copies of the plan
13-13 information that could expose vulnerabilities in the agency's
13-14 network or online systems.

13-15 (c) Not later than June 1 of each even-numbered year, each
13-16 state agency shall submit a copy of the agency's information
13-17 security plan to the command [~~department~~]. Subject to available
13-18 resources, the command [~~department~~] may select a portion of the
13-19 submitted security plans to be assessed by the command [~~department~~]
13-20 in accordance with command policies [~~department rules~~].

13-21 (d) Each state agency's information security plan is
13-22 confidential and exempt from disclosure under Chapter 552.

13-23 (e) Each state agency shall include in the agency's
13-24 information security plan a written document that is signed by the
13-25 head of the agency, the chief financial officer, and each executive
13-26 manager designated by the state agency and states that those
13-27 persons have been made aware of the risks revealed during the
13-28 preparation of the agency's information security plan.

13-29 (f) Not later than November 15 of each even-numbered year,
13-30 the command [~~department~~] shall submit a written report to the
13-31 governor, the lieutenant governor, the speaker of the house of
13-32 representatives, and each standing committee of the legislature
13-33 with primary jurisdiction over matters related to the command
13-34 [~~department~~] evaluating information security for this state's
13-35 information resources. In preparing the report, the command
13-36 [~~department~~] shall consider the information security plans
13-37 submitted by state agencies under this section, any vulnerability
13-38 reports submitted under Section 2063.303 [~~2054.077~~], and other
13-39 available information regarding the security of this state's
13-40 information resources. The command [~~department~~] shall omit from
13-41 any written copies of the report information that could expose
13-42 specific vulnerabilities [~~in the security of this state's~~
13-43 ~~information resources~~].

13-44 SECTION 14. Section 2054.516, Government Code, is
13-45 transferred to Subchapter E, Chapter 2063, Government Code, as
13-46 added by this Act, redesignated as Section 2063.405, Government
13-47 Code, and amended to read as follows:

13-48 Sec. 2063.405 [~~2054.516~~]. DATA SECURITY PLAN FOR ONLINE
13-49 AND MOBILE APPLICATIONS. (a) Each state agency implementing an
13-50 Internet website or mobile application that processes any sensitive
13-51 personal or personally identifiable information or confidential
13-52 information must:

13-53 (1) submit a biennial data security plan to the
13-54 command [~~department~~] not later than June 1 of each even-numbered
13-55 year to establish planned beta testing for the website or
13-56 application; and

13-57 (2) subject the website or application to a
13-58 vulnerability and penetration test and address any vulnerability
13-59 identified in the test.

13-60 (b) The command [~~department~~] shall review each data
13-61 security plan submitted under Subsection (a) and make any
13-62 recommendations for changes to the plan to the state agency as soon
13-63 as practicable after the command [~~department~~] reviews the plan.

13-64 SECTION 15. Section 2054.512, Government Code, is
13-65 transferred to Subchapter E, Chapter 2063, Government Code, as
13-66 added by this Act, redesignated as Section 2063.406, Government
13-67 Code, and amended to read as follows:

13-68 Sec. 2063.406 [~~2054.512~~]. CYBERSECURITY COUNCIL. (a) The
13-69 chief or the chief's designee [~~state cybersecurity coordinator~~]

14-1 shall ~~[establish and]~~ lead a cybersecurity council that includes
14-2 public and private sector leaders and cybersecurity practitioners
14-3 to collaborate on matters of cybersecurity concerning this state.

14-4 (b) The cybersecurity council must include:

14-5 (1) one member who is an employee of the office of the
14-6 governor;

14-7 (2) one member of the senate appointed by the
14-8 lieutenant governor;

14-9 (3) one member of the house of representatives
14-10 appointed by the speaker of the house of representatives;

14-11 (4) the director ~~[one member who is an employee]~~ of the
14-12 Elections Division of the Office of the Secretary of State; ~~[and]~~

14-13 (5) one member who is an employee of the department;
14-14 and

14-15 (6) additional members appointed by the chief ~~[state~~
14-16 ~~cybersecurity coordinator]~~, including representatives of
14-17 institutions of higher education and private sector leaders.

14-18 (c) Members of the cybersecurity council serve staggered
14-19 six-year terms, with as near as possible to one-third of the
14-20 members' terms expiring February 1 of each odd-numbered year.

14-21 (d) In appointing representatives from institutions of
14-22 higher education to the cybersecurity council, the chief ~~[state~~
14-23 ~~cybersecurity coordinator]~~ shall consider appointing members of
14-24 the Information Technology Council for Higher Education.

14-25 (e) ~~[(d)]~~ The cybersecurity council shall:

14-26 (1) consider the costs and benefits of establishing a
14-27 computer emergency readiness team to address cybersecurity
14-28 incidents ~~[cyber attacks]~~ occurring in this state during routine
14-29 and emergency situations;

14-30 (2) establish criteria and priorities for addressing
14-31 cybersecurity threats to critical state installations;

14-32 (3) consolidate and synthesize best practices to
14-33 assist state agencies in understanding and implementing
14-34 cybersecurity measures that are most beneficial to this state; and

14-35 (4) assess the knowledge, skills, and capabilities of
14-36 the existing information technology and cybersecurity workforce to
14-37 mitigate and respond to cyber threats and develop recommendations
14-38 for addressing immediate workforce deficiencies and ensuring a
14-39 long-term pool of qualified applicants.

14-40 (f) ~~[(e)]~~ The chief, in collaboration with the
14-41 cybersecurity council, shall provide recommendations to the
14-42 legislature on any legislation necessary to implement
14-43 cybersecurity best practices and remediation strategies for this
14-44 state.

14-45 SECTION 16. Section 2054.514, Government Code, is
14-46 transferred to Subchapter E, Chapter 2063, Government Code, as
14-47 added by this Act, redesignated as Section 2063.407, Government
14-48 Code, and amended to read as follows:

14-49 Sec. 2063.407 [2054.514]. RECOMMENDATIONS. The chief
14-50 ~~[state cybersecurity coordinator]~~ may implement any portion, or all
14-51 of the recommendations made by the cybersecurity council under
14-52 Section 2063.406 [Cybersecurity, Education, and Economic
14-53 Development Council under Subchapter N].

14-54 SECTION 17. Section 2054.0593, Government Code, is
14-55 transferred to Subchapter E, Chapter 2063, Government Code, as
14-56 added by this Act, redesignated as Section 2063.408, Government
14-57 Code, and amended to read as follows:

14-58 Sec. 2063.408 [2054.0593]. CLOUD COMPUTING STATE RISK AND
14-59 AUTHORIZATION MANAGEMENT PROGRAM. (a) In this section, "cloud
14-60 computing service" has the meaning assigned by Section 2157.007.

14-61 (b) The command ~~[department]~~ shall establish a state risk
14-62 and authorization management program to provide a standardized
14-63 approach for security assessment, authorization, and continuous
14-64 monitoring of cloud computing services that process the data of a
14-65 state agency. The program must allow a vendor to demonstrate
14-66 compliance by submitting documentation that shows the vendor's
14-67 compliance with a risk and authorization management program of:

14-68 (1) the federal government; or

14-69 (2) another state that the command ~~[department]~~

15-1 approves.

15-2 (c) The command [~~department~~] by rule shall prescribe:

15-3 (1) the categories and characteristics of cloud
15-4 computing services subject to the state risk and authorization
15-5 management program; and

15-6 (2) the requirements for certification through the
15-7 program of vendors that provide cloud computing services.

15-8 (d) A state agency shall require each vendor contracting
15-9 with the agency to provide cloud computing services for the agency
15-10 to comply with the requirements of the state risk and authorization
15-11 management program. The command [~~department~~] shall evaluate
15-12 vendors to determine whether a vendor qualifies for a certification
15-13 issued by the department reflecting compliance with program
15-14 requirements.

15-15 (e) A state agency may not enter or renew a contract with a
15-16 vendor to purchase cloud computing services for the agency that are
15-17 subject to the state risk and authorization management program
15-18 unless the vendor demonstrates compliance with program
15-19 requirements.

15-20 (f) A state agency shall require a vendor contracting with
15-21 the agency to provide cloud computing services for the agency that
15-22 are subject to the state risk and authorization management program
15-23 to maintain program compliance and certification throughout the
15-24 term of the contract.

15-25 SECTION 18. Subchapter N-2, Chapter 2054, Government Code,
15-26 is transferred to Chapter 2063, Government Code, as added by this
15-27 Act, redesignated as Subchapter F, Chapter 2063, Government Code,
15-28 and amended to read as follows:

15-29 SUBCHAPTER F [~~N-2~~]. TEXAS VOLUNTEER INCIDENT RESPONSE TEAM

15-30 Sec. 2063.501 [~~2054.52001~~]. DEFINITIONS. In this
15-31 subchapter:

15-32 (1) "Incident response team" means the Texas volunteer
15-33 incident response team established under Section 2063.502
15-34 [~~2054.52002~~].

15-35 (2) "Participating entity" means a state agency,
15-36 including an institution of higher education, or a local government
15-37 that receives assistance under this subchapter during a
15-38 cybersecurity incident [~~event~~].

15-39 (3) "Volunteer" means an individual who provides rapid
15-40 response assistance during a cybersecurity incident [~~event~~] under
15-41 this subchapter.

15-42 Sec. 2063.502 [~~2054.52002~~]. ESTABLISHMENT OF TEXAS
15-43 VOLUNTEER INCIDENT RESPONSE TEAM. (a) The command [~~department~~]
15-44 shall establish the Texas volunteer incident response team to
15-45 provide rapid response assistance to a participating entity under
15-46 the command's [~~department's~~] direction during a cybersecurity
15-47 incident [~~event~~].

15-48 (b) The command [~~department~~] shall prescribe eligibility
15-49 criteria for participation as a volunteer member of the incident
15-50 response team, including a requirement that each volunteer have
15-51 expertise in addressing cybersecurity incidents [~~events~~].

15-52 Sec. 2063.503 [~~2054.52003~~]. CONTRACT WITH VOLUNTEERS. The
15-53 command [~~department~~] shall enter into a contract with each
15-54 volunteer the command [~~department~~] approves to provide rapid
15-55 response assistance under this subchapter. The contract must
15-56 require the volunteer to:

15-57 (1) acknowledge the confidentiality of information
15-58 required by Section 2063.510 [~~2054.52010~~];

15-59 (2) protect all confidential information from
15-60 disclosure;

15-61 (3) avoid conflicts of interest that might arise in a
15-62 deployment under this subchapter;

15-63 (4) comply with command [~~department~~] security
15-64 policies and procedures regarding information resources
15-65 technologies;

15-66 (5) consent to background screening required by the
15-67 command [~~department~~]; and

15-68 (6) attest to the volunteer's satisfaction of any
15-69 eligibility criteria established by the command [~~department~~].

16-1 Sec. 2063.504 [~~2054.52004~~]. VOLUNTEER QUALIFICATION. (a)
 16-2 The command [~~department~~] shall require criminal history record
 16-3 information for each individual who accepts an invitation to become
 16-4 a volunteer.

16-5 (b) The command [~~department~~] may request other information
 16-6 relevant to the individual's qualification and fitness to serve as
 16-7 a volunteer.

16-8 (c) The command [~~department~~] has sole discretion to
 16-9 determine whether an individual is qualified to serve as a
 16-10 volunteer.

16-11 Sec. 2063.505 [~~2054.52005~~]. DEPLOYMENT. (a) In response
 16-12 to a cybersecurity incident [~~event~~] that affects multiple
 16-13 participating entities or a declaration by the governor of a state
 16-14 of disaster caused by a cybersecurity event, the command
 16-15 [~~department~~] on request of a participating entity may deploy
 16-16 volunteers and provide rapid response assistance under the
 16-17 command's [~~department's~~] direction and the managed security
 16-18 services framework established under Section 2063.204(c)
 16-19 [~~2054.0594(d)~~] to assist with the incident [~~event~~].

16-20 (b) A volunteer may only accept a deployment under this
 16-21 subchapter in writing. A volunteer may decline to accept a
 16-22 deployment for any reason.

16-23 Sec. 2063.506 [~~2054.52006~~]. CYBERSECURITY COUNCIL
 16-24 DUTIES. The cybersecurity council established under Section
 16-25 2063.406 [~~2054.512~~] shall review and make recommendations to the
 16-26 command [~~department~~] regarding the policies and procedures used by
 16-27 the command [~~department~~] to implement this subchapter. The command
 16-28 [~~department~~] may consult with the council to implement and
 16-29 administer this subchapter.

16-30 Sec. 2063.507 [~~2054.52007~~]. COMMAND [~~DEPARTMENT~~] POWERS
 16-31 AND DUTIES. (a) The command [~~department~~] shall:

16-32 (1) approve the incident response tools the incident
 16-33 response team may use in responding to a cybersecurity incident
 16-34 [~~event~~];

16-35 (2) establish the eligibility criteria an individual
 16-36 must meet to become a volunteer;

16-37 (3) develop and publish guidelines for operation of
 16-38 the incident response team, including the:

16-39 (A) standards and procedures the command
 16-40 [~~department~~] uses to determine whether an individual is eligible to
 16-41 serve as a volunteer;

16-42 (B) process for an individual to apply for and
 16-43 accept incident response team membership;

16-44 (C) requirements for a participating entity to
 16-45 receive assistance from the incident response team; and

16-46 (D) process for a participating entity to request
 16-47 and obtain the assistance of the incident response team; and

16-48 (4) adopt rules necessary to implement this
 16-49 subchapter.

16-50 (b) The command [~~department~~] may require a participating
 16-51 entity to enter into a contract as a condition for obtaining
 16-52 assistance from the incident response team. [~~The contract must~~
 16-53 ~~comply with the requirements of Chapters 771 and 791.~~]

16-54 (c) The command [~~department~~] may provide appropriate
 16-55 training to prospective and approved volunteers.

16-56 (d) In accordance with state law, the command [~~department~~]
 16-57 may provide compensation for actual and necessary travel and living
 16-58 expenses incurred by a volunteer on a deployment using money
 16-59 available for that purpose.

16-60 (e) The command [~~department~~] may establish a fee schedule
 16-61 for participating entities receiving incident response team
 16-62 assistance. The amount of fees collected may not exceed the
 16-63 command's [~~department's~~] costs to operate the incident response
 16-64 team.

16-65 Sec. 2063.508 [~~2054.52008~~]. STATUS OF VOLUNTEER;
 16-66 LIABILITY. (a) A volunteer is not an agent, employee, or
 16-67 independent contractor of this state for any purpose and has no
 16-68 authority to obligate this state to a third party.

16-69 (b) This state is not liable to a volunteer for personal

17-1 injury or property damage sustained by the volunteer that arises
17-2 from participation in the incident response team.

17-3 Sec. 2063.509 [~~2054.52009~~]. CIVIL LIABILITY. A volunteer
17-4 who in good faith provides professional services in response to a
17-5 cybersecurity incident [~~event~~] is not liable for civil damages as a
17-6 result of the volunteer's acts or omissions in providing the
17-7 services, except for wilful and wanton misconduct. This immunity
17-8 is limited to services provided during the time of deployment for a
17-9 cybersecurity incident [~~event~~].

17-10 Sec. 2063.510 [~~2054.52010~~]. CONFIDENTIAL INFORMATION.
17-11 Information written, produced, collected, assembled, or maintained
17-12 by the command [~~department~~], a participating entity, the
17-13 cybersecurity council, or a volunteer in the implementation of this
17-14 subchapter is confidential and not subject to disclosure under
17-15 Chapter 552 if the information:

17-16 (1) contains the contact information for a volunteer;
17-17 (2) identifies or provides a means of identifying a
17-18 person who may, as a result of disclosure of the information, become
17-19 a victim of a cybersecurity incident [~~event~~];

17-20 (3) consists of a participating entity's cybersecurity
17-21 plans or cybersecurity-related practices; or

17-22 (4) is obtained from a participating entity or from a
17-23 participating entity's computer system in the course of providing
17-24 assistance under this subchapter.

17-25 SECTION 19. Subchapter E, Chapter 2059, Government Code, is
17-26 transferred to Chapter 2063, Government Code, as added by this Act,
17-27 redesignated as Subchapter G, Chapter 2063, Government Code, and
17-28 amended to read as follows:

17-29 SUBCHAPTER G [~~E~~]. REGIONAL [~~NETWORK~~] SECURITY OPERATIONS CENTERS

17-30 Sec. 2063.601 [~~2059.201~~]. ELIGIBLE PARTICIPATING ENTITIES.
17-31 A state agency or an entity listed in Section 2059.058 is eligible
17-32 to participate in cybersecurity support and network security
17-33 provided by a regional [~~network~~] security operations center under
17-34 this subchapter.

17-35 Sec. 2063.602 [~~2059.202~~]. ESTABLISHMENT OF REGIONAL
17-36 [~~NETWORK~~] SECURITY OPERATIONS CENTERS. (a) Subject to Subsection
17-37 (b), the command [~~department~~] may establish regional [~~network~~]
17-38 security operations centers, under the command's [~~department's~~]
17-39 managed security services framework established by Section
17-40 2063.204(c) [~~2054.0594(d)~~], to assist in providing cybersecurity
17-41 support and network security to regional offices or locations for
17-42 state agencies and other eligible entities that elect to
17-43 participate in and receive services through the center.

17-44 (b) The command [~~department~~] may establish more than one
17-45 regional [~~network~~] security operations center only if the command
17-46 [~~department~~] determines the first center established by the command
17-47 [~~department~~] successfully provides to state agencies and other
17-48 eligible entities the services the center has contracted to
17-49 provide.

17-50 (c) The command [~~department~~] shall enter into an
17-51 interagency contract in accordance with Chapter 771 or an
17-52 interlocal contract in accordance with Chapter 791, as appropriate,
17-53 with an eligible participating entity that elects to participate in
17-54 and receive services through a regional [~~network~~] security
17-55 operations center.

17-56 Sec. 2063.603 [~~2059.203~~]. REGIONAL [~~NETWORK~~] SECURITY
17-57 OPERATIONS CENTER LOCATIONS AND PHYSICAL SECURITY. (a) In
17-58 creating and operating a regional [~~network~~] security operations
17-59 center, the command may [~~department shall~~] partner with a
17-60 university system or institution of higher education as defined by
17-61 Section 61.003, Education Code, other than a public junior college.
17-62 The system or institution shall:

17-63 (1) serve as an education partner with the command
17-64 [~~department~~] for the regional [~~network~~] security operations
17-65 center; and

17-66 (2) enter into an interagency contract with the
17-67 command [~~department~~] in accordance with Chapter 771.

17-68 (b) In selecting the location for a regional [~~network~~]
17-69 security operations center, the command [~~department~~] shall select a

18-1 university system or institution of higher education that has
18-2 supportive educational capabilities.

18-3 (c) A university system or institution of higher education
18-4 selected to serve as a regional ~~[network]~~ security operations
18-5 center shall control and monitor all entrances to and critical
18-6 areas of the center to prevent unauthorized entry. The system or
18-7 institution shall restrict access to the center to only authorized
18-8 individuals.

18-9 (d) A local law enforcement entity or any entity providing
18-10 security for a regional ~~[network]~~ security operations center shall
18-11 monitor security alarms at the regional ~~[network]~~ security
18-12 operations center subject to the availability of that service.

18-13 (e) The ~~command [department]~~ and a university system or
18-14 institution of higher education selected to serve as a regional
18-15 ~~[network]~~ security operations center shall restrict operational
18-16 information to only center personnel, except as provided by Chapter
18-17 321.

18-18 Sec. 2063.604 [~~2059.204~~]. REGIONAL ~~[NETWORK]~~ SECURITY
18-19 OPERATIONS CENTERS SERVICES AND SUPPORT. The ~~command [department]~~
18-20 may offer the following managed security services through a
18-21 regional ~~[network]~~ security operations center:

18-22 (1) real-time ~~cybersecurity [network security]~~
18-23 monitoring to detect and respond to ~~cybersecurity incidents~~
18-24 ~~[network security events]~~ that may jeopardize this state and the
18-25 residents of this state;

18-26 (2) alerts and guidance for defeating ~~cybersecurity~~
18-27 ~~[network security]~~ threats, including firewall configuration,
18-28 installation, management, and monitoring, intelligence gathering,
18-29 and protocol analysis;

18-30 (3) immediate response to counter ~~unauthorized~~
18-31 ~~[network security]~~ activity that exposes this state and the
18-32 residents of this state to risk, including complete intrusion
18-33 detection system installation, management, and monitoring for
18-34 participating entities;

18-35 (4) development, coordination, and execution of
18-36 statewide ~~cybersecurity~~ operations to isolate, contain, and
18-37 mitigate the impact of ~~cybersecurity [network security]~~ incidents
18-38 for participating entities; and

18-39 (5) cybersecurity educational services.

18-40 Sec. 2063.605 [~~2059.205~~]. NETWORK SECURITY GUIDELINES AND
18-41 STANDARD OPERATING PROCEDURES. (a) The ~~command [department]~~ shall
18-42 adopt and provide to each regional ~~[network]~~ security operations
18-43 center appropriate network security guidelines and standard
18-44 operating procedures to ensure efficient operation of the center
18-45 with a maximum return on the state's investment.

18-46 (b) The ~~command [department]~~ shall revise the standard
18-47 operating procedures as necessary to confirm network security.

18-48 (c) Each eligible participating entity that elects to
18-49 participate in a regional ~~[network]~~ security operations center
18-50 shall comply with the network security guidelines and standard
18-51 operating procedures.

18-52 SECTION 20. Sections 11.175(c) and (h-1), Education Code,
18-53 are amended to read as follows:

18-54 (c) A school district's cybersecurity policy may not
18-55 conflict with the information security standards for institutions
18-56 of higher education adopted by the ~~Texas Cyber Command [Department~~
18-57 ~~of Information Resources]~~ under Chapters [~~2054 and~~] 2059 and 2063,
18-58 Government Code.

18-59 (h-1) Notwithstanding Section 2063.103 [~~2054.5191~~],
18-60 Government Code, only the district's cybersecurity coordinator is
18-61 required to complete the cybersecurity training under that section
18-62 on an annual basis. Any other school district employee required to
18-63 complete the cybersecurity training shall complete the training as
18-64 determined by the district, in consultation with the district's
18-65 cybersecurity coordinator.

18-66 SECTION 21. Section 38.307(e), Education Code, is amended
18-67 to read as follows:

18-68 (e) The agency shall maintain the data collected by the task
18-69 force and the work product of the task force in accordance with:

19-1 (1) the agency's information security plan under
19-2 Section 2063.403 [~~2054.133~~], Government Code; and

19-3 (2) the agency's records retention schedule under
19-4 Section 441.185, Government Code.

19-5 SECTION 22. Section 325.011, Government Code, is amended to
19-6 read as follows:

19-7 Sec. 325.011. CRITERIA FOR REVIEW. The commission and its
19-8 staff shall consider the following criteria in determining whether
19-9 a public need exists for the continuation of a state agency or its
19-10 advisory committees or for the performance of the functions of the
19-11 agency or its advisory committees:

19-12 (1) the efficiency and effectiveness with which the
19-13 agency or the advisory committee operates;

19-14 (2)(A) an identification of the mission, goals, and
19-15 objectives intended for the agency or advisory committee and of the
19-16 problem or need that the agency or advisory committee was intended
19-17 to address; and

19-18 (B) the extent to which the mission, goals, and
19-19 objectives have been achieved and the problem or need has been
19-20 addressed;

19-21 (3)(A) an identification of any activities of the
19-22 agency in addition to those granted by statute and of the authority
19-23 for those activities; and

19-24 (B) the extent to which those activities are
19-25 needed;

19-26 (4) an assessment of authority of the agency relating
19-27 to fees, inspections, enforcement, and penalties;

19-28 (5) whether less restrictive or alternative methods of
19-29 performing any function that the agency performs could adequately
19-30 protect or provide service to the public;

19-31 (6) the extent to which the jurisdiction of the agency
19-32 and the programs administered by the agency overlap or duplicate
19-33 those of other agencies, the extent to which the agency coordinates
19-34 with those agencies, and the extent to which the programs
19-35 administered by the agency can be consolidated with the programs of
19-36 other state agencies;

19-37 (7) the promptness and effectiveness with which the
19-38 agency addresses complaints concerning entities or other persons
19-39 affected by the agency, including an assessment of the agency's
19-40 administrative hearings process;

19-41 (8) an assessment of the agency's rulemaking process
19-42 and the extent to which the agency has encouraged participation by
19-43 the public in making its rules and decisions and the extent to which
19-44 the public participation has resulted in rules that benefit the
19-45 public;

19-46 (9) the extent to which the agency has complied with:

19-47 (A) federal and state laws and applicable rules
19-48 regarding equality of employment opportunity and the rights and
19-49 privacy of individuals; and

19-50 (B) state law and applicable rules of any state
19-51 agency regarding purchasing guidelines and programs for
19-52 historically underutilized businesses;

19-53 (10) the extent to which the agency issues and
19-54 enforces rules relating to potential conflicts of interest of its
19-55 employees;

19-56 (11) the extent to which the agency complies with
19-57 Chapters 551 and 552 and follows records management practices that
19-58 enable the agency to respond efficiently to requests for public
19-59 information;

19-60 (12) the effect of federal intervention or loss of
19-61 federal funds if the agency is abolished;

19-62 (13) the extent to which the purpose and effectiveness
19-63 of reporting requirements imposed on the agency justifies the
19-64 continuation of the requirement; and

19-65 (14) an assessment of the agency's cybersecurity
19-66 practices using confidential information available from the
19-67 Department of Information Resources, the Texas Cyber Command, or
19-68 any other appropriate state agency.

19-69 SECTION 23. Section 411.0765(b), Government Code, is

20-1 amended to read as follows:

- 20-2 (b) A criminal justice agency may disclose criminal history
 20-3 record information that is the subject of an order of nondisclosure
 20-4 of criminal history record information under this subchapter to the
 20-5 following noncriminal justice agencies or entities only:
 20-6 (1) the State Board for Educator Certification;
 20-7 (2) a school district, charter school, private school,
 20-8 regional education service center, commercial transportation
 20-9 company, or education shared services arrangement;
 20-10 (3) the Texas Medical Board;
 20-11 (4) the Texas School for the Blind and Visually
 20-12 Impaired;
 20-13 (5) the Board of Law Examiners;
 20-14 (6) the State Bar of Texas;
 20-15 (7) a district court regarding a petition for name
 20-16 change under Subchapter B, Chapter 45, Family Code;
 20-17 (8) the Texas School for the Deaf;
 20-18 (9) the Department of Family and Protective Services;
 20-19 (10) the Texas Juvenile Justice Department;
 20-20 (11) the Department of Assistive and Rehabilitative
 20-21 Services;
 20-22 (12) the Department of State Health Services, a local
 20-23 mental health service, a local intellectual and developmental
 20-24 disability authority, or a community center providing services to
 20-25 persons with mental illness or intellectual or developmental
 20-26 disabilities;
 20-27 (13) the Texas Private Security Board;
 20-28 (14) a municipal or volunteer fire department;
 20-29 (15) the Texas Board of Nursing;
 20-30 (16) a safe house providing shelter to children in
 20-31 harmful situations;
 20-32 (17) a public or nonprofit hospital or hospital
 20-33 district, or a facility as defined by Section 250.001, Health and
 20-34 Safety Code;
 20-35 (18) the securities commissioner, the banking
 20-36 commissioner, the savings and mortgage lending commissioner, the
 20-37 consumer credit commissioner, or the credit union commissioner;
 20-38 (19) the Texas State Board of Public Accountancy;
 20-39 (20) the Texas Department of Licensing and Regulation;
 20-40 (21) the Health and Human Services Commission;
 20-41 (22) the Department of Aging and Disability Services;
 20-42 (23) the Texas Education Agency;
 20-43 (24) the Judicial Branch Certification Commission;
 20-44 (25) a county clerk's office in relation to a
 20-45 proceeding for the appointment of a guardian under Title 3, Estates
 20-46 Code;
 20-47 (26) the Texas Cyber Command [~~Department of~~
 20-48 ~~Information Resources~~] but only regarding an employee, applicant
 20-49 for employment, contractor, subcontractor, intern, or volunteer
 20-50 who provides network security services under Chapter 2059 to:
 20-51 (A) the Texas Cyber Command [~~Department of~~
 20-52 ~~Information Resources~~]; or
 20-53 (B) a contractor or subcontractor of the Texas
 20-54 Cyber Command [~~Department of Information Resources~~];
 20-55 (27) the Texas Department of Insurance;
 20-56 (28) the Teacher Retirement System of Texas;
 20-57 (29) the Texas State Board of Pharmacy;
 20-58 (30) the Texas Civil Commitment Office;
 20-59 (31) a bank, savings bank, savings and loan
 20-60 association, credit union, or mortgage banker, a subsidiary or
 20-61 affiliate of those entities, or another financial institution
 20-62 regulated by a state regulatory entity listed in Subdivision (18)
 20-63 or by a corresponding federal regulatory entity, but only regarding
 20-64 an employee, contractor, subcontractor, intern, or volunteer of or
 20-65 an applicant for employment by that bank, savings bank, savings and
 20-66 loan association, credit union, mortgage banker, subsidiary or
 20-67 affiliate, or financial institution; and
 20-68 (32) an employer that has a facility that handles or
 20-69 has the capability of handling, transporting, storing, processing,

21-1 manufacturing, or controlling hazardous, explosive, combustible,
21-2 or flammable materials, if:

21-3 (A) the facility is critical infrastructure, as
21-4 defined by 42 U.S.C. Section 5195c(e), or the employer is required
21-5 to submit to a risk management plan under Section 112(r) of the
21-6 federal Clean Air Act (42 U.S.C. Section 7412) for the facility; and

21-7 (B) the information concerns an employee,
21-8 applicant for employment, contractor, or subcontractor whose
21-9 duties involve or will involve the handling, transporting, storing,
21-10 processing, manufacturing, or controlling hazardous, explosive,
21-11 combustible, or flammable materials and whose background is
21-12 required to be screened under a federal provision described by
21-13 Paragraph (A).

21-14 SECTION 24. Section 418.0195(a), Government Code, is
21-15 amended to read as follows:

21-16 (a) This section applies only to a computer network used by:

21-17 (1) a state agency; or

21-18 (2) an entity other than a state agency receiving
21-19 network security services from the Texas Cyber Command [~~Department~~
21-20 ~~of Information Resources~~] under Section 2059.058.

21-21 SECTION 25. Sections 772.012(b) and (c), Government Code,
21-22 are amended to read as follows:

21-23 (b) To apply for a grant under this chapter, a local
21-24 government must submit with the grant application a written
21-25 certification of the local government's compliance with the
21-26 cybersecurity training required by Section 2063.103 [~~2054.5191~~].

21-27 (c) On a determination by the criminal justice division
21-28 established under Section 772.006 that a local government awarded a
21-29 grant under this chapter has not complied with the cybersecurity
21-30 training required by Section 2063.103 [~~2054.5191~~], the local
21-31 government shall pay to this state an amount equal to the amount of
21-32 the grant award. A local government that is the subject of a
21-33 determination described by this subsection is ineligible for
21-34 another grant under this chapter until the second anniversary of
21-35 the date the local government is determined ineligible.

21-36 SECTION 26. Section 2054.380(b), Government Code, is
21-37 amended to read as follows:

21-38 (b) Revenue derived from the collection of fees imposed
21-39 under Subsection (a) may be appropriated to the department for:

21-40 (1) developing statewide information resources
21-41 technology policies and planning under this chapter [~~and Chapter~~
21-42 ~~2059~~]; and

21-43 (2) providing shared information resources technology
21-44 services under this chapter.

21-45 SECTION 27. Section 2054.0701(c), Government Code, is
21-46 amended to read as follows:

21-47 (c) A program offered under this section must:

21-48 (1) be approved by the Texas Higher Education
21-49 Coordinating Board in accordance with Section 61.0512, Education
21-50 Code;

21-51 (2) develop the knowledge and skills necessary for an
21-52 entry-level information technology position in a state agency; and

21-53 (3) include a one-year apprenticeship with:

21-54 (A) the department;

21-55 (B) another relevant state agency;

21-56 (C) an organization working on a major
21-57 information resources project; or

21-58 (D) a regional [~~network~~] security operations
21-59 center established under Section 2063.602 [~~2059.202~~].

21-60 SECTION 28. Section 2056.002(b), Government Code, is
21-61 amended to read as follows:

21-62 (b) The Legislative Budget Board and the governor's office
21-63 shall determine the elements required to be included in each
21-64 agency's strategic plan. Unless modified by the Legislative Budget
21-65 Board and the governor's office, and except as provided by
21-66 Subsection (c), a plan must include:

21-67 (1) a statement of the mission and goals of the state
21-68 agency;

21-69 (2) a description of the indicators developed under

22-1 this chapter and used to measure the output and outcome of the
22-2 agency;

22-3 (3) identification of the groups of people served by
22-4 the agency, including those having service priorities, or other
22-5 service measures established by law, and estimates of changes in
22-6 those groups expected during the term of the plan;

22-7 (4) an analysis of the use of the agency's resources to
22-8 meet the agency's needs, including future needs, and an estimate of
22-9 additional resources that may be necessary to meet future needs;

22-10 (5) an analysis of expected changes in the services
22-11 provided by the agency because of changes in state or federal law;

22-12 (6) a description of the means and strategies for
22-13 meeting the agency's needs, including future needs, and achieving
22-14 the goals established under Section 2056.006 for each area of state
22-15 government for which the agency provides services;

22-16 (7) a description of the capital improvement needs of
22-17 the agency during the term of the plan and a statement, if
22-18 appropriate, of the priority of those needs;

22-19 (8) identification of each geographic region of this
22-20 state, including the Texas-Louisiana border region and the
22-21 Texas-Mexico border region, served by the agency, and if
22-22 appropriate the agency's means and strategies for serving each
22-23 region;

22-24 (9) a description of the training of the agency's
22-25 contract managers under Section 656.052;

22-26 (10) an analysis of the agency's expected expenditures
22-27 that relate to federally owned or operated military installations
22-28 or facilities, or communities where a federally owned or operated
22-29 military installation or facility is located;

22-30 (11) an analysis of the strategic use of information
22-31 resources as provided by the instructions prepared under Section
22-32 2054.095;

22-33 (12) a written certification of the agency's
22-34 compliance with the cybersecurity training required under Sections
22-35 2063.103 [~~2054.5191~~] and 2063.104 [~~2054.5192~~]; and

22-36 (13) other information that may be required.

22-37 SECTION 29. Section 2059.001, Government Code, is amended
22-38 by adding Subdivision (1-a) to read as follows:

22-39 (1-a) "Command" means the Texas Cyber Command.

22-40 SECTION 30. Section 2059.051, Government Code, is amended
22-41 to read as follows:

22-42 Sec. 2059.051. COMMAND [~~DEPARTMENT~~] RESPONSIBLE FOR
22-43 PROVIDING COMPUTER NETWORK SECURITY SERVICES. The command
22-44 [~~department~~] shall provide network security services to:

22-45 (1) state agencies; and
22-46 (2) other entities by agreement as provided by Section
22-47 2059.058.

22-48 SECTION 31. Section 2059.052, Government Code, is amended
22-49 to read as follows:

22-50 Sec. 2059.052. SERVICES PROVIDED TO INSTITUTIONS OF HIGHER
22-51 EDUCATION. The command [~~department~~] may provide network security
22-52 services to an institution of higher education, and may include an
22-53 institution of higher education in a center, only if and to the
22-54 extent approved by the Information Technology Council for Higher
22-55 Education.

22-56 SECTION 32. Section 2059.053, Government Code, is amended
22-57 to read as follows:

22-58 Sec. 2059.053. RULES. The command [~~department~~] may adopt
22-59 rules necessary to implement this chapter.

22-60 SECTION 33. Section 2059.054, Government Code, is amended
22-61 to read as follows:

22-62 Sec. 2059.054. OWNERSHIP OR LEASE OF NECESSARY
22-63 EQUIPMENT. The command [~~department~~] may purchase in accordance
22-64 with Chapters 2155, 2156, 2157, and 2158 any facilities or
22-65 equipment necessary to provide network security services to state
22-66 agencies.

22-67 SECTION 34. Section 2059.055(a), Government Code, is
22-68 amended to read as follows:

22-69 (a) Confidential network security information may be

23-1 released only to officials responsible for the network, law
 23-2 enforcement, the state auditor's office, and agency or elected
 23-3 officials designated by the command [~~department~~].

23-4 SECTION 35. Section 2059.056, Government Code, is amended
 23-5 to read as follows:

23-6 Sec. 2059.056. RESPONSIBILITY FOR EXTERNAL AND INTERNAL
 23-7 SECURITY THREATS. If the command [~~department~~] provides network
 23-8 security services for a state agency or other entity under this
 23-9 chapter, the command [~~department~~] is responsible for network
 23-10 security from external threats for that agency or entity. Network
 23-11 security management for that state agency or entity regarding
 23-12 internal threats remains the responsibility of that state agency or
 23-13 entity.

23-14 SECTION 36. Section 2059.057, Government Code, is amended
 23-15 to read as follows:

23-16 Sec. 2059.057. BIENNIAL REPORT. (a) The command
 23-17 [~~department~~] shall biennially prepare a report on:

23-18 (1) the command's [~~department's~~] accomplishment of
 23-19 service objectives and other performance measures under this
 23-20 chapter; and

23-21 (2) the status, including the financial performance,
 23-22 of the consolidated network security system provided through the
 23-23 center.

23-24 (b) The command [~~department~~] shall submit the report to:

23-25 (1) the governor;

23-26 (2) the lieutenant governor;

23-27 (3) the speaker of the house of representatives; and

23-28 (4) the state auditor's office.

23-29 SECTION 37. Section 2059.058, Government Code, is amended
 23-30 to read as follows:

23-31 Sec. 2059.058. AGREEMENT TO PROVIDE NETWORK SECURITY
 23-32 SERVICES TO ENTITIES OTHER THAN STATE AGENCIES. In addition to the
 23-33 command's [~~department's~~] duty to provide network security services
 23-34 to state agencies under this chapter, the command [~~department~~] by
 23-35 agreement may provide network security services to:

23-36 (1) each house of the legislature and a legislative
 23-37 agency;

23-38 (2) a local government;

23-39 (3) the supreme court, the court of criminal appeals,
 23-40 or a court of appeals;

23-41 (4) a public hospital owned or operated by this state
 23-42 or a political subdivision or municipal corporation of this state,
 23-43 including a hospital district or hospital authority;

23-44 (5) the Texas Permanent School Fund Corporation;

23-45 (6) an open-enrollment charter school, as defined by
 23-46 Section 5.001, Education Code;

23-47 (7) a private school, as defined by Section 5.001,
 23-48 Education Code;

23-49 (8) a private or independent institution of higher
 23-50 education, as defined by Section 61.003, Education Code;

23-51 (9) a volunteer fire department, as defined by Section
 23-52 152.001, Tax Code; and

23-53 (10) an independent organization certified under
 23-54 Section 39.151, Utilities Code, for the ERCOT power region.

23-55 SECTION 38. Section 2059.101, Government Code, is amended
 23-56 to read as follows:

23-57 Sec. 2059.101. NETWORK SECURITY CENTER. The command
 23-58 [~~department~~] shall establish a network security center to provide
 23-59 network security services to state agencies.

23-60 SECTION 39. Sections 2059.102(a), (b), and (d), Government
 23-61 Code, are amended to read as follows:

23-62 (a) The command [~~department~~] shall manage the operation of
 23-63 network security system services for all state agencies at the
 23-64 center.

23-65 (b) The command [~~department~~] shall fulfill the network
 23-66 security requirements of each state agency to the extent
 23-67 practicable. However, the command [~~department~~] shall protect
 23-68 criminal justice and homeland security networks of this state to
 23-69 the fullest extent possible in accordance with federal criminal

24-1 justice and homeland security network standards.

24-2 (d) A state agency may not purchase network security
24-3 services unless the command [~~department~~] determines that the
24-4 agency's requirement for network security services cannot be met at
24-5 a comparable cost through the center. The command [~~department~~]
24-6 shall develop an efficient process for this determination.

24-7 SECTION 40. Sections 2059.103(a), (b), and (d), Government
24-8 Code, are amended to read as follows:

24-9 (a) The command [~~department~~] shall locate the center at a
24-10 location that has an existing secure and restricted facility,
24-11 cyber-security infrastructure, available trained workforce, and
24-12 supportive educational capabilities.

24-13 (b) The command [~~department~~] shall control and monitor all
24-14 entrances and critical areas to prevent unauthorized entry. The
24-15 command [~~department~~] shall limit access to authorized individuals.

24-16 (d) The command [~~department~~] shall restrict operational
24-17 information to personnel at the center, except as provided by
24-18 Chapter 321.

24-19 SECTION 41. Section 2059.104, Government Code, is amended
24-20 to read as follows:

24-21 Sec. 2059.104. CENTER SERVICES AND SUPPORT. (a) The
24-22 command [~~department~~] shall provide the following managed security
24-23 services through the center:

24-24 (1) real-time network security monitoring to detect
24-25 and respond to network security events that may jeopardize this
24-26 state and the residents of this state, including vulnerability
24-27 assessment services consisting of a comprehensive security posture
24-28 assessment, external and internal threat analysis, and penetration
24-29 testing;

24-30 (2) continuous, 24-hour alerts and guidance for
24-31 defeating network security threats, including firewall
24-32 preconfiguration, installation, management and monitoring,
24-33 intelligence gathering, protocol analysis, and user
24-34 authentication;

24-35 (3) immediate incident response to counter network
24-36 security activity that exposes this state and the residents of this
24-37 state to risk, including complete intrusion detection systems
24-38 installation, management, and monitoring and a network operations
24-39 call center;

24-40 (4) development, coordination, and execution of
24-41 statewide cyber-security operations to isolate, contain, and
24-42 mitigate the impact of network security incidents at state
24-43 agencies;

24-44 (5) operation of a central authority for all statewide
24-45 information assurance programs; and

24-46 (6) the provision of educational services regarding
24-47 network security.

24-48 (b) The command [~~department~~] may provide:

24-49 (1) implementation of best-of-breed information
24-50 security architecture engineering services, including public key
24-51 infrastructure development, design, engineering, custom software
24-52 development, and secure web design; or

24-53 (2) certification and accreditation to ensure
24-54 compliance with the applicable regulatory requirements for
24-55 cyber-security and information technology risk management,
24-56 including the use of proprietary tools to automate the assessment
24-57 and enforcement of compliance.

24-58 SECTION 42. Sections 2059.105(a) and (b), Government Code,
24-59 are amended to read as follows:

24-60 (a) The command [~~department~~] shall adopt and provide to all
24-61 state agencies appropriate network security guidelines and
24-62 standard operating procedures to ensure efficient operation of the
24-63 center with a maximum return on investment for the state.

24-64 (b) The command [~~department~~] shall revise the standard
24-65 operating procedures as necessary to confirm network security.

24-66 SECTION 43. Section 2059.1055, Government Code, is amended
24-67 to read as follows:

24-68 Sec. 2059.1055. NETWORK SECURITY IN A STATE OF DISASTER.
24-69 The command [~~department~~] shall disconnect the computer network of

25-1 an entity receiving security services under this chapter from the
 25-2 Internet if the governor issues an order under Section 418.0195 to
 25-3 disconnect the network because of a substantial external threat to
 25-4 the entity's computer network.

25-5 SECTION 44. Section 2059.106, Government Code, is amended
 25-6 to read as follows:

25-7 Sec. 2059.106. PRIVATE VENDOR. The command [~~department~~]
 25-8 may contract with a private vendor to build and operate the center
 25-9 and act as an authorized agent to acquire, install, integrate,
 25-10 maintain, configure, and monitor the network security services and
 25-11 security infrastructure elements.

25-12 SECTION 45. Section 2059.151, Government Code, is amended
 25-13 to read as follows:

25-14 Sec. 2059.151. PAYMENT FOR SERVICES. The department shall
 25-15 develop a system of billings and charges for services provided by
 25-16 the command in operating and administering the network security
 25-17 system that allocates the total state cost to each state agency or
 25-18 other entity served by the system based on proportionate usage.

25-19 SECTION 46. Section 2059.152, Government Code, is amended
 25-20 by adding Subsection (d) to read as follows:

25-21 (d) The department shall enter into an agreement with the
 25-22 command to transfer funds as necessary for the performance of
 25-23 functions under this chapter.

25-24 SECTION 47. Section 2059.153, Government Code, is amended
 25-25 to read as follows:

25-26 Sec. 2059.153. GRANTS. The command [~~department~~] may apply
 25-27 for and use for purposes of this chapter the proceeds from grants
 25-28 offered by any federal agency or other source.

25-29 SECTION 48. Section 2157.068(d), Government Code, is
 25-30 amended to read as follows:

25-31 (d) The department may charge a reasonable administrative
 25-32 fee to a state agency, local government, or governmental entity of
 25-33 another state that purchases commodity items through the department
 25-34 in an amount that is sufficient to recover costs associated with the
 25-35 administration of this section. Revenue derived from the
 25-36 collection of fees imposed under this subsection may be
 25-37 appropriated to the department for:

25-38 (1) developing statewide information resources
 25-39 technology policies and planning under Chapter [~~Chapters~~] 2054 [~~and~~
 25-40 ~~2059~~]; and

25-41 (2) providing shared information resources technology
 25-42 services under Chapter 2054.

25-43 SECTION 49. Section 2170.057(a), Government Code, is
 25-44 amended to read as follows:

25-45 (a) The department shall develop a system of billings and
 25-46 charges for services provided in operating and administering the
 25-47 consolidated telecommunications system that allocates the total
 25-48 state cost to each entity served by the system based on
 25-49 proportionate usage. The department shall set and charge a fee to
 25-50 each entity that receives services provided under this chapter in
 25-51 an amount sufficient to cover the direct and indirect costs of
 25-52 providing the service. Revenue derived from the collection of fees
 25-53 imposed under this subsection may be appropriated to the department
 25-54 for:

25-55 (1) developing statewide information resources
 25-56 technology policies and planning under Chapter [~~Chapters~~] 2054 [~~and~~
 25-57 ~~2059~~]; and

25-58 (2) providing[+
 25-59 [~~(A)~~] shared information resources technology
 25-60 services under Chapter 2054[+, and
 25-61 [~~(B)~~] network security services under Chapter
 25-62 2059].

25-63 SECTION 50. The following provisions of the Government Code
 25-64 are repealed:

- 25-65 (1) Section 2054.059;
- 25-66 (2) Section 2054.076(b-1);
- 25-67 (3) Section 2054.511; and
- 25-68 (4) Section 2054.5181.

25-69 SECTION 51. (a) In this section, "department" means the

26-1 Department of Information Resources.

26-2 (b) On the effective date of this Act, the Texas Cyber
26-3 Command, organized as provided by Section 2063.002, Government
26-4 Code, as added by this Act, is created with the powers and duties
26-5 assigned by Chapter 2063, Government Code, as added by this Act, and
26-6 Chapter 2059, Government Code, as amended by this Act.

26-7 (b-1) As soon as practicable on or after the effective date
26-8 of this Act, the governor shall appoint the chief of the Texas Cyber
26-9 Command, as described by Section 2063.0025, Government Code, as
26-10 added by this Act, to a term expiring February 1, 2027.

26-11 (c) Notwithstanding Subsection (b) of this section, the
26-12 department shall continue to perform duties and exercise powers
26-13 under Chapters 2054 and 2059, Government Code, as that law existed
26-14 immediately before the effective date of this Act, until the date
26-15 provided by the memorandum of understanding entered into under
26-16 Subsection (e) of this section.

26-17 (d) Not later than December 31, 2026:

26-18 (1) all functions and activities performed by the
26-19 department that relate to cybersecurity under Chapter 2063,
26-20 Government Code, as added by this Act, or network security under
26-21 Chapter 2059, Government Code, as amended by this Act, are
26-22 transferred to the Texas Cyber Command;

26-23 (2) all employees of the department who primarily
26-24 perform duties related to cybersecurity under Chapter 2063,
26-25 Government Code, as added by this Act, or network security under
26-26 Chapter 2059, Government Code, as amended by this Act, become
26-27 employees of the Texas Cyber Command, but continue to work in the
26-28 same physical location unless moved in accordance with the
26-29 memorandum of understanding entered into under Subsection (e) of
26-30 this section;

26-31 (3) a rule or form adopted by the department that
26-32 relates to cybersecurity under Chapter 2063, Government Code, as
26-33 added by this Act, or network security under Chapter 2059,
26-34 Government Code, as amended by this Act, is a rule or form of the
26-35 Texas Cyber Command and remains in effect until changed by the
26-36 command;

26-37 (4) a reference in law to the department that relates
26-38 to cybersecurity under Chapter 2063, Government Code, as added by
26-39 this Act, or network security under Chapter 2059, Government Code,
26-40 as amended by this Act, means the Texas Cyber Command;

26-41 (5) a contract negotiation for a contract specified as
26-42 provided by Subdivision (7) of this subsection in the memorandum of
26-43 understanding entered into under Subsection (e) of this section or
26-44 other proceeding involving the department that is related to
26-45 cybersecurity under Chapter 2063, Government Code, as added by this
26-46 Act, or network security under Chapter 2059, Government Code, as
26-47 amended by this Act, is transferred without change in status to the
26-48 Texas Cyber Command, and the Texas Cyber Command assumes, without a
26-49 change in status, the position of the department in a negotiation or
26-50 proceeding relating to cybersecurity or network security to which
26-51 the department is a party;

26-52 (6) all money, leases, rights, and obligations of the
26-53 department related to cybersecurity under Chapter 2063, Government
26-54 Code, as added by this Act, or network security under Chapter 2059,
26-55 Government Code, as amended by this Act, are transferred to the
26-56 Texas Cyber Command;

26-57 (7) contracts specified as necessary to accomplish the
26-58 goals and duties of the Texas Cyber Command, as established by
26-59 Chapter 2063, Government Code, as added by this Act, in the
26-60 memorandum of understanding entered into under Subsection (e) of
26-61 this section are transferred to the Texas Cyber Command;

26-62 (8) all property, including records, in the custody of
26-63 the department related to cybersecurity under Chapter 2063,
26-64 Government Code, as added by this Act, or network security under
26-65 Chapter 2059, Government Code, as amended by this Act, becomes
26-66 property of the Texas Cyber Command, but stays in the same physical
26-67 location unless moved in accordance with the specific steps and
26-68 methods created under Subsection (e) of this section; and

26-69 (9) all funds appropriated by the legislature to the

27-1 department for purposes related to cybersecurity under Chapter
27-2 2063, Government Code, as added by this Act, or network security
27-3 under Chapter 2059, Government Code, as amended by this Act, are
27-4 transferred to the Texas Cyber Command.

27-5 (e) Not later than January 1, 2026, the department and Texas
27-6 Cyber Command shall enter into a memorandum of understanding
27-7 relating to the transfer of powers and duties from the department to
27-8 the Texas Cyber Command as provided by this Act. The memorandum
27-9 must include:

27-10 (1) a timetable and specific steps and methods for the
27-11 transfer of all powers, duties, obligations, rights, contracts,
27-12 leases, records, real or personal property, and unspent and
27-13 unobligated appropriations and other funds relating to the
27-14 administration of the powers and duties as provided by this Act;

27-15 (2) measures to ensure against any unnecessary
27-16 disruption to cybersecurity or network security operations during
27-17 the transfer process; and

27-18 (3) a provision that the terms of any memorandum of
27-19 understanding entered into related to the transfer remain in effect
27-20 until the transfer is completed.

27-21 SECTION 52. This Act takes effect September 1, 2025.

* * * * *

27-22