BILL ANALYSIS

H.B. 3185
By: Metcalf
Delivery of Government Efficiency
Committee Report (Unamended)

BACKGROUND AND PURPOSE

The bill author has informed the committee that law enforcement agencies currently face delays in obtaining crucial data regarding cybercrime investigations because subpoenas often require court approval and cooperation from out-of-state internet service providers. The bill author has further informed the committee that cybercriminals exploit these delays by deleting or altering records before they can be retrieved, meaning that critical evidence can disappear before being legally accessed in an investigation.

H.B. 3185 seeks to reduce bureaucratic delays and strengthen law enforcement's ability to combat cybercrime and protect victims by allowing prosecuting attorneys to issue administrative subpoenas for specific subscriber and transactional records, such as IP addresses, account details, and payment information. The bill ensures confidentiality of collected data and aligns cybercrime investigations with existing procedures for Internet crimes against children cases.

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 this bill does not expressly grant any additional rulemaking authority to a state officer, department, agency, or institution.

ANALYSIS

H.B. 3185 amends the Government Code to authorize a prosecuting attorney to issue and cause to be served an administrative subpoena that requires the production of records or other documentation as described by the bill's provisions if the subpoena relates to an investigation of a cybercrime and there is reasonable cause to believe that the Internet or electronic service account provided through an electronic communication service or remote computing service has been used in the commission of a cybercrime. The bill defines "cybercrime" as any of the following Penal Code offenses committed using an Internet website or an electronic service account provided through an electronic communication service or remote computing service:

- theft offenses;
- fraud offenses;
- computer crime offenses;
- telecommunications crime offenses;
- money laundering offenses;
- insurance fraud offenses;
- disorderly conduct and related offenses;
- organized crime offenses;
- racketeering and unlawful debt collection offenses; and

- terroristic offenses.

H.B. 3185 does the following with respect to an administrative subpoena issued under the bill's provisions:

- requires a subpoena to describe any objects or items to be produced and prescribe a reasonable return date by which those objects or items must be assembled and made available;
- authorizes a subpoena, except as provided by these provisions, to require the production of any records or other documentation relevant to the investigation, including the following:
    - a name;
    - an address;
    - a local or long distance telephone connection record, satellite-based Internet service provider connection record, or record of session time and duration;
    - the duration of the applicable service, including the start date for the service and the type of service used;
    - a telephone or instrument number or other number used to identify a subscriber, including a temporarily assigned network address; and
    - the source of payment for the service, including a credit card or bank account number;
- prohibits a provider of an electronic communication service or remote computing service from disclosing the following information in response to a subpoena but requires such a provider to disclose that information if the disclosure is required by a court order:
    - an in-transit electronic communication;
    - an account membership related to an Internet group, newsgroup, mailing list, or specific area of interest;
    - an account password; or
    - any account content, including any form of electronic mail, an address book, a contact list, a buddy list, or Internet proxy content or Internet history;
- authorizes a person authorized to serve process under the Texas Rules of Civil Procedure to serve a subpoena and requires the person to serve the subpoena in accordance with those rules; and
- authorizes the person receiving a subpoena, before the return date specified on the subpoena, to petition in an appropriate court located in the county where the subpoena was issued for an order to modify or quash the subpoena or to prohibit disclosure of applicable information by a court.

H.B. 3185 requires the prosecuting attorney to do the following, as appropriate, if a criminal case or proceeding does not result from the production of records or other documentation under the administrative subpoena within a reasonable period:

- destroy the records or documentation; or
- return the records or documentation to the person who produced the records or documentation.

Any information, records, or data reported or obtained under the subpoena is confidential and may not be disclosed to any other person unless the disclosure is made as part of a criminal case related to those materials.

EFFECTIVE DATE

September 1, 2025.