

By: Capriglione

H.B. No. 150

A BILL TO BE ENTITLED

AN ACT

relating to the establishment of the Texas Cyber Command as a component institution of The University of Texas System and the transfer to it of certain powers and duties of the Department of Information Resources.

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

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

CHAPTER 2063. TEXAS CYBER COMMAND

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 2063.001. DEFINITIONS. In this chapter:

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

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

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

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

(A) chemical facilities;

(B) commercial facilities;

1 (C) communication facilities;
2 (D) manufacturing facilities;
3 (E) dams;
4 (F) defense industrial bases;
5 (G) emergency services systems;
6 (H) energy facilities;
7 (I) financial services systems;
8 (J) food and agriculture facilities;
9 (K) government facilities;
10 (L) health care and public health facilities;
11 (M) information technology and information
12 technology systems;
13 (N) nuclear reactors, materials, and waste;
14 (O) transportation systems; or
15 (P) water and wastewater systems.

16 (5) "Cybersecurity" means the measures taken to
17 protect a computer, computer network, computer system, or other
18 technology infrastructure against unauthorized:

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

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

23 (6) "Cybersecurity incident" includes:

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

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

computer system; or

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

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

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

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

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

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

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

(13) "State agency" means:

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

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

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

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

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

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

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

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

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

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

22 (1) developing tools to enhance cybersecurity
23 defenses;

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

26 (3) in collaboration with the department,
27 establishing appropriate cybersecurity standards; and

1 (4) creating partnerships needed to effectively carry
2 out the command's functions.

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

5 (1) promote public awareness of cybersecurity issues;

6 (2) develop cybersecurity best practices and minimum
7 standards for governmental entities;

8 (3) develop and provide training to state agencies and
9 covered entities on cybersecurity measures and awareness;

10 (4) administer the cybersecurity threat intelligence
11 center under Section 2063.201;

12 (5) provide support to state agencies and covered
13 entities experiencing a cybersecurity incident;

14 (6) administer the digital forensics laboratory under
15 Section 2063.203;

16 (7) administer a statewide portal for enterprise
17 cybersecurity threat, risk, and incident management, and operate a
18 cybersecurity hotline available for state agencies and covered
19 entities 24 hours a day, seven days a week;

20 (8) collaborate with law enforcement agencies to
21 provide training and support related to cybersecurity incidents;

22 (9) serve as a clearinghouse for information relating
23 to all aspects of protecting the cybersecurity of governmental
24 entities, including sharing appropriate intelligence and
25 information with governmental entities, federal agencies, and
26 covered entities;

27 (10) collaborate with the department to ensure

information resources and information resources technologies
obtained by the department meet the cybersecurity standards and
requirements established under this chapter;

(11) offer cybersecurity resources to state agencies
and covered entities as determined by the command; and

(12) adopt policies to ensure state agencies implement
sufficient cybersecurity measures to defend information resources,
information resources technologies, and sensitive personal
information maintained by the agencies.

(b) The command may:

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

(2) adopt and use an official seal;

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

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

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

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

(c) Except as otherwise provided by this chapter, the

command shall deposit money paid to the command under this chapter in the state treasury to the credit of the general revenue fund.

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

Sec. 2063.007. EMERGENCY PURCHASING. In the event the emergency response to a cybersecurity incident requires the command to purchase an item, the command is exempt from the requirements of Sections [2155.0755](#), [2155.083](#), and [2155.132\(c\)](#) in making the purchase.

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

Sec. 2063.009. APPLICATION OF SUNSET ACT. The command is subject to Chapter 325 (Texas Sunset Act). Unless continued in existence as provided by that chapter, the command is abolished September 1, 2035.

SUBCHAPTER B. MINIMUM STANDARDS AND TRAINING

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

(b) The command shall establish and periodically assess mandatory cybersecurity training that must be completed by all information resources employees of state agencies. The command shall consult with the Information Technology Council for Higher

1 Education established under Section 2054.121 regarding applying
2 the training requirements to employees of institutions of higher
3 education.

4 (c) The command shall adopt policies to ensure governmental
5 entities are complying with the requirements of this section.

6 SUBCHAPTER C. CYBERSECURITY PREVENTION, RESPONSE, AND RECOVERY

7 Sec. 2063.201. CYBERSECURITY THREAT INTELLIGENCE CENTER.

8 (a) In this section, "center" means the cybersecurity threat
9 intelligence center established under this section.

10 (b) The command shall establish a cybersecurity threat
11 intelligence center. The center, in coordination with the
12 department, shall:

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

15 (2) use regional security operations centers
16 established under Subchapter G and the cybersecurity incident
17 response unit under Section 2063.202 to assist governmental
18 entities in responding to a cybersecurity incident.

19 (c) The chief may employ a director for the center.

20 Sec. 2063.202. CYBERSECURITY INCIDENT RESPONSE UNIT. (a)
21 The command shall establish a dedicated cybersecurity incident
22 response unit to:

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

26 (2) engage in threat neutralization, including
27 removing malware, disallowing unauthorized access, and patching

1 vulnerabilities in information resources technologies;

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

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

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

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

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

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

27 (b) The chief shall employ a director for the cybersecurity

incident response unit.

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

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

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

(B) document chains of custody; and

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

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

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

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

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

(6) in collaboration with the Department of Public Safety, the Texas Military Department, the office of the attorney

1 general, and other state agencies, provide forensic analysis of a
2 cybersecurity incident to support an investigation, attribution
3 process, or other law enforcement or judicial action; and

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

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

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

11 SUBCHAPTER E. CYBERSECURITY PREPARATION AND PLANNING

12 Sec. 2063.404. ONGOING INFORMATION TRANSMISSIONS.
13 Information received from state agencies by the department under
14 Section 2054.069 shall be transmitted by the department to the
15 command on an ongoing basis.

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

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

27 (b) The chief directs the day-to-day operations and

1 policies of the command and oversees and is responsible for all
2 functions and duties of the command. [~~The executive director,~~
3 ~~using existing funds, shall employ a chief information security~~
4 ~~officer.~~]

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

7 (1) implementing the duties described by Section
8 2063.004 [2054.059];

9 (2) [~~responding to reports received under Section~~
10 ~~2054.1125,~~

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

13 (3) [~~(4)~~] overseeing the development of cybersecurity
14 [~~statewide information security~~] policies and standards;

15 (4) [~~(5)~~] collaborating with [~~state agencies, local~~]
16 governmental entities[7] and other entities operating or
17 exercising control over state information systems or
18 state-controlled data critical to strengthen this state's
19 cybersecurity and information security policies, standards, and
20 guidelines;

21 (5) [~~(6)~~] overseeing the implementation of the
22 policies, standards, and requirements [~~guidelines~~] developed under
23 this chapter [~~Subdivisions (3) and (4)~~];

24 (6) [~~(7)~~] providing cybersecurity [~~information~~
25 ~~security~~] leadership, strategic direction, and coordination for
26 the state cybersecurity [~~information security~~] program;

27 (7) [~~(8)~~] providing strategic direction to:

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

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

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

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

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

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

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

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

(2) update standards for maintenance of certification

1 by the cybersecurity training programs under this section.

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

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

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

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

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

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

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

24 Sec. 2063.103 ~~[2054.5191]~~. CYBERSECURITY TRAINING REQUIRED
25 ~~[+ CERTAIN EMPLOYEES AND OFFICIALS]~~. (a) Each elected or appointed
26 official and employee of a governmental entity who has access to the
27 entity's information resources or information resources

technologies ~~[state agency shall identify state employees who use a computer to complete at least 25 percent of the employee's required duties. At least once each year, an employee identified by the state agency and each elected or appointed officer of the agency]~~ shall annually complete a cybersecurity training program certified under Section 2063.102 ~~[2054.519]~~.

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

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

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

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

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

1 shall:

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

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

7 (d) ~~[(e)]~~ A state agency may select the most appropriate
8 cybersecurity training program certified under Section 2063.102
9 ~~[2054.519]~~ for employees and officials of the state agency. The
10 executive head of each state agency shall verify completion of a
11 cybersecurity training program by employees and officials of the
12 state agency in a manner specified by the command ~~[department]~~.

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

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

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

- 24 (1) granted military leave;
- 25 (2) granted leave under the federal Family and Medical
26 Leave Act of 1993 (29 U.S.C. Section 2601 et seq.);
- 27 (3) granted leave related to a sickness or disability

covered by workers' compensation benefits, if that employee or official no longer has access to the governmental entity's information resources or information resources technologies [~~state agency's or local government's database and systems~~];

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

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

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

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

(b) A state agency shall require any contractor who has access to a state computer system or database to complete a cybersecurity training program certified under Section 2063.102

1 [2054.519] as selected by the agency.

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

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

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

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

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

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

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

27 (b) [~~The department shall provide administrative support to~~

~~the information sharing and analysis organization.~~

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

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

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

SUBCHAPTER D. REPORTING

SECTION 9. Sections 2054.0591 and 2054.077, Government

Code, are transferred to Subchapter D, Chapter 2063, Government Code, as added by this Act, redesignated as Sections 2063.301 and 2063.302, Government Code, respectively, and amended to read as follows:

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

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

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

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

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

(b) Not later than October 1 of each even-numbered year, the command shall submit a report to the Legislative Budget Board that prioritizes, for the purpose of receiving funding, state agency

cybersecurity projects. Each state agency shall coordinate with the command to implement this subsection.

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

Sec. 2063.302 ~~[2054.077]~~. VULNERABILITY REPORTS. (a) In this section, a term defined by Section 33.01, Penal Code, has the meaning assigned by that section.

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

(c) Except as provided by this section, a vulnerability report and any information or communication prepared or maintained for use in the preparation of a vulnerability report is

1 confidential and is not subject to disclosure under Chapter 552.

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

- 4 (1) the command ~~[department]~~;
- 5 (2) the state auditor;
- 6 (3) the agency's executive director;
- 7 (4) the agency's designated information resources
8 manager; and

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

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

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

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

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

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

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

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

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

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

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

(2) conducting cybersecurity simulation exercises for

1 state agencies to encourage coordination in defending against and
2 responding to cybersecurity risks and incidents;

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

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

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

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

18 SECTION 12. Section 2054.133, Government Code, is
19 transferred to Subchapter E, Chapter 2063, Government Code, as
20 added by this Act, redesignated as Section 2063.403, Government
21 Code, and amended to read as follows:

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

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

27 (1) consider any vulnerability report prepared under

1 Section 2063.302 [~~2054.077~~] for the agency;

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

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

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

10 (5) include:

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

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

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

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

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

27 (e) Each state agency shall include in the agency's

1 information security plan a written document that is signed by the
2 head of the agency, the chief financial officer, and each executive
3 manager designated by the state agency and states that those
4 persons have been made aware of the risks revealed during the
5 preparation of the agency's information security plan.

6 (f) Not later than November 15 of each even-numbered year,
7 the command [~~department~~] shall submit a written report to the
8 governor, the lieutenant governor, the speaker of the house of
9 representatives, and each standing committee of the legislature
10 with primary jurisdiction over matters related to the command
11 [~~department~~] evaluating information security for this state's
12 information resources. In preparing the report, the command
13 [~~department~~] shall consider the information security plans
14 submitted by state agencies under this section, any vulnerability
15 reports submitted under Section 2063.302 [~~2054.077~~], and other
16 available information regarding the security of this state's
17 information resources. The command [~~department~~] shall omit from
18 any written copies of the report information that could expose
19 specific vulnerabilities [~~in the security of this state's~~
20 ~~information resources~~].

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

25 Sec. 2063.405 [~~2054.516~~]. DATA SECURITY PLAN FOR ONLINE
26 AND MOBILE APPLICATIONS. (a) Each state agency implementing an
27 Internet website or mobile application that processes any sensitive

1 personal or personally identifiable information or confidential
2 information must:

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

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

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

14 SECTION 14. Section [2054.512](#), Government Code, is
15 transferred to Subchapter E, Chapter 2063, Government Code, as
16 added by this Act, redesignated as Section 2063.406, Government
17 Code, and amended to read as follows:

18 Sec. 2063.406 [[2054.512](#)]. CYBERSECURITY COUNCIL. (a) The
19 chief or the chief's designee [~~state cybersecurity coordinator~~]
20 shall [~~establish and~~] lead a cybersecurity council that includes
21 public and private sector leaders and cybersecurity practitioners
22 to collaborate on matters of cybersecurity concerning this state.

23 (b) The cybersecurity council must include:

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

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

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

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

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

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

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

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

17 (e) ~~(d)~~ The cybersecurity council shall:

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

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

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

27 (4) assess the knowledge, skills, and capabilities of

1 the existing information technology and cybersecurity workforce to
2 mitigate and respond to cyber threats and develop recommendations
3 for addressing immediate workforce deficiencies and ensuring a
4 long-term pool of qualified applicants.

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

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

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

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

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

24 Sec. 2063.501 [2054.52001]. DEFINITIONS. In this
25 subchapter:

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

1 [2054.52002].

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

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

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

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

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

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

26 (2) protect all confidential information from
27 disclosure;

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

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

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

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

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

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

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

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

1 ~~[2054.0594(d)]~~ to assist with the incident ~~[event]~~.

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

5 Sec. 2063.506 ~~[2054.52006]~~. CYBERSECURITY COUNCIL
6 DUTIES. The cybersecurity council established under Section
7 2063.406 ~~[2054.512]~~ shall review and make recommendations to the
8 command ~~[department]~~ regarding the policies and procedures used by
9 the command ~~[department]~~ to implement this subchapter. The command
10 ~~[department]~~ may consult with the council to implement and
11 administer this subchapter.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

- 13 (1) contains the contact information for a volunteer;
14 (2) identifies or provides a means of identifying a
15 person who may, as a result of disclosure of the information, become
16 a victim of a cybersecurity incident [~~event~~];
17 (3) consists of a participating entity's cybersecurity
18 plans or cybersecurity-related practices; or
19 (4) is obtained from a participating entity or from a
20 participating entity's computer system in the course of providing
21 assistance under this subchapter.

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

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

(3) immediate response to counter network security activity that exposes this state and the residents of this state to risk, including complete intrusion detection system installation, management, and monitoring for participating entities;

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

(5) cybersecurity educational services.

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

1 with a maximum return on the state's investment.

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

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

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

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

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

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

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

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

27 (B) the extent to which those activities are

1 needed;

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

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

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

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

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

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

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

26 (B) state law and applicable rules of any state
27 agency regarding purchasing guidelines and programs for

1 historically underutilized businesses;

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

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

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

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

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

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

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

27 SECTION 20. Section 38.307(e), Education Code, is amended

1 to read as follows:

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

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

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

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

10 (6) "Other agency of higher education" means The
11 University of Texas System, System Administration; The University
12 of Texas at El Paso Museum; Texas Epidemic Public Health Institute
13 at The University of Texas Health Science Center at Houston; the
14 Texas Cyber Command; The Texas A&M University System,
15 Administrative and General Offices; Texas A&M AgriLife Research;
16 Texas A&M AgriLife Extension Service; Rodent and Predatory Animal
17 Control Service (a part of the Texas A&M AgriLife Extension
18 Service); Texas A&M Engineering Experiment Station (including the
19 Texas A&M Transportation Institute); Texas A&M Engineering
20 Extension Service; Texas A&M Forest Service; Texas Division of
21 Emergency Management; Texas Tech University Museum; Texas State
22 University System, System Administration; Sam Houston Memorial
23 Museum; Panhandle-Plains Historical Museum; Cotton Research
24 Committee of Texas; Texas Water Resources Institute; Texas A&M
25 Veterinary Medical Diagnostic Laboratory; and any other unit,
26 division, institution, or agency which shall be so designated by
27 statute or which may be established to operate as a component part

1 of any public senior college or university, or which may be so
2 classified as provided in this chapter.

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

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

- 7 (1) The University of Texas at Arlington;
- 8 (2) The University of Texas at Austin;
- 9 (3) The University of Texas at Dallas;
- 10 (4) The University of Texas at El Paso;
- 11 (5) The University of Texas Permian Basin;
- 12 (6) The University of Texas at San Antonio;
- 13 (7) The University of Texas Southwestern Medical
14 Center;
- 15 (8) The University of Texas Medical Branch at
16 Galveston;
- 17 (9) The University of Texas Health Science Center at
18 Houston;
- 19 (10) The University of Texas Health Science Center at
20 San Antonio;
- 21 (11) The University of Texas M. D. Anderson Cancer
22 Center;
- 23 (12) Stephen F. Austin State University, a member of
24 The University of Texas System;
- 25 (13) The University of Texas at Tyler; ~~and~~
- 26 (14) The University of Texas Rio Grande Valley; and
- 27 (15) the Texas Cyber Command (Chapter 2063, Government

1 Code).

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

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

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

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

19 (c) A program offered under this section must:

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

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

25 (3) include a one-year apprenticeship with:

26 (A) the department;

27 (B) another relevant state agency;

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

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

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

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

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

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

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

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

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

26 (6) a description of the means and strategies for
27 meeting the agency's needs, including future needs, and achieving

1 the goals established under Section 2056.006 for each area of state
2 government for which the agency provides services;

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

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

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

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

17 (11) an analysis of the strategic use of information
18 resources as provided by the instructions prepared under Section
19 2054.095;

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

23 (13) other information that may be required.

24 SECTION 26. (a) In this section, "department" means the
25 Department of Information Resources.

26 (b) On the effective date of this Act:

27 (1) the Texas Cyber Command, organized as provided by

1 Section 2063.002, Government Code, as added by this Act, is created
2 with the powers and duties assigned by Chapter 2063, Government
3 Code, as added by this Act; and

4 (2) the chief information security officer of the
5 department becomes the chief of the Texas Cyber Command, as
6 described by Section 2063.0025, Government Code, as added by this
7 Act.

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

14 (d) Not later than December 31, 2026:

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

19 (2) all employees of the department who primarily
20 perform duties related to cybersecurity, including employees who
21 provide administrative support for those services, under Chapter
22 2063, Government Code, as added by this Act, become employees of the
23 Texas Cyber Command, but continue to work in the same physical
24 location unless moved in accordance with the memorandum of
25 understanding entered into under Subsection (e) of this section;

26 (3) a rule or form adopted by the department that
27 relates to cybersecurity under Chapter 2063, Government Code, as

1 added by this Act, is a rule or form of the Texas Cyber Command and
2 remains in effect until changed by the command;

3 (4) a reference in law to the department that relates
4 to cybersecurity under Chapter 2063, Government Code, as added by
5 this Act, means the Texas Cyber Command;

6 (5) a contract negotiation or other proceeding
7 involving the department that is related to cybersecurity under
8 Chapter 2063, Government Code, as added by this Act, is transferred
9 without change in status to the Texas Cyber Command, and the Texas
10 Cyber Command assumes, without a change in status, the position of
11 the department in a negotiation or proceeding relating to
12 cybersecurity to which the department is a party;

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

17 (7) all property, including records, in the custody of
18 the department related to cybersecurity under Chapter 2063,
19 Government Code, as added by this Act, becomes property of the Texas
20 Cyber Command, but stays in the same physical location unless moved
21 in accordance with the specific steps and methods created under
22 Subsection (e) of this section; and

23 (8) all funds appropriated by the legislature to the
24 department for purposes related to cybersecurity, including funds
25 for providing administrative support, under Chapter 2063,
26 Government Code, as added by this Act, are transferred to the Texas
27 Cyber Command.

1 (e) Not later than January 1, 2026, the department and the
2 board of regents of The University of Texas System shall enter into
3 a memorandum of understanding relating to the transfer of powers
4 and duties from the department to the Texas Cyber Command as
5 provided by this Act. The memorandum must include:

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

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

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

17 SECTION 27. This Act takes effect September 1, 2025.