

1-1 By: Paxton S.B. No. 1204
 1-2 (In the Senate - Filed February 24, 2023; March 9, 2023,
 1-3 read first time and referred to Committee on Business & Commerce;
 1-4 April 6, 2023, reported adversely, with favorable Committee
 1-5 Substitute by the following vote: Yeas 11, Nays 0; April 6, 2023,
 1-6 sent to printer.)

1-7 COMMITTEE VOTE

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

1-20 COMMITTEE SUBSTITUTE FOR S.B. No. 1204 By: Campbell

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

1-23 relating to state and local government information technology and
 1-24 information security.

1-25 BE IT ENACTED BY THE LEGISLATURE OF THE STATE OF TEXAS:

1-26 SECTION 1. Section 2054.003, Government Code, is amended by
 1-27 adding Subdivisions (11) and (11-a) to read as follows:

1-28 (11) "Peer-to-peer payment" means a transfer of funds
 1-29 using a peer-to-peer payment system.

1-30 (11-a) "Peer-to-peer payment system" means a digital
 1-31 non-credit card system used for transferring funds from one party
 1-32 to another.

1-33 SECTION 2. The heading to Section 2054.0594, Government
 1-34 Code, is amended to read as follows:

1-35 Sec. 2054.0594. INFORMATION SHARING AND ANALYSIS
 1-36 ORGANIZATIONS [~~ORGANIZATION~~].

1-37 SECTION 3. Section 2054.0594, Government Code, is amended
 1-38 by amending Subsections (a), (b), and (c) and adding Subsection
 1-39 (a-1) to read as follows:

1-40 (a) The department shall establish an intrastate
 1-41 information sharing and analysis organization to provide a forum
 1-42 for state agencies, local governments, public and private
 1-43 institutions of higher education, and [~~the~~] private sector entities
 1-44 in this state to share information regarding cybersecurity threats,
 1-45 best practices, and remediation strategies.

1-46 (a-1) The department may establish an interstate
 1-47 information sharing and analysis organization to provide a forum
 1-48 for states to share information regarding cybersecurity threats,
 1-49 best practices, and remediation strategies.

1-50 (b) The department shall provide administrative support to
 1-51 each [~~the~~] information sharing and analysis organization
 1-52 established under this section.

1-53 (c) A participant in an [~~the~~] information sharing and
 1-54 analysis organization established under this section shall assert
 1-55 any exception available under state or federal law, including
 1-56 Section 552.139, in response to a request for public disclosure of
 1-57 information shared through the organization. Section 552.007 does
 1-58 not apply to information described by this subsection.

1-59 SECTION 4. Section 2054.060, Government Code, is amended by
 1-60 adding Subsection (a-1) to read as follows:

2-1 (a-1) Unless expressly prohibited by other law or a rule
 2-2 adopted by the state agency, a state agency shall accept a digital
 2-3 signature included in any communication or payment electronically
 2-4 delivered to the state agency.

2-5 SECTION 5. The heading to Section 2054.068, Government
 2-6 Code, is amended to read as follows:

2-7 Sec. 2054.068. STATE AGENCY INFORMATION TECHNOLOGY
 2-8 INFRASTRUCTURE: INFORMATION SECURITY RATING; AUDIT; REPORT.

2-9 SECTION 6. Section 2054.068, Government Code, is amended by
 2-10 amending Subsections (b), (c), and (d) and adding Subsections
 2-11 (c-1), (c-2), (c-3), (c-4), (e-1), (e-2), and (e-3) to read as
 2-12 follows:

2-13 (b) The department shall collect from each state agency
 2-14 information on the status and condition of the agency's information
 2-15 technology infrastructure, including ~~[information regarding]~~:

2-16 (1) information on the agency's information security
 2-17 program;

2-18 (2) an inventory of the agency's servers, mainframes,
 2-19 cloud services, and other information technology equipment;

2-20 (3) identification information for ~~[of]~~ vendors that
 2-21 operate and manage the agency's information technology
 2-22 infrastructure; ~~[and]~~

2-23 (4) the results of the information security assessment
 2-24 required by Section 2054.515; and

2-25 (5) any additional related information requested by
 2-26 the department.

2-27 (c) A state agency shall provide the information required by
 2-28 Subsection (b) to the department not later than June 1 of each
 2-29 even-numbered year ~~[according to a schedule determined by the~~
 2-30 ~~department]~~.

2-31 (c-1) The department shall assign to each state agency,
 2-32 other than an institution of higher education, one of the following
 2-33 information security ratings based on the agency's information
 2-34 security risk profile:

2-35 (1) above average;

2-36 (2) average; or

2-37 (3) below average.

2-38 (c-2) In assigning an information security rating to a state
 2-39 agency under Subsection (c-1), the department shall consider:

2-40 (1) the information the agency provides under
 2-41 Subsection (b);

2-42 (2) the agency's comprehensive information security
 2-43 risk position relative to the agency's risk environment; and

2-44 (3) any additional document or information the
 2-45 department requests from the agency.

2-46 (c-3) The department:

2-47 (1) shall develop options and make recommendations for
 2-48 improvements in the information security maturity of any state
 2-49 agency assigned an information security rating of below average
 2-50 under Subsection (c-1); and

2-51 (2) may assist any state agency in determining whether
 2-52 additional security measures would increase the agency's
 2-53 information security maturity.

2-54 (c-4) The department may audit the information security and
 2-55 technology of any state agency assigned an information security
 2-56 rating under Subsection (c-1) or contract with a vendor to perform
 2-57 the audit. The department shall make available on request by any
 2-58 person listed in Subsection (d) the results of an audit conducted
 2-59 under this subsection.

2-60 (d) Not later than November 15 of each even-numbered year,
 2-61 the department shall submit to the governor, chair of the house
 2-62 appropriations committee, chair of the senate finance committee,
 2-63 speaker of the house of representatives, lieutenant governor, and
 2-64 staff of the Legislative Budget Board:

2-65 (1) a consolidated report of the information submitted
 2-66 by state agencies under Subsection (b); and

2-67 (2) any department recommendations relevant to and
 2-68 necessary for improving this state's information technology
 2-69 infrastructure and information security.

3-1 (e-1) The department shall compile a summary of the
 3-2 consolidated report required under Subsection (d) and make the
 3-3 summary available to the public. The summary may not disclose any
 3-4 confidential information.

3-5 (e-2) The consolidated report required under Subsection (d)
 3-6 and all information a state agency submits to substantiate or
 3-7 otherwise related to the report are confidential and not subject to
 3-8 disclosure under Chapter 552. The state agency or the department
 3-9 may redact or withhold information as confidential under Chapter
 3-10 552 without requesting a decision from the attorney general under
 3-11 Subchapter G, Chapter 552.

3-12 (e-3) Following review of the consolidated report, the
 3-13 Legislative Budget Board may direct the department to select for
 3-14 participation in a statewide technology center established under
 3-15 Subchapter L any state agency assigned an information security
 3-16 rating under Subsection (c-1). The department shall notify each
 3-17 selected state agency of the agency's selection as required by
 3-18 Section 2054.385. The department is not required to conduct the
 3-19 cost and requirements analysis under Section 2054.384 for a state
 3-20 agency selected for participation under this subsection. This
 3-21 subsection expires September 1, 2027.

3-22 SECTION 7. Subchapter C, Chapter 2054, Government Code, is
 3-23 amended by adding Section 2054.0692 to read as follows:

3-24 Sec. 2054.0692. GUIDANCE ON USE OF DISTRIBUTED LEDGER
 3-25 TECHNOLOGY. (a) The department shall develop and disseminate
 3-26 guidance for the use of distributed ledger technology, including
 3-27 blockchain, among state agencies.

3-28 (b) The guidance must include a framework or model for
 3-29 deciding if distributed ledger technology is appropriate for
 3-30 meeting a state agency's needs. The guidance may include:

3-31 (1) examples of potential uses of distributed ledger
 3-32 technology by an agency;

3-33 (2) sample procurement and contractual language; and

3-34 (3) information on educational resources for agencies
 3-35 on distributed ledger technology.

3-36 SECTION 8. Section 2054.095(b), Government Code, is amended
 3-37 to read as follows:

3-38 (b) Except as otherwise modified by the Legislative Budget
 3-39 Board or the governor, instructions under Subsection (a) must
 3-40 require each state agency's strategic plan to include:

3-41 (1) a description of the agency's information
 3-42 resources management organizations, policies, and practices,
 3-43 including the extent to which the agency uses its project
 3-44 management practices, as defined by Section 2054.152;

3-45 (2) a description of how the agency's information
 3-46 resources programs support and promote its mission, goals, and
 3-47 objectives and the goals and policies of the state strategic plan
 3-48 for information resources; ~~and~~

3-49 (3) a description of customer service technology,
 3-50 including telephone systems and websites, that improves customer
 3-51 service performance; and

3-52 (4) other planning components that the department may
 3-53 prescribe.

3-54 SECTION 9. Section 2054.1115, Government Code, is amended
 3-55 by amending Subsection (a) and adding Subsection (c) to read as
 3-56 follows:

3-57 (a) A state agency or local government that uses the state
 3-58 electronic Internet portal may use electronic payment methods,
 3-59 including the acceptance of peer-to-peer payments, credit cards,
 3-60 and debit cards, for:

3-61 (1) point-of-sale transactions, including:

3-62 (A) person-to-person transactions;

3-63 (B) transactions that use an automated process to
 3-64 facilitate a person-to-person transaction; and

3-65 (C) transactions completed by a person at an
 3-66 unattended self-standing computer station using an automated
 3-67 process;

3-68 (2) telephone transactions; or

3-69 (3) mail transactions.

4-1 (c) The department shall identify the three most commonly
4-2 used peer-to-peer payment systems and post a list containing those
4-3 systems in a conspicuous location on the department's Internet
4-4 website. The department shall biennially review and, if necessary,
4-5 update the list required under this subsection.

4-6 SECTION 10. Section 2054.136, Government Code, is amended
4-7 to read as follows:

4-8 Sec. 2054.136. DESIGNATED INFORMATION SECURITY OFFICER.

4-9 (a) Each state agency shall designate an information security
4-10 officer who:

4-11 (1) reports to the agency's executive-level
4-12 management;

4-13 (2) has authority over information security for the
4-14 entire agency;

4-15 (3) possesses the training and experience required to
4-16 perform the duties required by department rules; and

4-17 (4) to the extent feasible, has information security
4-18 duties as the officer's primary duties.

4-19 (b) An employee designated under Subsection (a) may be
4-20 designated to serve as a joint information security officer by two
4-21 or more state agencies. The department must approve the joint
4-22 designation.

4-23 SECTION 11. Subchapter L, Chapter 2054, Government Code, is
4-24 amended by adding Section 2054.393 to read as follows:

4-25 Sec. 2054.393. MARKETING OF SERVICES. (a) Notwithstanding
4-26 Section 2113.011 and subject to Subsection (b), the department may
4-27 use appropriated money to market to state agencies and local
4-28 governments shared information resources technology services
4-29 offered by the department under this subchapter, including data
4-30 center, disaster recovery, and cybersecurity services.

4-31 (b) An expenditure of money under this section must be
4-32 approved by the executive director.

4-33 SECTION 12. The heading to Section 2054.515, Government
4-34 Code, is amended to read as follows:

4-35 Sec. 2054.515. STATE AGENCY INFORMATION SECURITY
4-36 ASSESSMENT [~~AND REPORT~~].

4-37 SECTION 13. Sections 2054.515(a), (c), and (d), Government
4-38 Code, are amended to read as follows:

4-39 (a) At least once every two years, each state agency shall
4-40 conduct an information security assessment of the agency's[+
4-41 [~~(1)~~] information resources systems, network systems,
4-42 digital data storage systems, digital data security measures, and
4-43 information resources vulnerabilities[~~, and~~

4-44 [~~(2)~~] ~~data governance program with participation from~~
4-45 ~~the agency's data management officer, if applicable, and in~~
4-46 ~~accordance with requirements established by department rule].~~

4-47 (c) Each state agency shall complete the information
4-48 security assessment in consultation with the department or the
4-49 vendor the department selects and submit the results of the
4-50 assessment to the department in accordance with Section 2054.068(b)
4-51 [The department by rule shall establish the requirements for the
4-52 information security assessment and report required by this
4-53 section].

4-54 (d) All [~~The report and all~~] documentation related to the
4-55 information security assessment is [~~and report are~~] confidential
4-56 and not subject to disclosure under Chapter 552. The state agency
4-57 or department may redact or withhold the information as
4-58 confidential under Chapter 552 without requesting a decision from
4-59 the attorney general under Subchapter G, Chapter 552.

4-60 SECTION 14. Section 2054.577(c), Government Code, is
4-61 amended to read as follows:

4-62 (c) Money in the fund:

4-63 (1) may be used to improve and modernize state agency
4-64 information resources, including legacy system projects and
4-65 cybersecurity projects; [~~and~~]

4-66 (2) may be used to mitigate a breach or suspected
4-67 breach of system security, as defined by Section 521.053, Business
4-68 & Commerce Code, or the introduction of ransomware, as defined by
4-69 Section 33.023, Penal Code, into a computer, computer network, or

5-1 computer system at a state agency;
5-2 (3) may not be used to replace money appropriated to a
5-3 state agency for the purposes of operating and maintaining state
5-4 agency information resources or reduce the amount of money
5-5 appropriated to a state agency for those purposes; and
5-6 (4) may not be used to pay a person who commits the
5-7 offense of electronic data tampering punishable under Section
5-8 33.023, Penal Code.

5-9 SECTION 15. Chapter 2056, Government Code, is amended by
5-10 adding Section 2056.0023 to read as follows:

5-11 Sec. 2056.0023. INFORMATION TECHNOLOGY MODERNIZATION PLAN.

5-12 (a) As part of the strategic plan required under Section 2056.002,
5-13 a state agency shall include an information technology
5-14 modernization plan that outlines the manner in which the agency
5-15 intends to transition its information technology and data-related
5-16 services and capabilities into a more modern, integrated, secure,
5-17 and effective technological environment.

5-18 (b) The Department of Information Resources may provide a
5-19 template for the information technology modernization plan
5-20 required by this section.

5-21 SECTION 16. The following provisions are repealed:

5-22 (1) Section 2054.068(f), Government Code; and

5-23 (2) Section 2054.515(b), Government Code, as amended
5-24 by Chapters 567 (S.B. 475) and 856 (S.B. 800), Acts of the 87th
5-25 Legislature, Regular Session, 2021.

5-26 SECTION 17. The Department of Information Resources shall
5-27 develop and disseminate the guidance and decision model required by
5-28 Section 2054.0692, Government Code, as added by this Act, not later
5-29 than December 1, 2023.

5-30 SECTION 18. This Act takes effect September 1, 2023.

5-31

* * * * *