BILL ANALYSIS

C.S.H.B. 896
By: Hernandez
Criminal Jurisprudence
Committee Report (Substituted)

BACKGROUND AND PURPOSE

Recognizing that cyber security is not only a national issue but also a state issue, interested parties assert that there is a current need for the legislature to enact certain revisions to the law relating to the offense of breach of computer security so that the law is readily available to use against a person committing such an offense. These parties explain that legislation enacted in 2011 addressed the prosecution of and punishment for the offense but inadvertently removed certain language and that this has resulted in the need to clarify matters relating to the legislature's original intention to punish the intent to obtain a benefit through computer hacking. C.S.H.B. 896 seeks to address this issue and give prosecutors the ability to effectively prosecute these types of offenses.

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

C.S.H.B. 896 amends the Penal Code to expand the conduct that constitutes the offense of breach of computer security to include knowingly accessing, with the intent to defraud or harm another or to alter, damage, or delete property, a computer, computer network, or computer system that is owned by the government or a business or other commercial entity engaged in a business activity if such action is in violation of a contractual agreement to which the actor has expressly agreed or in violation of a clear and conspicuous prohibition by the owner of the computer, network, or system and is taken with the additional intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system. The bill establishes a defense to prosecution for such conduct if the actor's conduct consisted solely of action taken pursuant to a contract that was entered into with the owner of the computer, computer network, or computer system for the purpose of assessing the security of the computer, network, or system or for the purpose of providing other security-related services.

EFFECTIVE DATE

September 1, 2015.

COMPARISON OF ORIGINAL AND SUBSTITUTE

While C.S.H.B. 896 may differ from the original in minor or nonsubstantive ways, the following

comparison is organized and formatted in a manner that indicates the substantial differences between the introduced and committee substitute versions of the bill.

INTRODUCED	HOUSE COMMITTEE SUBSTITUTE
SECTION 1. Section 33.02(b-1), Penal Code, is amended to read as follows:	SECTION 1. Section 33.02, Penal Code, is amended by amending Subsection (b-1) and adding Subsection (f) to read as follows:
(b-1) A person commits an offense if: (1) with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses a computer, computer network, or computer system without the effective consent of the owner; or (2) with the intent to obtain a benefit, the person knowingly accesses a computer, computer network, or computer system	(b-1) A person commits an offense if, with the intent to defraud or harm another or alter, damage, or delete property, the person knowingly accesses: (1) a computer, computer network, or computer system without the effective consent of the owner; or
in violation of: (A) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or (B) a contractual agreement to which the person has expressly agreed.	(2) a computer, computer network, or computer system: (A) that is owned by: (i) the government; or (ii) a business or other commercial entity engaged in a business activity; (B) in violation of: (i) a clear and conspicuous prohibition by the owner of the computer, computer network, or computer system; or (ii) a contractual agreement to which the person has expressly agreed; and (C) with the intent to obtain or use a file, data, or proprietary information stored in the computer, network, or system. (f) It is a defense to prosecution under Subsection (b-1)(2) that the actor's conduct consisted solely of action taken pursuant to a contract that was entered into with the owner of the computer, computer network, or computer system for the purpose of assessing the security of the computer, network, or system or providing other security-related services.
SECTION 2. The change in law made by this Act applies only to an offense committed on or after the effective date of this Act. An offense committed before the effective date of this Act is governed by the law in effect when the offense was committed, and the former law is continued in effect for that purpose. For purposes of this section, an offense was committed before the effective date of this Act if any element of the offense occurred before that date.	SECTION 2. Same as introduced version.

SECTION 3. This Act takes effect September 1, 2015.	SECTION 3. Same as introduced version.