Public Safety Committee

HB 2375

Brief Description: Concerning cybercrime.

Sponsors: Representatives Magendanz, Orwall, Smith, Tarleton, MacEwen, Muri, Stanford and Wylie.

Brief Summary of Bill

- Creates the crimes of Electronic Data Interference, Electronic Data Theft, Spoofing, and Electronic Data Tampering in the first and second degree.

Hearing Date: 1/20/16

Staff: Kelly Leonard (786-7147).

Background:

Computer Trespass. The Legislature created the crimes of Computer Trespass in the first and second degree in 1984. A person commits Computer Trespass in the first degree if he or she, without authorization, intentionally gains access to a computer system or electronic database of another; and
- the access is made with the intent to commit another crime; or
- the violation involves a computer or database maintained by a government agency.

A person commits Computer Trespass in the second degree if he or she, without authorization, intentionally gains access to a computer system or electronic database of another under circumstances not constituting the offense in the first degree.

Computer Trespass in the first degree is a class C felony with a seriousness level of II, and Computer Trespass in the second degree is a gross misdemeanor.

Sentencing. Crimes are classified as misdemeanors, gross misdemeanors, or felonies (of which there are class A, B, and C felonies). The classification of a crime generally determines the

---

maximum term of confinement and/or fine for an offense. For each classification, the maximum terms of confinement and maximum fines are as follows:

Classification	Maximum Confinement	Maximum Fine
Misdemeanor	90 days	$1,000
Gross Misdemeanor	364 days	$5,000
Class C Felony	5 years	$10,000
Class B Felony	10 years	$20,000
Class A Felony	Life	$50,000

When a person is convicted of a felony, the Sentencing Reform Act (SRA) applies and determines a specific range of sentence within the statutory maximum. Under the SRA, sentences for felony offenses are determined by reference to a sentencing grid. The sentencing grid provides a standard range of months for the sentence, based on both the severity, or "seriousness level," of the offense and the convicted person's "offender score," which is based on the offender's criminal history.

Summary of Bill:

Definitions. The following terms are defined: "access;" "cybercrime;" "contaminant;" "data;" "data network;" "data program;" "data services;" and "data system." The definition for "computer program" is removed.

Computer Trespass. The crimes of Computer Trespass in the first and second degree are retained and moved to a new chapter within the Criminal Code.

Electronic Data Interference. The crime of Electronic Data Interference is created. A person commits Electronic Data Interference if the person maliciously and without authorization causes the transmission of data, a data program, or other electronic command designed to interrupt or suspend access to or use of a data network or data service. Electronic Data Interference is a ranked class C felony with a seriousness level of II.

Electronic Data Theft. The crime of Electronic Data Theft is created. A person commits Electronic Data Theft if he or she intentionally, without authorization, and without reasonable grounds to believe that he or she has such authorization, obtains any electronic data with the intent to devise or execute any scheme to defraud, deceive, extort, or commit any other crime, or wrongfully control, gain access, or obtain money, property, or electronic data. Electronic Data Theft is a ranked class C felony with a seriousness level of II.

Electronic Data Tampering. The crimes of Electronic Data Tampering in the first and second degrees are created. A person commits Electronic Data Tampering in the first degree if he or she intentionally, without authorization, and without reasonable grounds to believe that he or she has such authorization, adds, alters, damages, deletes, or destroys any electronic data, data system or data network, or introduces any contaminant into any electronic data, data system or data network, and:

- doing so is for the purpose of devising or executing any scheme to defraud, deceive, or extort, or commit any other crime, or of wrongfully controlling, gaining access, or obtaining money, property, or electronic data; or
- the electronic data, data system or data network are maintained by a governmental agency.

A person commits Electronic Data Tampering in the second degree if he or she intentionally, without authorization, and without reasonable grounds to believe that he or she has such authorization, adds, alters, damages, deletes, or destroys any electronic data, data system or data network under circumstances not constituting the offense in the first degree, or introduces any contaminant into any electronic data, data system or data network under circumstances not constituting the offense in the first degree.

Electronic Data Tampering in the first degree is a ranked class C felony with a seriousness level of II, and Electronic Data Tampering in the second degree is a gross misdemeanor.

Spoofing. The crime of Spoofing is created. A person commits Spoofing if he or she, without authorization, knowingly initiates the transmission, display, or receipt, of another person's or fictitious person's electronic data for the purpose of gaining unauthorized access to electronic data, a data system or data network, and with the intent to commit another crime. Spoofing is a gross misdemeanor.

Prosecution of Other Crimes. A person who, in the commission of a cybercrime, commits any other crime may be punished for that other crime as well as for the cybercrime and may be prosecuted for each crime separately.

Appropriation: None.

Fiscal Note: Requested on January 18, 2016.

Effective Date: The bill takes effect 90 days after adjournment of the session in which the bill is passed.