|  |
| --- |
| BILL ANALYSIS |

|  |
| --- |
| C.S.H.B. 150 |
| By: Capriglione |
| Delivery of Government Efficiency |
| Committee Report (Substituted) |

|  |
| --- |
| **BACKGROUND AND PURPOSE**  The bill's author has informed the committee of the increasing number of cyberattacks on Texas state agencies, local governments, political subdivisions, critical infrastructure, and private entities. Furthermore, these sophisticated attacks are seemingly being carried out not only by cybercriminals, but also hostile nation-state actors. Currently, in addition to their core missions of procurement and information technology, the Department of Information Resources (DIR) is tasked with certain cybersecurity responsibilities. However, the bill's author has also informed the committee that given the scale of these threats, the state's cybersecurity merits its own purpose-built agency whose sole focus is to prevent, respond to, and defend against cybersecurity threats and increase the cybersecurity posture and resiliency of the state.  C.S.H.B. 150 seeks to address this issue by establishing the Texas Cyber Command, which will execute and enhance existing cybersecurity responsibilities performed by DIR, improve the operational capacity of the state through the Cyber Threat Intelligence Center, Critical Incident Response Unit, and Forensics Laboratory, and leverage the robust cybersecurity ecosystem of the San Antonio region, including federal partners, academic institutions, and private sector entities. |
| **CRIMINAL JUSTICE IMPACT**  It is the committee's opinion that this bill does not expressly create a criminal offense, increase the punishment for an existing criminal offense or category of offenses, or change the eligibility of a person for community supervision, parole, or mandatory supervision. |
| **RULEMAKING AUTHORITY**  It is the committee's opinion that rulemaking authority is expressly granted to the Texas Cyber Command and the chief of the Texas Cyber Command in SECTION 1 of this bill. |
| **ANALYSIS**  C.S.H.B. 150 provides for the establishment of the Texas Cyber Command as a component institution of The University of Texas System. The bill transfers to the command certain of the powers and duties relating to cybersecurity that are currently assigned under the Information Resources Management Act to the Department of Information Resources (DIR) and certain duties relating to regional network security centers under statutes governing the Texas computer network security system that are also currently assigned to DIR. Accordingly, the bill amends the Government Code to create a new statutory framework for the regulation of the command that incorporates the transferred provisions as renumbered by the bill, revises a number of the renumbered provisions, including updating applicable definitions and relevant terminology, and establishes certain new provisions within that framework. The bill amends certain other provisions of that code and conforms others to the new statutory framework. The bill also amends the Education Code to reflect the establishment of the command within the UT system and to conform certain other provisions of that code to reflect the transfer of applicable DIR powers and duties to the command. The bill also sets out transition and procedural provisions relating to the transfer of the applicable powers and duties from DIR to the command.  **Definitions Applicable to New Statutory Framework**  C.S.H.B. 150 defines the following terms for purposes of the bill's provisions establishing the Texas Cyber Command and for purposes of the provisions transferred and renumbered, incorporated, and applicably revised by the bill:   * "covered entity" as a private entity operating critical infrastructure or a local government that the command contracts with in order to provide cybersecurity services as provided by the bill; * "critical infrastructure" as infrastructure in Texas vital to the security, governance, public health and safety, economy, or morale of the state or the nation, including chemical facilities, commercial facilities, communication facilities, manufacturing facilities, dams, defense industrial bases, emergency services systems, energy facilities, financial services systems, food and agriculture facilities, government facilities, health care and public health facilities, information technology and information technology systems, nuclear reactors, materials, and waste, transportation systems, or water and wastewater systems; * "cybersecurity" as the measures taken for a computer, computer network, computer system, or other technology infrastructure to protect against, respond to, and recover from unauthorized use, access, disruption, modification, or destruction or from unauthorized disclosure, modification, or destruction of information; * "cybersecurity incident" as including:   + a breach or suspected breach of system security;   + the introduction of ransomware into a computer, computer network, or computer system; or   + any other cybersecurity-related occurrence that jeopardizes information or an information system designated by an adopted Texas Cyber Command policy; * "governmental entity" as the state, a state agency, or a local government; * "information resources" and "information resources technologies" by reference to the meaning assigned to those terms by the Information Resources Management Act in the Government Code; * "local government" by reference to the meanings assigned to that term by the Information Resources Management Act in the Government Code; * "sensitive personal information" by reference to the meaning assigned to that term by the Identity Theft Enforcement and Protection Act in the Business & Commerce Code; and * "state agency" as:   + a department, commission, board, office, or other agency that is in the executive branch of state government and that was created by the state constitution or a statute;   + 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   + a university system or a public institution of higher education.   **Establishment of the Texas Cyber Command**  General Provisions (Subchapter A)  *Organization*  C.S.H.B. 150 amends the Government Code to establish the Texas Cyber Command as a component of The University of Texas System administratively attached to The University of Texas at San Antonio and managed by a chief of the command. The chief of the command is appointed by the governor and confirmed with the advice and consent of the senate. The chief of the command serves at the pleasure of the governor and must possess professional training and knowledge relevant to the functions and duties of the command. The bill requires the command to employ other coordinating and planning officers and other personnel necessary to the performance of its functions. The University of Texas at San Antonio, under an agreement with the command, must provide administrative support services for the command as necessary to carry out the bill's purposes.  *Transferred Provision: Command Chief*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision establishing the information resources security function for the state, defining the "state information security program," and requiring the employment of a chief information security officer by the executive director of DIR to oversee cybersecurity matters for the state. The bill renames the program as the state cybersecurity program and revises the definition of the program to mean the policies, standards, procedures, elements, structure, strategies, objectives, plans, metrics, reports, services, and resources that establish the cybersecurity function for the state. The bill makes the following changes with respect to this transferred provision:   * removes the chief information security officer employed by the executive director of DIR as the person responsible for overseeing cybersecurity matters for the state and makes the chief of the command the person responsible for that oversight; * replaces references to the terms "statewide information security," "state information security," and "information resources security" with references to "cybersecurity"; * establishes that the chief of the command directs the day-to-day operations and policies of the command and oversees cybersecurity matters for the state, including implementing the general powers and duties established under the bill's provisions and subsequently described; * removes an obsolete reference to an expired statutory provision and replaces references to statewide technology centers with references to regional security operations centers to conform to the bill's subsequently described and transferred provisions regarding such centers; and * with regard to the requirement for oversight by the chief of the command over cybersecurity matters that involve collaborating with certain entities operating or exercising control over state information systems or state-controlled data to strengthen the state's cybersecurity and information security policies, standards, and guidelines, specifies that the oversight is applicable to such systems or data critical to strengthen such policies, standards, and guidelines.   *Establishment and Purpose*  C.S.H.B. 150 establishes the command to prevent and respond to cybersecurity incidents that affect governmental entities and critical infrastructure in Texas. The bill establishes that the command is responsible for cybersecurity for Texas, including the following:   * developing tools to enhance cybersecurity defenses; * facilitating education and training of a cybersecurity workforce; * developing cyber threat intelligence, monitoring information systems to detect and warn entities of cyber attacks, proactively searching for cyber threats to critical infrastructure and state systems, developing and executing cybersecurity incident responses, and conducting digital forensics of cybersecurity incidents to support law enforcement and attribute the incidents; * creating partnerships needed to effectively carry out the command's functions; and * receiving all cybersecurity incident reports from state agencies and covered entities.   *General Powers and Duties*  C.S.H.B. 150 requires the command to do the following:   * promote public awareness of cybersecurity issues; * develop cybersecurity best practices and minimum standards for governmental entities; * develop and provide training to state agencies and covered entities on cybersecurity measures and awareness; * administer the cybersecurity threat intelligence center, as established under the bill's provisions; * provide support to state agencies and covered entities experiencing a cybersecurity incident and respond to cybersecurity reports received under the bill's applicable provisions and other reports as appropriate; * administer the digital forensics laboratory, as established under the bill's provisions; * 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; * collaborate with law enforcement agencies to provide training and support related to cybersecurity incidents; * 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; * collaborate with DIR to ensure information resources and information resources technologies obtained by DIR meet the cybersecurity standards and requirements established under the bill's provisions; * offer cybersecurity resources to state agencies and covered entities as determined by the command; * 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 * collaborate with federal agencies to protect against, respond to, and recover from cybersecurity incidents.   Furthermore, the bill authorizes the command to do the following:   * adopt and enforce rules necessary to carry out the bill's provisions; * adopt and use an official seal; * establish ad hoc advisory committees as necessary to carry out the command's duties under the bill's provisions; * acquire and convey property or an interest in property; * 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; * 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 enter into license agreements with any third parties for the receipt of fees, royalties, or other monetary or nonmonetary value; and * solicit and accept gifts, grants, donations, or loans from and contract with any entity to accomplish the command's duties.   C.S.H.B. 150 requires the command to deposit money paid to the command in the state treasury to the credit of the general revenue fund, except as otherwise provided.  *Cost Recovery*  C.S.H.B. 150 requires the command to recover the cost of providing direct technical assistance, training services, and other services to covered entities when reasonable and practical.  *Transferred Provision: Cybersecurity Emergency Funding*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision authorizing DIR to make a request to the governor or the Legislative Budget Board (LBB) under applicable state law to provide funding to manage the operational and financial impacts from a cybersecurity event that creates a need for emergency funding. The bill amends that provision to authorize the command instead to make that request.  *Emergency Purchasing*  C.S.H.B. 150, in the event the emergency response to a cybersecurity incident requires the command to purchase an item, exempts the command in making the purchase from the requirements of statutory provisions relating to the verification of use of the best value standard, notice in the electronic state business daily regarding procurements exceeding $25,000 in value, and the applicable monitoring of delegated purchases exceeding $50,000 by the comptroller of public accounts.  *Rules*  C.S.H.B. 150 authorizes the chief of the command to adopt rules necessary for carrying out the bill's provisions.  *Application of Sunset Act*  C.S.H.B. 150 subjects the command to the Texas Sunset Act and abolishes the command on September 1, 2031, unless continued in existence as provided by that act.  Minimum Standards and Training (Subchapter B)  *Best Practices and Minimum Standards for Cybersecurity and Training*  C.S.H.B. 150 requires the command to do the following:   * develop and annually assess best practices and minimum standards for use by governmental entities to enhance the security of information resources in Texas; * establish and periodically assess mandatory cybersecurity training that must be completed by all information resources employees of state agencies and consult with the Information Technology Council for Higher Education established under the Information Resources Management Act regarding applying the training requirements to employees of institutions of higher education; and * adopt policies to ensure governmental entities are complying with these requirements.   *Transferred Provision: State Certified Cybersecurity Training Programs*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision making DIR responsible under current law for certifying certain state cybersecurity training programs and revises that transferred provision to reflect the following with respect to the bill's transfer of that responsibility from DIR to the command:   * the command, in consultation with industry stakeholders and the cybersecurity council as established under the Information Resources Management Act and transferred to the command's purview under the bill's provisions, must annually certify at least five cybersecurity training programs for state and local government employees and must update standards for maintenance of certification by the cybersecurity training programs under this transferred and revised provision; * in order to be certified under this provision, a cybersecurity training program must focus on forming appropriate cybersecurity habits and procedures that protect information resources and must teach best practices and minimum standards, as established under the bill's provisions establishing minimum standards for cybersecurity and training; * the command may identify and certify training programs provided by state agencies and local governments that satisfy the described training requirements; * the command may contract with an independent third party to certify cybersecurity training programs under this provision; and * the command must annually publish on the command's website the list of cybersecurity training programs certified under this provision.   *Transferred Provisions: Cybersecurity Training Required for Certain Employees, Officers, and Officials*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision requiring certain, but not all, state and local government employees, each elected or appointed officer of a state agency, and certain, but not all, local government elected or appointed officials to complete at least once each year a state certified cybersecurity training program. The bill changes the transferred provision to require instead that each elected or appointed official and each employee of a governmental entity who has access to the entity's information resources or information resources technologies to annually complete a state certified cybersecurity training program. Accordingly, the bill removes the following from the transferred provision:   * the conditions limiting the applicability of that training requirement to state employees who use a computer to complete at least 25 percent of the employee's required duties; and * the conditions limiting such applicability to local government employees and elected or appointed local government 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.   Moreover, while current law in the transferred provision authorizes the governing body of a local government or the governing body's designee to deny access to the local government's computer system or database to a local government employee and elected or appointed official who is determined by the governing body or designee to be noncompliant with the training requirement, the bill provides that the governing body of any governmental entity or the governing body's designee may deny access to the governmental entity's information resources or information resources technologies to any employee or official of a governmental entity who is noncompliant with the training requirement. The bill retains certain of the other authorizations and requirements of the transferred provision without revision and revises others to reflect the previously described changes to provide the following:   * the governing body of a local government may select the most appropriate cybersecurity training program certified by the command under the bill's provisions for employees and officials of the local government to complete, the governing body must verify and report on the completion of a cybersecurity training program by employees and officials of the local government to the command, and, in a retained but unchanged provision, the governing body must require periodic audits to ensure compliance with these transferred provisions; * a state agency may select the most appropriate cybersecurity training program certified by the command under the bill's provisions for employees and officials of the state agency, the executive head of each state agency must verify completion of a cybersecurity training program by employees and officials of the state agency in a manner specified by the command, and, in a retained but unchanged provision, the executive head of each state agency must periodically require an internal review of the agency to ensure compliance with these transferred provisions; and * the command must develop a form for use by governmental entities in verifying completion of cybersecurity training program requirements under these transferred provisions, and the form must allow the state agency and local government to indicate the percentage of employee and official completion.   Furthermore, the bill retains and does not revise the exemptions from the requirement for the completion of annual cybersecurity training applicable to employees and officials who have been granted military leave or leave under the federal Family and Medical Leave Act. However, the following exemptions are applicably revised to reflect the previously described changes to the cybersecurity training requirement and, accordingly, the bill provides that those revised training requirements do not apply to employees and officials who have been, as follows:   * 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; * 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 * denied access to a governmental entity's information resources or information resources technologies under the bill's transferred and revised provisions for noncompliance with the revised annual training requirement.   *Transferred Provision: Cybersecurity Training Required for Certain State Contractors*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision requiring a contractor, including a subcontractor, officer, or employee of the contractor, who has access to a state computer system or database to complete a cybersecurity training program and revises that transferred provision to specify that such training is the cybersecurity training certified by the command under the bill's provisions. The bill retains the following related provisions, unchanged by the bill, to provide the following:   * the cybersecurity training program must be completed during the term of the contract and during any renewal period; and * required completion of a cybersecurity training program must be included in the terms of a contract awarded by a state agency.   Furthermore, in a retained provision, a contractor required to complete a cybersecurity training program certified by the command under the bill's provisions must verify completion of the program to the contracting state agency, and the person who oversees contract management for the agency must, not later than August 31 of each year, report the contractor's completion to the command. In a retained but unchanged provision, the person who oversees contract management for the agency must periodically review agency contracts to ensure compliance with these transferred provisions.  Cybersecurity Prevention, Response, and Recovery (Subchapter C)  C.S.H.B. 150 establishes a cybersecurity threat intelligence center, a cybersecurity incident response unit, and a digital forensics laboratory and also transfers to the bill's statutory framework from the Information Resources Management Act the provision regarding the required establishment of an information sharing and analysis organization. The bill requires the command to adopt policies and procedures necessary to enable these entities established under or transferred into the purview of the command to carry out their respective duties and purposes.  *Cybersecurity Threat Intelligence Center*  C.S.H.B. 150 requires the command to establish a cybersecurity threat intelligence center and requires the center to collaborate with federal cybersecurity intelligence and law enforcement agencies to achieve the center's purposes. The center, in coordination with the digital forensics laboratory established under the bill's provisions, must operate the information sharing and analysis organization, as established and transferred and revised by the bill, and provide strategic guidance to regional security operations centers, as established and transferred and revised by the bill, and to the cybersecurity incident response unit, established by the bill, to assist governmental entities in responding to a cybersecurity incident. The bill requires the chief of the command to employ a director for the center.  *Cybersecurity Incident Response Unit*  C.S.H.B. 150 requires the command to establish a dedicated cybersecurity incident response unit to carry out the following duties:   * detect and contain cybersecurity incidents in collaboration with the cybersecurity threat intelligence center; * engage in threat neutralization as necessary and appropriate, including removing malware, disallowing unauthorized access, and patching vulnerabilities in information resources technologies; * in collaboration with the digital forensics laboratory established by the bill, undertake mitigation efforts if sensitive personal information is breached during a cybersecurity incident; * 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; * assist in the restoration of information resources and information resources technologies after a cybersecurity incident and conduct post-incident monitoring; * in collaboration with the cybersecurity threat intelligence center and digital forensics laboratory, 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; * in collaboration with the cybersecurity threat intelligence center, the digital forensics laboratory, the Texas Division of Emergency Management, and other state agencies, conduct, support, and participate in cyber-related exercises; and * undertake any other activities necessary to carry out these duties.   The bill requires the chief of the command to employ a director for the cybersecurity incident response unit.  *Digital Forensics Laboratory*  C.S.H.B. 150 requires the command to establish a digital forensics laboratory to perform the following duties:   * in collaboration with the cybersecurity incident response unit, develop procedures to:   + preserve evidence of a cybersecurity incident, including logs and communication;   + document chains of custody; and   + timely notify and maintain contact with the appropriate law enforcement agencies investigating a cybersecurity incident; * 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; * conduct analyses of causes of cybersecurity incidents and of remediation options; * conduct assessments of the scope of harm caused by cybersecurity incidents, including data loss, compromised systems, and system disruptions; * provide information and training to state agencies and covered entities on producing reports required by regulatory and auditing bodies; * 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 * undertake any other activities necessary to carry out these duties.   The bill requires the chief of the command to employ a director for the digital forensics laboratory.  *Transferred Provision: Information Sharing and Analysis Organization*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision requiring the establishment by DIR of an information sharing and analysis organization and revises the provision to require the command to establish instead at least one such organization for the same purpose that is set out in current law, to remove the requirement that DIR provide administrative support to the organization, and to retain the following provisions of current law, unchanged by the bill:   * the requirement that a participant in the organization assert any exception available under state or federal law, including the exception under state public information law for information related to security or infrastructure issues for computers, in response to a request for public disclosure of information shared through the organization; and * the exception, with respect to information shared through the organization, from the applicability of state public information law regarding the voluntary disclosure of certain information when disclosure is not required under state public information law.   In addition, the bill revises the requirement under this transferred provision that DIR establish a framework for regional cybersecurity working groups to execute mutual aid agreements with a number of specified entities to assist with responding to a cybersecurity event in Texas. Accordingly, the bill revises that transferred requirement to provide the following:   * the command, instead of DIR, must establish the framework; * regional cybersecurity task forces, instead of the working groups, execute those agreements; and * in addition to executing the agreements, as provided under current law in the transferred provision, with state agencies, local governments, regional planning commissions, public and private institutions of higher education, and the private sector, the working groups may also execute agreements with the regional security operations centers established under provisions transferred and revised by the bill and with the cybersecurity incident response unit established under the bill's provisions.   Furthermore, references in this transferred provision to a cybersecurity event are replaced with references to a cybersecurity incident and references to working groups are replaced with references to the task forces. The bill retains applicably updated provisions of this transferred provision to provide the following:   * a task force may be established within the geographic area of a regional planning commission established under applicable state law; and * a 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.   Transferred Provisions: Reporting (Subchapter D)  *Cybersecurity Report and Report to the LBB*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provisions regarding the biennial cybersecurity report identifying preventive and recovery efforts the state can undertake to improve cybersecurity in Texas. The bill revises that transferred provision to make the command, rather than DIR, responsible for submitting the report 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. The bill also does the following:   * further revises that transferred provision to remove the requirement that the report include an evaluation of a program that provides an information security officer to assist small state agencies and local governments that are unable to justify hiring a full-time information security officer; and * adds a new reporting requirement in the transferred provision requiring the command to submit, not later than October 1 of each even-numbered year, a report to the LBB that prioritizes, for the purpose of receiving funding, state agency cybersecurity projects and requiring each state agency to coordinate with the command in order to implement this added requirement.   Furthermore, the bill changes the related transferred provision that, under current law, authorizes the redaction or withholding of certain information contained in the biennial cybersecurity report that is confidential under applicable state public information law or other state or federal law without the necessity of requesting a decision from the attorney general under applicable state public information law. Accordingly, the bill provides the following:   * the command, rather than DIR, is responsible for redacting or withholding such information; and * the disclosure of such information is not a voluntary disclosure for purposes of state public information law regarding the voluntary disclosure of certain information when disclosure is not required.   This related transferred provision, as revised by the bill, is also applicable to confidential information contained in the command's report to the LBB regarding state agency cybersecurity projects as added by the bill.  *Cybersecurity Incident Notifications by State Agency or Local Government*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision setting out a state agency's or local government's duty, by a specified deadline, to notify DIR or, if election data is involved, the secretary of state of a breach or suspected breach of system security and the introduction of ransomware into a computer, computer network, or computer system. Accordingly, the bill revises that transferred provision to do the following:   * require the state agency or local government, by the same specified deadline, to notify the command, including the command chief, rather than DIR's chief information security officer, of the breach or introduction of ransomware; * retain the requirement that the secretary of state be applicably notified of an applicable incident by the same specified deadline; and * require the state agency or local government to comply with all command rules, rather than DIR rules, in the event of such an incident.   The bill, with respect to the requirement for notification within a specified deadline applicable after the eradication, closure, and recovery from such an incident of the details of that incident, requires the state agency or local government to notify the command, including the command chief, of the details by that same deadline and removes the requirement that the chief information security officer of DIR be notified of those details. The bill clarifies that these transferred and revised notification provisions do not apply to an applicable incident that a local government must report to ERCOT. The bill replaces references in these transferred and revised notification provisions to a "security incident" with references to a "cybersecurity incident."  *Vulnerability Reports*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provisions requiring the information security officer of a state agency to prepare or have prepared a biennial report, including an executive summary of the report's findings, 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. The bill does the following:   * makes the command a recipient of an electronic copy of this vulnerability report on its completion; * removes DIR as a recipient of the electronic copy of this vulnerability report; * retains as recipients of an electronic copy of this vulnerability report the state auditor, the applicable agency's executive director, the applicable agency's designated information resources manager, and any other information technology security oversight group specifically authorized by the legislature to receive the report; and * retains the provision making a vulnerability report and any information or communication prepared or maintained for use in the preparation of such a report confidential and exempt from disclosure under state public information law.   In addition, under current law this transferred provision requires a state agency to prepare another summary, separate from the aforementioned executive summary and available to the public on request, of the agency's vulnerability report that does not contain any information the release of which might compromise the security of the state agency's or state agency contractor's computers, computer programs, computer networks, computer systems, printers, interfaces to computer systems, including mobile and peripheral devices, computer software, data processing, or electronically stored information. The bill removes the specification making that summary available to the public on request.  Cybersecurity Preparation and Planning (Subchapter E)  *Transferred Provisions: Designated Information Security Officer*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision requiring each state agency to designate an information security officer who reports to the agency's executive-level management, has authority over information security for the entire agency, to the extent feasible has information security duties as the officer's primary duties, and possesses the training and experience required to perform the duties established by DIR rules. The bill revises the latter required characteristic to provide that the security officer instead must possess the training and experience required to ensure the agency complies with requirements and policies established by the command.  *Transferred Provisions: Cybersecurity Risks and Incidents*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act each of the provisions regarding the requirement that DIR develop a plan to address cybersecurity risks and incidents in Texas and authorizing DIR to enter into an agreement with a national organization to support DIR's efforts in implementing the plan for which DIR lacks resources to address internally. The bill revises that provision to reflect that the command, rather than DIR, is responsible for developing that plan and entering into that agreement. The bill retains the provision, unchanged, setting out provisions that may be included in that agreement and revises the otherwise unchanged provisions requiring the command, rather than DIR, to seek to prevent unnecessary duplication of existing programs or efforts of the command or another state agency in implementing the prescribed agreement and to consult with institutions of higher education in Texas when appropriate based on an institution's expertise in addressing specific cybersecurity risks and incidents.  *Transferred Provisions: Information Security Plan*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision requiring each state agency to develop, and periodically update, an information security plan for protecting the security of the agency's information. The bill retains the transferred provision setting out the actions a state agency must take in developing the plan but revises one required action to reflect that the best practices for information security included in the plan are those developed by the command, rather than DIR, and to clarify that the requirement for the plan to include a written explanation of why the best practices are not sufficient for the agency's security is applicable if best practices are not applied. Furthermore, the bill does the following with respect to such a plan:   * revises the transferred requirement for each state agency to submit a copy of the agency's information security plan to DIR to require that the plan be submitted instead to the command; * revises the transferred provision regarding submission of the plan to replace the authorization for DIR, subject to available resources, to select a portion of the submitted security plans to be assessed by DIR in accordance with DIR rules with a provision that instead authorizes the command, subject to available resources, to select a portion of the submitted security plans to be assessed by the command in accordance with command policies; and * revises the requirement applicable to the biennial written report that evaluates information security for the state's information resources to do the following:   + add the speaker of the house of representatives as a report recipient;   + reflect that the command, rather than DIR, submits the report;   + specify that each standing committee receiving the report is a committee with primary jurisdiction over matters related to the command, rather than to DIR;   + specify that the command, rather than DIR, must consider applicable security plans, vulnerability reports, and other information regarding the security of the state's information resources in preparing the report; and   + remove the specification that, with respect to the required omission from any written copies of the report information that could expose specific vulnerabilities, such vulnerabilities are vulnerabilities in the security of the state's information resources.   *Ongoing Information Transmissions*  C.S.H.B. 150, with respect to the information received from state agencies by DIR under the Information Resources Management Act for purposes of preparing the biennial prioritized cybersecurity and legacy systems projects report, requires that such information be transmitted by DIR to the command on an ongoing basis.  *Transferred Provisions: Data Security Plan for Online and Mobile Applications*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provisions requiring each state agency implementing a website or mobile application that processes any sensitive personal or personally identifiable information or confidential information to submit a biennial data security plan for certain testing and review by DIR. The bill revises those transferred provisions as follows:   * each state agency must submit the biennial data security plan to the command, rather than DIR, to establish planned beta testing for the website or application and subject the website or application to a vulnerability and penetration test and address any vulnerability identified in the test; and * the command, rather than DIR, must review each submitted plan and make any recommendations for changes to the plan to the state agency as soon as practicable after the command reviews the plan.   *Transferred Provisions: Cybersecurity Council*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provisions requiring the state cybersecurity coordinator to establish and lead the state cybersecurity council, setting out the composition of the council membership, specifying the council's duties, and requiring the council to provide recommendations to the legislature. The bill revises those transferred provisions as follows:   * replaces the provision requiring the state cybersecurity coordinator to establish and lead the council with a provision requiring the command chief or the chief's designee to lead the council instead; * requires the council to include one additional member who is a DIR employee; * replaces the provision requiring that the additional members who must be representatives of institutions of higher education and private sector leaders be appointed by the state cybersecurity coordinator with a provision requiring that those additional members be appointed instead by the command chief; * replaces the provision requiring the state cybersecurity coordinator, in appointing representatives from institutions of higher education to the cybersecurity council, to consider appointing members of the Information Technology Council for Higher Education with a provision requiring that the command chief consider appointing those technology council members to the cybersecurity council; * adds a provision that sets staggered six-year terms for council members, with as near as possible to one-third of the members' terms expiring February 1 of each odd-numbered year; * with respect to the cybersecurity council's duty to consider the costs and benefits of establishing a computer readiness team to address cyber attacks, replaces the reference to "cyber attacks" with a reference to "cybersecurity incidents"; and * with respect to the cybersecurity council's duty to provide recommendations to the legislature on any legislation necessary to implement cybersecurity best practices and remediation strategies for the state, requires the command chief, in collaboration with the cybersecurity council, to provide such recommendations.   *Transferred Provisions: Recommendations*  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act the provision authorizing the state cybersecurity coordinator to implement any portion or all of the recommendations made by the Cybersecurity, Education, and Economic Development Council. The bill updates that transferred provision to remove the reference to expired state law, remove the reference to the specified council, and replace the provision authorizing the state cybersecurity coordinator to implement such recommendations with a provision authorizing the command chief to do so.  Transferred Provisions: Texas Volunteer Incident Response Team (Subchapter F)  C.S.H.B. 150 transfers to the bill's statutory framework from the Information Resources Management Act each of the provisions regarding the Texas Volunteer Incident Response Team that, under current law, provides rapid response assistance to a participating entity during a cybersecurity event. The bill retains the name of the team, replaces the references in those provisions to a cybersecurity event with references to a cybersecurity incident, and applicably revises each of those provisions to incorporate revisions reflecting that the command, instead of DIR, is responsible for establishing the team. Accordingly, the bill retains the following provisions, as transferred and applicably revised, that provide for the following general matters:   * eligibility criteria for participation as a volunteer member of the team; * contracts entered into between the command and each volunteer; * criminal history record information and other information required for each volunteer who accepts an invitation to become a volunteer; * deployment of the team in response to a cybersecurity incident that affects multiple participating entities or to the governor's declaration of a state of disaster caused by a cybersecurity event; * the cybersecurity council's review of and recommendations to the command regarding policies and procedures used by the command to implement provisions regarding the team; * the command's consultation with the cybersecurity council to implement and administer provisions regarding the team; * the status of a volunteer whereby the volunteer is not an agent, employee, or independent contractor of the state for any purpose, and the state is not liable to a volunteer for personal injury or property damage sustained by the volunteer arising from participation in the team; and * information written, produced, collected, assembled, or maintained by the command, a participating entity, the cybersecurity council or a volunteer in the implementation of these transferred provisions that, under specified conditions, is confidential and not subject to disclosure under state public information law.   Furthermore, with respect to the transferred provision authorizing the command to require a participating entity to enter into a contract as a condition for obtaining assistance from the team, the bill removes the requirement that the contract comply with the requirements of the Interagency Cooperation Act and the Interlocal Cooperation Act.  Transferred Provisions: Regional Security Operations Centers (Subchapter G)  C.S.H.B. 150 transfers to the bill's statutory framework from statutes governing the Texas computer network security system each of the provisions regarding regional network security centers that, under the current law as transferred, assist in providing cybersecurity support and network security to regional offices or locations for state agencies and other agencies eligible to participate in and receive services through the center. The bill renames the centers as regional security operations centers and applicably revises each of those transferred provisions to reflect that change and also incorporates revisions to each of those provisions reflecting that the command, rather than DIR, is responsible for establishing the centers. Accordingly, the bill retains the following provisions, as transferred and applicably revised, that provide for the following general matters:   * eligibility of participating entities; * establishment of the centers and the use of interagency contracts and interlocal contracts with an eligible participating entity; * locations and physical security of the centers; * managed security services the command may offer through a center; and * network security guidelines and standard operating procedures.   Furthermore, with respect to the retained and applicably revised provision regarding the locations and physical security of the centers, while current law in that provision requires DIR to partner with a university system or institution of higher education other than a public junior college in creating and operating such a center, the bill removes that as a requirement but authorizes the command to partner with another system or institution other than a public junior college. Additionally, with respect to the retained and applicably revised provision regarding the managed security services the command may offer through a center, the bill does the following with respect to the applicable terminology used in that provision:   * replaces the reference to "network security monitoring" with a reference to "cybersecurity monitoring"; * replaces references to "network security events" and to "network security threats" with references to "cybersecurity incidents" and "cybersecurity threats," respectively; * replaces a reference to "network security incidents" with a reference to "cybersecurity incidents"; and * replaces the reference to network security activity that exposes the state and residents of the state to risk with a reference to unauthorized activity that exposes the state and residents of the state to risk.     **Criteria for Sunset Review**  C.S.H.B. 150 includes an assessment of a state agency's cybersecurity practices using confidential information available from the command among the criteria the Sunset Advisory Commission and its staff must consider in determining whether a public need exists for the continuation of a state agency or its advisory committees or for the performance of the functions of the agency or its advisory committees.  **Education Code Provisions**  C.S.H.B. 150 amends the Education Code to include the command in the definition of "other agency of higher education" for purposes of the Higher Education Coordinating Act of 1965 and to include the command in the list of institutions and entities comprising The University of Texas System. The bill makes a number of conforming changes in the code reflecting the bill's creation of the command and reflecting the bill's transfers of statutes applicable to DIR's cybersecurity powers and duties under current law to the bill's new statutory framework governing the command.  **Transition Provisions**  C.S.H.B. 150 establishes that on the bill's effective date the command, organized as provided by the bill's provisions, is created with the powers and duties assigned by the bill, and requires the governor, as soon as practicable on or after the bill's effective date, to appoint the chief of the command.  C.S.H.B. 150 requires DIR to continue to perform duties and exercise powers under the Information Resources Management Act as that law existed immediately before the bill's effective date, until the date provided by the memorandum of understanding entered into under these transition provisions. Not later than December 31, 2026:   * all functions and activities performed by DIR that relate to cybersecurity under the bill's provisions are transferred to the command; * all DIR employees who primarily perform duties related to cybersecurity, including employees who provide administrative support for those services under the bill's provisions, become employees of the command, but continue to work in the same physical location unless moved in accordance with the memorandum of understanding entered into as provided by these bill provisions; * a rule or form adopted by DIR that relates to cybersecurity under the bill's provisions is a rule or form of the command and remains in effect until changed by the command; * a reference in law to DIR that relates to cybersecurity under the bill's provisions means the command; * a contract negotiation for a contract specified as necessary to accomplish the goals and duties of the command in the memorandum of understanding required under these transition provisions of the bill or other proceeding involving DIR that is related to cybersecurity under the bill's provisions is transferred without change in status to the command, and the command assumes, without a change in status, the position of DIR in a negotiation or proceeding relating to cybersecurity to which DIR is a party; * all money, leases, rights, and obligations of DIR related to cybersecurity under the bill's provisions are transferred to the command; * contracts specified as necessary to accomplish the goals and duties of the command in the applicable memorandum of understanding are transferred to the command; * all property, including records, in DIR custody related to cybersecurity under the bill's provisions becomes property of the command, but stays in the same physical location unless moved in accordance with the steps and methods specified by the bill's transition provisions; and * all funds appropriated by the legislature to DIR for purposes related to cybersecurity, including funds for providing administrative support under the bill's provisions, are transferred to the command.   C.S.H.B. 150 requires DIR, in collaboration with the chief of the command, and the board of regents of The University of Texas System, not later than January 1, 2026, to enter into a memorandum of understanding relating to the transfer of powers and duties from DIR to the Texas command as provided by the bill's provisions. The memorandum must include the following:   * a timetable and specific steps and methods for the transfer of all powers, duties, obligations, rights, contracts, leases, records, real or personal property, and unspent and unobligated appropriations and other funds relating to the administration of the powers and duties as provided by the bill; * measures to ensure against any unnecessary disruption to cybersecurity operations during the transfer process; and * a provision that the terms of any memorandum of understanding entered into related to the transfer remain in effect until the transfer is completed. |
| **EFFECTIVE DATE**  September 1, 2025. |
| **COMPARISON OF INTRODUCED AND SUBSTITUTE**  Definitions  The substitute changes the introduced version's definition of "cybersecurity." Whereas the introduced defined that term to mean the measures taken to protect a computer, computer network, computer system, or other technology infrastructure against certain unauthorized actions, the substitute revises the definition to mean the measures taken for a computer, computer network, computer system, or other technology infrastructure to protect against, respond to, and recover from those same unauthorized actions.  The substitute changes the introduced version's definition of "state agency" to remove from the definition a department, commission, board, office, or other agency that is in the legislative branch of state government and that was created by the constitution or a statute.  Establishment and Purpose  The substitute omits the introduced version's provision that made the command, in collaboration with DIR, responsible for establishing appropriate cybersecurity standards.  The substitute includes a provision absent from the introduced making the command responsible for developing cyber threat intelligence, monitoring information systems to detect and warn entities of cyber attacks, proactively searching for cyber threats to critical infrastructure and state systems, developing and executing cybersecurity incident responses, and conducting digital forensics of cybersecurity incidents to support law enforcement and attribute the incidents.  The substitute includes a provision absent from the introduced making the command responsible for receiving all cybersecurity incident reports from state agencies and covered entities.  General Powers and Duties  The substitute includes a provision absent from the introduced requiring the command to respond to cybersecurity reports received under the bill's applicable provisions and other reports as appropriate.  The substitute includes a provision absent from the introduced requiring the command to collaborate with federal agencies to protect against, respond to, and recover from cybersecurity incidents.  Whereas the introduced version authorized the command, as part of its general powers and duties, to adopt and enforce policies necessary to carry out the bill's provisions, the substitute authorizes the command, as part of its general powers and duties, to instead adopt and enforce rules to carry out the bill's provisions.  The substitute includes a provision absent from the introduced authorizing the command to solicit and accept gifts, grants, donations, or loans from and contract with any entity to accomplish the command's duties.  Rules  Whereas the introduced version authorized the governor to adopt rules necessary for carrying out the bill's provisions, the substitute omits that provision and authorizes the command chief instead to adopt the necessary rules.  Application of Sunset Act  The substitute changes the bill provision establishing the date on which the command is set to be abolished under the Texas Sunset Act from September 1, 2035, as specified in the introduced, to September 1, 2031.  Cybersecurity Threat Intelligence Center  The substitute and the introduced both provide for the establishment of a cybersecurity threat intelligence center, but the bill provisions differ as follows:   * the substitute includes a provision absent from the introduced requiring the center to collaborate with federal cybersecurity intelligence and law enforcement agencies to achieve the purposes of the bill provision establishing the center; * the substitute requires the center to coordinate certain activities prescribed in the bill provision with the digital forensics laboratory, which is established by both the introduced and substitute, and omits the provision from the introduced version that required the center to coordinate those prescribed activities with DIR; * the substitute includes a provision absent from the introduced that requires the cybersecurity threat intelligence center to provide strategic guidance to regional security operations centers and the cybersecurity incident response unit to assist governmental entities in responding to a cybersecurity incident; * the substitute omits the introduced version's provision that required the cybersecurity threat intelligence center to use those regional security operations centers and the cybersecurity incident response unit to assist governmental entities in responding to such an incident; and * whereas the introduced authorized the command chief to employ a director for the cybersecurity threat intelligence center, the substitute requires the command chief to do so.   Cybersecurity Incident Response Unit  The substitute and the introduced both provide for the establishment of a cybersecurity incident response unit for the same purposes, including for the purposes of engaging in threat neutralization. However, the substitute includes a specification in that bill provision absent from the introduced clarifying that the threat neutralization is as necessary and appropriate.  Information Sharing and Analysis Organization  The substitute and the introduced both provide for the establishment of an information sharing and analysis organization, but the substitute requires the establishment of at least one such organization while the introduced requires the establishment of a single organization.  Cybersecurity Incident Notification by State Agency or Local Government  The substitute includes a provision absent from the introduced that transfers to the bill's newly created statutory framework another provision from the Information Resources Management Act providing for a state agency's or local government's duty, by a specified deadline, to notify DIR or, if election data is involved, the secretary of state of a breach or suspected breach of system security and the introduction of ransomware into a computer, computer network, or computer system. The substitute accordingly revises that transferred provision to do the following:   * require the state agency or local government, by the same specified deadline, to notify the command, including the command chief, rather than DIR's chief information security officer, of the breach or introduction of ransomware; * retain the requirement that the secretary of state be applicably notified of an applicable incident by the same specified deadline; * require the state agency or local government to comply with all command rules, rather than DIR rules, in the event of such an incident; * with respect to the requirement for notification, within a specified deadline, applicable after the eradication, closure, and recovery from such an incident of the details of that incident, require the state agency or local government to notify the command, including the command chief, of the details by that same deadline and remove the requirement that the chief information security officer of DIR be notified of those details; * clarify that these transferred and revised notification provisions do not apply to an applicable incident that a local government must report to ERCOT; and * replace references in these transferred and revised notification provisions to a "security incident" with references to a "cybersecurity incident."   Regional Security Operations Centers Services and Support  Whereas both the substitute and the introduced transfer to the bill's newly created statutory framework certain provisions currently governing the regional network security centers operated under the Texas computer network security system, among them a provision regarding management of the services that may be offered under the transferred provisions with respect to certain terminology used in reference to those services, the substitute, but not the introduced, includes the following revisions to that provision:   * the substitute replaces the reference to "network security monitoring" with a reference to "cybersecurity monitoring"; * the substitute replaces references to "network security events" and to "network security threats" with references to "cybersecurity incidents" and "cybersecurity threats," respectively; * the substitute replaces "network security incidents" with "cybersecurity incidents;" and * the substitute replaces the reference to network security activity that exposes the state and residents of the state to risk with a reference to unauthorized activity that exposes the state and residents of the state to risk.   Transition Provisions  In the bill's transition provision, the introduced provided that the chief information security officer of DIR becomes the chief of the command, as specified in the introduced version's statutory provisions, on the bill's effective date. However, the substitute in the transition provision requires the governor to appoint the chief of the command, as specified in the substitute's statutory provisions, as soon as practicable on or after the bill's effective date.  The substitute and the introduced both set out a transition provision requiring DIR and the board of regents of The University of Texas System to enter into a memorandum of understanding relating to the applicable transfer of powers and duties from DIR to the command. However, the substitute includes a provision absent from the introduced specifying that DIR must collaborate with the command chief in entering the memorandum of understanding.  Whereas the introduced provided in a transition provision for the transfer of all contracts related to cybersecurity from DIR to the command, the substitute omits that provision and provides for the transfer instead of only the contracts specified as necessary to accomplish the goals and duties of the command in the memorandum of understanding. Whereas both the substitute and the introduced provide in a transition provision for the transfer of a contract negotiation that is related to cybersecurity without change in status, the substitute includes a specification absent from the introduced establishing that the contract negotiation is for a contract specified as necessary to accomplish the goals and duties of the command in the memorandum of understanding. |
|  |
|  |
|  |
|  |
|  |