BILL ANALYSIS

BACKGROUND AND PURPOSE

Artificial Intelligence systems have grown in size and usage over the past few years, with many industries adopting this technology to help with professional workflow. The Texas Tribune has reported that more than a third of state agencies are currently using AI, including in roles of customer service, translation, and cybersecurity. However, many people are unaware of how to leverage AI technology in ways that are accurate and useful to their needs, leading to the risk of this technology being used incorrectly.

H.B. 3512 seeks to address these issues by requiring applicable state employees to take AI literacy training in a manner similar to the current cybersecurity training required for state employees. The bill requires the Department of Information Resources to certify and periodically update the AI training and applicable employees to annually complete the training.

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 Department of Information Resources in SECTION 9 of this bill.

ANALYSIS

H.B. 3512 amends the Government Code to require the Department of Information Resources (DIR), in consultation with interested persons and the cybersecurity council established by the state cybersecurity coordinator, to do the following annually:

- certify at least five artificial intelligence (AI) training programs for state and local government employees;
- update standards for maintenance of certification by the AI training programs; and
- ensure that the AI training programs are equal in length to the cybersecurity training programs certified under current law.

The bill requires an AI training program, in order to be certified by DIR, to focus on forming an understanding of how AI technology may be used in relation to a state employee's responsibilities and duties and to teach best practices on literacy in deploying and operating the AI technologies. The bill authorizes DIR to identify and certify training programs provided by state agencies and local governments that satisfy those training requirements and to contract with an independent third party to certify an AI training program. The bill requires DIR to annually publish the list of certified AI training programs on the DIR website and to adopt the rules necessary to develop and implement the AI training programs as soon as practicable after the bill's effective date.

H.B. 3512 includes AI training and training programs in the scope of the following provisions currently applicable with respect to cybersecurity training and training programs:

- requirements relating to a local government's duty to include a written certification of its compliance with such a program with a grant application submitted under provisions relating to governmental planning;
- requirements for certain state agency and local government employees and elected or appointed officers of the agency or with access to a local government computer system or database to annually complete such a training program;
- requirements relating to the duty of the governing body of such a local government and the executive head of such a state agency to verify and report on completion of such a training program by applicable employees; and
- the requirement for the strategic plan of a state agency to include a written certification of the agency's compliance with the training unless modified by the Legislative Budget Board and the governor's office.

H.B. 3512 amends the Education Code to include AI training in the scope of the provision requiring only the cybersecurity coordinator of a school district to complete cybersecurity training on an annual basis and any other district employee required to complete the training to do so as determined by the district, in consultation with the district's cybersecurity coordinator.

EFFECTIVE DATE

September 1, 2025.