GOVERNMENT CODE

TITLE 10. GENERAL GOVERNMENT

SUBTITLE B. INFORMATION AND PLANNING

CHAPTER 2063. TEXAS CYBER COMMAND

SUBCHAPTER A. GENERAL PROVISIONS

Sec. 2063.001. DEFINITIONS. In this chapter:

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

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

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

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

(A) chemical facilities;

(B) commercial facilities;

(C) communication facilities;

(D) manufacturing facilities;

(E) dams;

(F) defense industrial bases;

(G) emergency services systems;

(H) energy facilities;

(I) financial services systems;

(J) food and agriculture facilities;

(K) government facilities;

(L) health care and public health facilities;

(M) information technology and information technology systems;

(N) nuclear reactors, materials, and waste;

(O) transportation systems; or

(P) water and wastewater systems.

(5) "Cybersecurity" means the measures taken for a

computer, computer network, computer system, or other technology infrastructure to protect against, respond to, and recover from unauthorized:

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

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

(6) "Cybersecurity incident" includes:

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

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

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

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

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

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

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

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

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

(13) "State agency" means:

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

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

(C) a university system or an institution of

higher education as defined by Section 61.003, Education Code.
Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

Sec. 2063.002. ORGANIZATION. (a) The Texas Cyber Command is a state agency.

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

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

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

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

(2) a facility to the command located in San Antonio that has a sensitive compartmented information facility for use in carrying out the purposes of this chapter and Chapter 2059.
Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

Sec. 2063.0025. COMMAND CHIEF. (a) In this section, "state cybersecurity program" means the policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish the cybersecurity function for this state.

(b) The chief directs the day-to-day operations and policies of the command and oversees and is responsible for all functions and duties of the command.

(c) The chief shall oversee cybersecurity matters for this state including:

(1) implementing the duties described by Section 2063.004;

(2) developing a statewide cybersecurity framework;

(3) overseeing the development of cybersecurity policies and standards;

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

(5) overseeing the implementation of the policies, standards, and requirements developed under this chapter;

(6) providing cybersecurity leadership, strategic direction, and coordination for the state cybersecurity program;

(7) providing strategic direction to:

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

(B) regional security operations centers operated under Subchapter G; and

(8) overseeing the preparation and submission of the report described by Section 2063.301.

Added by Acts 2023, 88th Leg., R.S., Ch. 1079 (S.B. 621), Sec. 1, eff. September 1, 2023.

Transferred, redesignated and amended from Government Code, Section 2054.510 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 2, eff. September 1, 2025.

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

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

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

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

(3) monitoring and coordinating cyber threat intelligence and information systems to detect and warn entities of

cyber attacks, identifying cyber threats to critical infrastructure and state systems, planning and executing cybersecurity incident responses, and conducting digital forensics of cybersecurity incidents to support law enforcement and attribute the incidents;

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

(1) promote public awareness of cybersecurity issues;

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

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

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

(5) provide support to state agencies and covered entities experiencing a cybersecurity incident and respond to cybersecurity reports received under Subchapter D and other reports as appropriate;

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

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

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

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

covered entities;

(10) collaborate with the department to ensure information resources and information resources technologies obtained by the department meet the cybersecurity standards and requirements established under this chapter;

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

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

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

(b) The command may:

(1) adopt and use an official seal;

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

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

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

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

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

Sec. 2063.005. COST RECOVERY. The command may recover the

cost of providing direct technical assistance, training services, and other services to covered entities when reasonable and practical.

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

Added by Acts 2017, 85th Leg., R.S., Ch. 955 (S.B. 1910), Sec. 1, eff. September 1, 2017.

Transferred, redesignated and amended from Government Code, Section 2054.0592 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 3, eff. September 1, 2025.

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

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

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

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

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

(A) the necessity for making the purchase;

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

(C) any competitive processes used, if applicable.

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

Sec. 2063.009. RULES. The chief may adopt rules necessary for carrying out the purposes of this chapter.

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

SUBCHAPTER B. MINIMUM STANDARDS AND TRAINING

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

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

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

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

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

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

(2) teach best practices and minimum standards established under this subchapter.

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

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

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

(f) In addition to the requirements for certification under Subsection (b), a cybersecurity training program must include education on:

(1) the threat of foreign adversaries and other hostile foreign actors, including the United Front Work Department of the Central Committee of the Chinese Communist Party and other coordinated foreign influence operations;

(2) known efforts by foreign adversaries to target and influence subnational governments, including efforts made by the United Front Work Department;

(3) identifying and recognizing suspected foreign influence operations;

(4) informational resources promulgated by federal, state, and nongovernmental organizations on United Front Work Department activities in this state and adjacent states; and

(5) reporting to the Texas Ethics Commission as required by Section 572.070 and to law enforcement agencies suspected foreign influence operations and other interactions with persons acting on behalf of a foreign adversary.

(g) In Subsection (f), "foreign adversary" has the meaning assigned by Section 572.070.

Added by Acts 2019, 86th Leg., R.S., Ch. 1308 (H.B. 3834), Sec. 3, eff. June 14, 2019.

Amended by:

Acts 2021, 87th Leg., R.S., Ch. 51 (H.B. 1118), Sec. 5, eff. May 18, 2021.

Transferred, redesignated and amended from Government Code, Section 2054.519 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150),

Sec. 4, eff. September 1, 2025.

Amended by:

Acts 2025, 89th Leg., R.S., Ch. 881 (S.B. 2514), Sec. 3, eff. September 1, 2025.

Text of section as transferred, redesignated, and amended by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150)

For text of section as amended by Acts 2025, 89th Leg., R.S., Ch. 628 (H.B. 3512), see Sec. 2054.5191.

Sec. 2063.103. CYBERSECURITY TRAINING REQUIRED. (a) Each elected or appointed official and employee of a governmental entity who has access to the entity's information resources or information resources technologies shall annually complete a cybersecurity training program certified under Section 2063.102.

(b) The governing body of a governmental entity or the governing body's designee may deny access to the governmental entity's information resources or information resources technologies to an employee or official who is noncompliant with the requirements of Subsection (a).

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

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

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

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

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

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

(g) The requirements of Subsection (a) do not apply to employees and officials who have been:

(1) granted military leave;

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

(3) granted leave related to a sickness or disability covered by workers' compensation benefits, if that employee or official no longer has access to the governmental entity's information resources or information resources technologies;

(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; or

(5) denied access to a governmental entity's information resources or information resources technologies under Subsection (b) for noncompliance with the requirements of Subsection (a).

Added by Acts 2019, 86th Leg., R.S., Ch. 1308 (H.B. 3834), Sec. 3, eff. June 14, 2019.

Amended by:

Acts 2021, 87th Leg., R.S., Ch. 51 (H.B. 1118), Sec. 3, eff. May 18, 2021.

Transferred, redesignated and amended from Government Code, Section 2054.5191 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 5, eff. September 1, 2025.

Sec. 2063.104. 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 as selected by the agency.

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

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

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

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

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

Added by Acts 2019, 86th Leg., R.S., Ch. 1308 (H.B. 3834), Sec. 3, eff. June 14, 2019.

Amended by:

Acts 2021, 87th Leg., R.S., Ch. 856 (S.B. 800), Sec. 12, eff. September 1, 2021.

Transferred, redesignated and amended from Government Code, Section 2054.5192 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 6, eff. September 1, 2025.

SUBCHAPTER C. CYBERSECURITY PREVENTION, RESPONSE, AND RECOVERY

Sec. 2063.201. CYBERSECURITY THREAT INTELLIGENCE CENTER.

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

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

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

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

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

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

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

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

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

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

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

experienced a cybersecurity incident in order to remediate identified cybersecurity vulnerabilities;

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

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

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

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

(B) document chains of custody; and

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

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

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

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

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

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

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

(b) 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) The command shall establish a framework for regional cybersecurity task forces 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 to assist with responding to a cybersecurity incident in this state. A task force may be established within the geographic area of a regional planning commission established under Chapter 391, Local Government Code. The task force may establish a list of available cybersecurity experts and share resources to assist in responding to the cybersecurity incident and recovery

from the incident.

Added by Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 5, eff. September 1, 2017.

Amended by:

Acts 2019, 86th Leg., R.S., Ch. 509 (S.B. 64), Sec. 10, eff. September 1, 2019.

Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 3, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Section 2054.0594 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 7, eff. September 1, 2025.

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

SUBCHAPTER D. REPORTING

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

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

(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.

(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) The command 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.

Added by Acts 2017, 85th Leg., R.S., Ch. 955 (S.B. 1910), Sec. 1, eff. September 1, 2017.

Amended by:

Acts 2019, 86th Leg., R.S., Ch. 509 (S.B. 64), Sec. 9, eff. September 1, 2019.

Transferred, redesignated and amended from Government Code, Section 2054.0591 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 9, eff. September 1, 2025.

Sec. 2063.302. CYBERSECURITY INCIDENT NOTIFICATION BY STATE AGENCY OR LOCAL GOVERNMENT. (a) A state agency or local government that owns, licenses, or maintains computerized data that includes sensitive personal information, confidential information, or information the disclosure of which is regulated by law shall, in the event of a cybersecurity incident:

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

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

(A) the command, including the chief; or

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

(3) comply with all command rules relating to reporting cybersecurity incidents as required by this section.

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

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

(e) Contract language in a cybersecurity insurance contract or other contract for goods or services prohibiting or restricting a state agency's or local government's compliance with this section or otherwise circumventing the requirements of this section is void and unenforceable.

Added by Acts 2009, 81st Leg., R.S., Ch. 419 (H.B. 2004), Sec. 4, eff. September 1, 2009.

Amended by:

Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 8, eff. September 1, 2017.

Acts 2019, 86th Leg., R.S., Ch. 509 (S.B. 64), Sec. 14, eff. September 1, 2019.

Transferred, redesignated and amended from Government Code, Section 2054.1125 by Acts 2023, 88th Leg., R.S., Ch. 67 (S.B. 271), Sec. 1, eff. September 1, 2023.

Transferred, redesignated and amended from Government Code, Section 2054.603 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 9, eff. September 1, 2025.

Amended by:

Acts 2025, 89th Leg., R.S., Ch. 683 (H.B. 5331), Sec. 1, eff. September 1, 2025.

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

(b) The information security officer of a state agency shall prepare or have prepared a report, including an executive summary

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

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

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

(1) the command;

(2) the state auditor;

(3) the agency's executive director;

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

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

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

Added by Acts 2001, 77th Leg., ch. 792, Sec. 1, eff. June 14, 2001.

Amended by:

Acts 2009, 81st Leg., R.S., Ch. 183 (H.B. 1830), Sec. 5, eff. September 1, 2009.

Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 7, eff.

September 1, 2017.

Acts 2019, 86th Leg., R.S., Ch. 509 (S.B. 64), Sec. 13, eff. September 1, 2019.

Acts 2021, 87th Leg., R.S., Ch. 856 (S.B. 800), Sec. 9, eff. September 1, 2021.

Transferred, redesignated and amended from Government Code, Section 2054.077 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 9, eff. September 1, 2025.

SUBCHAPTER E. CYBERSECURITY PREPARATION AND PLANNING

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

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

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

(3) possesses the training and experience required to ensure the agency complies with requirements and policies established by the command; and

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

Added by Acts 2017, 85th Leg., R.S., Ch. 955 (S.B. 1910), Sec. 4, eff. September 1, 2017.

Transferred, redesignated and amended from Government Code, Section 2054.136 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 10, eff. September 1, 2025.

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

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

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

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

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

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

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

Added by Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 11, eff. September 1, 2017.

Amended by:

Acts 2019, 86th Leg., R.S., Ch. 1308 (H.B. 3834), Sec. 2, eff. June 14, 2019.

Acts 2019, 86th Leg., R.S., Ch. 1308 (H.B. 3834), Sec. 4, eff. June 14, 2019.

Transferred, redesignated and amended from Government Code, Section 2054.518 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 11, eff. September 1, 2025.

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

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

(1) consider any vulnerability report prepared under Section 2063.303 for the agency;

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

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

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

(5) include:

(A) the best practices for information security developed by the command; or

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

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

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

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

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

(f) Not later than November 15 of each even-numbered year, the command shall submit a written report to the governor, the lieutenant governor, the speaker of the house of representatives, and each standing committee of the legislature with primary jurisdiction over matters related to the command evaluating

information security for this state's information resources. In preparing the report, the command shall consider the information security plans submitted by state agencies under this section, any vulnerability reports submitted under Section 2063.303, and other available information regarding the security of this state's information resources. The command shall omit from any written copies of the report information that could expose specific vulnerabilities.

Added by Acts 2013, 83rd Leg., R.S., Ch. 1222 (S.B. 1597), Sec. 1, eff. September 1, 2013.

Amended by:

Acts 2015, 84th Leg., R.S., Ch. 369 (S.B. 34), Sec. 1, eff. September 1, 2015.

Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 10, eff. September 1, 2017.

Acts 2017, 85th Leg., R.S., Ch. 955 (S.B. 1910), Sec. 3, eff. September 1, 2017.

Acts 2019, 86th Leg., R.S., Ch. 509 (S.B. 64), Sec. 15, eff. September 1, 2019.

Acts 2019, 86th Leg., R.S., Ch. 573 (S.B. 241), Sec. 1.14, eff. September 1, 2019.

Transferred, redesignated and amended from Government Code, Section 2054.133 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 12, eff. September 1, 2025.

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1, eff. September 1, 2025.

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

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

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

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

Added by Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 11, eff. September 1, 2017.

Added by Acts 2017, 85th Leg., R.S., Ch. 955 (S.B. 1910), Sec. 5, eff. September 1, 2017.

Reenacted and amended by Acts 2019, 86th Leg., R.S., Ch. 467 (H.B. 4170), Sec. 8.016, eff. September 1, 2019.

Reenacted and amended by Acts 2019, 86th Leg., R.S., Ch. 509 (S.B. 64), Sec. 16, eff. September 1, 2019.

Amended by:

Acts 2021, 87th Leg., R.S., Ch. 856 (S.B. 800), Sec. 11, eff. September 1, 2021.

Transferred, redesignated and amended from Government Code, Section 2054.516 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 13, eff. September 1, 2025.

Sec. 2063.406. CYBERSECURITY COUNCIL. (a) The chief or the chief's designee shall lead a cybersecurity council that includes public and private sector leaders and cybersecurity practitioners to collaborate on matters of cybersecurity concerning this state.

(b) The cybersecurity council must include:

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

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

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

(4) the director of the Elections Division of the Office of the Secretary of State;

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

(6) additional members appointed by the chief, including representatives of institutions of higher education and private sector leaders.

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

(d) In appointing representatives from institutions of higher education to the cybersecurity council, the chief shall consider appointing members of the Information Technology Council for Higher Education.

(e) The cybersecurity council shall:

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

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

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

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

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

Added by Acts 2013, 83rd Leg., R.S., Ch. 32 (S.B. 1102), Sec. 1, eff. May 10, 2013.

Redesignated from Government Code, Section 2054.552 by Acts 2015, 84th Leg., R.S., Ch. 1236 (S.B. 1296), Sec. 21.001(29), eff.

September 1, 2015.

Amended by:

Acts 2017, 85th Leg., R.S., Ch. 683 (H.B. 8), Sec. 9, eff. September 1, 2017.

Acts 2021, 87th Leg., R.S., Ch. 376 (S.B. 851), Sec. 1, eff. September 1, 2021.

Transferred, redesignated and amended from Government Code, Section 2054.512 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 14, eff. September 1, 2025.

Sec. 2063.407. RECOMMENDATIONS. The chief may implement any portion, or all of the recommendations made by the cybersecurity council under Section 2063.406.

Added by Acts 2013, 83rd Leg., R.S., Ch. 32 (S.B. 1102), Sec. 1, eff. May 10, 2013.

Redesignated from Government Code, Section 2054.554 by Acts 2015, 84th Leg., R.S., Ch. 1236 (S.B. 1296), Sec. 21.001(29), eff. September 1, 2015.

Transferred, redesignated and amended from Government Code, Section 2054.514 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 15, eff. September 1, 2025.

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

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

(1) the federal government; or

(2) another state that the command approves.

(c) The command by rule shall prescribe:

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

management program; and

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

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

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

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 2, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Section 2054.0593 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 16, eff. September 1, 2025.

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

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

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

Added by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 1,

eff. September 1, 2025.

SUBCHAPTER F. TEXAS VOLUNTEER INCIDENT RESPONSE TEAM

Sec. 2063.501. DEFINITIONS. In this subchapter:

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

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

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

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

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

Sec. 2063.503. CONTRACT WITH VOLUNTEERS. The command shall enter into a contract with each volunteer the command approves to

provide rapid response assistance under this subchapter. The contract must require the volunteer to:

(1) acknowledge the confidentiality of information required by Section 2063.510;

(2) protect all confidential information from disclosure;

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

(4) comply with command security policies and procedures regarding information resources technologies;

(5) consent to background screening required by the command; and

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

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

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

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

Sec. 2063.505. DEPLOYMENT. (a) In response to a cybersecurity incident that affects multiple participating entities or a declaration by the governor of a state of disaster caused by a cybersecurity event, the command on request of a

participating entity may deploy volunteers and provide rapid response assistance under the command's direction and the managed security services framework established under Section 2063.204(c) to assist with the incident.

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

Sec. 2063.507. COMMAND POWERS AND DUTIES. (a) The command shall:

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

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

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

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

(B) process for an individual to apply for and

accept incident response team membership;

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

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

(4) adopt rules necessary to implement this subchapter.

(b) The command may require a participating entity to enter into a contract as a condition for obtaining assistance from the incident response team.

(c) The command may provide appropriate training to prospective and approved volunteers.

(d) In accordance with state law, the command 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 may establish a fee schedule for participating entities receiving incident response team assistance. The amount of fees collected may not exceed the command's costs to operate the incident response team.

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

Sec. 2063.508. 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.

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331

(H.B. 150), Sec. 17, eff. September 1, 2025.

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

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

(1) contains the contact information for a volunteer;

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

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

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 6, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter N-2, Chapter 2054 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 17, eff. September 1, 2025.

SUBCHAPTER G. REGIONAL SECURITY OPERATIONS CENTERS

Sec. 2063.601. 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 security operations center under this subchapter.

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 9, eff. June 14, 2021.

Amended by:

Acts 2023, 88th Leg., R.S., Ch. 242 (H.B. 4553), Sec. 12, eff. September 1, 2023.

Transferred, redesignated and amended from Government Code, Subchapter E, Chapter 2059 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 18, eff. September 1, 2025.

Sec. 2063.602. ESTABLISHMENT OF REGIONAL SECURITY OPERATIONS CENTERS. (a) Subject to Subsection (b), the command may establish regional security operations centers, under the command's managed security services framework established by Section 2063.204(c), 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 may establish more than one regional security operations center only if the command determines the first center established by the command successfully provides to state agencies and other eligible entities the services the center has contracted to provide.

(c) The command 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 security operations center.

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 9, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter E, Chapter 2059 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 18, eff. September 1, 2025.

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

(1) serve as an education partner with the command for the regional security operations center; and

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

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

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

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

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 9, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter E, Chapter 2059 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 18, eff. September 1, 2025.

Sec. 2063.604. REGIONAL SECURITY OPERATIONS CENTERS SERVICES AND SUPPORT. The command may offer the following managed security services through a regional security operations center:

(1) real-time cybersecurity monitoring to detect and

respond to cybersecurity incidents that may jeopardize this state and the residents of this state;

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

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

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

(5) cybersecurity educational services.

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 9, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter E, Chapter 2059 by Acts 2025, 89th Leg., R.S., Ch. 331 (H.B. 150), Sec. 18, eff. September 1, 2025.

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

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

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

Added by Acts 2021, 87th Leg., R.S., Ch. 567 (S.B. 475), Sec. 9, eff. June 14, 2021.

Transferred, redesignated and amended from Government Code, Subchapter E, Chapter 2059 by Acts 2025, 89th Leg., R.S., Ch. 331

(H.B. 150), Sec. 18, eff. September 1, 2025.