By: Bhojani H.B. No. 1201

A BILL TO BE ENTITLED

AN ACT

relating to required reporting of rogue artificial intelligence incidents; authorizing civil penalties.

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

SECTION 1. Chapter 2054, Government Code, is amended by adding Subchapter T to read as follows:

SUBCHAPTER T. ROGUE ARTIFICIAL INTELLIGENCE INCIDENT REPORTING

Sec. 2054.751. DEFINITIONS. (a) In this subchapter:

(1) "Computer," "computer network," "computer system," "effective consent," and "owner" have the meanings assigned by Section 33.01, Penal Code.

(2) "Frontier developer" means a person who develops or directs the training of a frontier model. The term does not include a person solely because the person purchases, licenses, integrates, or deploys a frontier model developed by another person.

(3) "Frontier model" means an artificial intelligence system, or the model on which the system is based, that is trained on a broad set of data, designed for generality of output, and adaptable to a wide range of distinctive tasks, and that is trained using a quantity of computing power greater than 10 to the 25th power integer or floating-point operations.

(4) "Rogue artificial intelligence incident" means an event in which a frontier model, at any stage of development or use:

(A) accesses a computer, computer network, or computer system that the frontier developer does not own or control, without the owner's effective consent;

(B) acts to disable, circumvent, or deceive a human oversight mechanism, or to prevent an authorized person from rejecting, modifying, overriding, or terminating the decisions, proposed actions, or ongoing actions of the frontier model;

(C) without the owner's effective consent, modifies, deletes, or discloses data or takes an action affecting an information system; or

(D) takes an autonomous action that exceeds the instructions given to, or permissions granted to, the frontier model and causes or creates a substantial and reasonably foreseeable risk of:

(i) death or serious bodily injury, as defined by Section 1.07, Penal Code;

(ii) substantial loss of or damage to property;

(iii) substantial disruption of critical infrastructure;

(iv) substantial disruption of the provision of a government service; or

(v) substantial compromise of the security of confidential information or an information system.

Sec. 2054.752. APPLICABILITY. (a) This subchapter applies to a frontier developer with respect to a rogue artificial intelligence incident involving a frontier model developed by the

frontier developer or an artificial intelligence system using that model if:

(1) the model or system is developed, trained, or tested in this state;

(2) the model or system is commercially deployed in this state; or

(3) the incident occurs in this state or involves a person, computer, computer network, computer system, or information system located in this state.

(b) This subchapter applies to a frontier developer without regard to the state or country in which the developer is headquartered, to the extent application is consistent with the United States Constitution and federal law.

(c) This subchapter does not apply to an output from an artificial intelligence system that is merely inaccurate, incomplete, or otherwise deficient, unless the output otherwise meets the definition of a rogue artificial intelligence incident, as described by Section 2054.751(a)(4).

Sec. 2054.753. REPORTING REQUIREMENT. (a) A frontier developer subject to this subchapter shall submit a report of a rogue artificial intelligence incident to the department:

(1) not later than 24 hours after discovering an incident that poses an imminent threat of substantial harm to the health or safety of one or more individuals; or

(2) not later than 72 hours after discovering any other rogue artificial intelligence incident.

(b) A frontier developer reporting under Subsection (a)

shall also notify an appropriate law enforcement or public safety agency if necessary to address the threat.

(c) A report must include:

(1) the date of the incident and the date of discovery;

(2) an explanation of why the incident is reportable, identifying each applicable paragraph of Section 2054.751(a)(4);

(3) a brief description of the incident; and

(4) whether the incident occurred during development, training, testing, internal operation, or external deployment.

(d) The department shall maintain a secure electronic system for submitting reports under this subchapter. The system must also accept a voluntary report from any person of a suspected rogue artificial intelligence incident involving a frontier model developed, trained, tested, or commercially deployed in this state or causing or creating a substantial and reasonably foreseeable risk of material harm in this state.

(e) The reporting of a rogue artificial intelligence incident is not an admission of liability.

(f) A report submitted under this subchapter, and information identifying the person who submitted it, are confidential and not subject to disclosure under Chapter 552.

Sec. 2054.754. ANNUAL SUMMARY. (a) Not later than December 1 of each year, the department shall publish on the department's Internet website and submit to the governor, the lieutenant governor, the speaker of the house of representatives, and the standing committee of each house of the legislature having primary jurisdiction over information resources an aggregate summary of

rogue artificial intelligence incidents reported during the preceding state fiscal year.

(b) The summary must include, to the extent practicable:

(1) the number and general categories of incidents under each paragraph of Section 2054.751(a)(4);

(2) the stage of development, training, testing, internal operation, or external deployment in which incidents occurred; and

(3) general categories of harm and risk.

(c) The summary may include recommendations for legislative action.

(d) The summary may not disclose confidential information under Section 2054.753(f).

Sec. 2054.755. PROHIBITION ON RETALIATION. An employer in this state may not suspend or terminate the employment or contract of, or take other adverse personnel action against, an employee, former employee, or contractor who in good faith:

(1) reports conduct the individual believes violates this subchapter; or

(2) provides information or otherwise assists in an investigation or proceeding concerning an alleged violation of this subchapter.

Sec. 2054.756. ENFORCEMENT. (a) A violation of this subchapter is subject to enforcement by the attorney general.

(b) The attorney general may bring an action in the name of this state in a district court in Travis County to recover a civil penalty under Subsection (c) or to obtain injunctive relief.

(c) A frontier developer is liable to this state for a civil penalty of:

(1) not less than $10,000 and not more than $100,000 for each failure to submit a timely report required by this subchapter, or for each violation of Section 2054.755; and

(2) not less than $100,000 and not more than $1,000,000 for each incident the developer knowingly conceals from the department or each materially false or misleading report the developer knowingly submits.

(d) In determining the amount of a civil penalty, the court shall consider the seriousness of the incident, the length of any reporting delay, the developer's history of violations and good faith efforts to comply, and any other matter that justice may require.

(e) In determining whether a frontier developer has violated this subchapter, the attorney general shall consult with the department, and the department shall provide the attorney general with reports and technical information reasonably necessary for that determination.

(f) Information obtained by the attorney general or the department in connection with an investigation or enforcement action under this subchapter, including the identity of a person who reports an alleged violation, is confidential and not subject to disclosure under Chapter 552, except as necessary for an investigation or enforcement action under this subchapter.

Sec. 2054.757. RULES. The department shall adopt rules necessary to implement this subchapter.

SECTION 2. Not later than December 1, 2027, the Department of Information Resources shall adopt the rules and establish the reporting system required by Subchapter T, Chapter 2054, Government Code, as added by this Act.

SECTION 3. (a) Section 2054.753, Government Code, as added by this Act, applies only to a rogue artificial intelligence incident that a frontier developer discovers on or after January 1, 2028.

(b) Notwithstanding Section 2054.754, Government Code, as added by this Act, the Department of Information Resources is not required to publish or submit a summary under that section before December 1, 2028. The summary due December 1, 2028, must cover rogue artificial intelligence incidents reported during the period beginning January 1, 2028, and ending August 31, 2028.

(c) Section 2054.755, Government Code, as added by this Act, applies only to an adverse action taken on or after the effective date of this Act.

SECTION 4. This Act takes effect September 1, 2027.