FINAL BILL REPORT
E2SHB 2375

C 164 L 16
Synopsis as Enacted

Brief Description: Concerning cybercrime.

Sponsors: House Committee on General Government & Information Technology (originally sponsored by Representatives Magendanz, Orwall, Smith, Tarleton, MacEwen, Muri, Stanford and Wylie).

House Committee on Public Safety
House Committee on General Government & Information Technology
Senate Committee on Law & Justice

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.

Summary:

Computer Trespass. Computer Trespass in the first degree is modified by specifying that access must be made with the intent to commit another crime in violation of a state law that is not a cybercrime.

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 that

---

This analysis was prepared by non-partisan legislative staff for the use of legislative members in their deliberations. This analysis is not a part of the legislation nor does it constitute a statement of legislative intent.

intentionally interrupts or suspends access to or use of a data network or data service. Electronic Data Interference is a ranked class C felony with a seriousness level 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 in violation of a state law that is not a cybercrime, 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 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 maliciously, without authorization, and without reasonable grounds to believe that he or she has such authorization, alters data as it transmits between two data systems over an open or unsecure network or introduces any malware 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 in violation of a state law that is not a cybercrime, 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 maliciously, without authorization, and without reasonable grounds to believe that he or she has such authorization, alters data as it transmits between two data systems over an open or unsecure network under circumstances not constituting the offense in the first degree, or introduces any malware 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 the identifying information of another organization or person for the purpose of gaining unauthorized access to electronic data, a data system, or a data network and with the intent to commit another crime in violation of a state law that is not a cybercrime. 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.

Definitions. The following terms are defined: "access;" "cybercrime;" "data;" "data network;" "data program;" "data services;" "data system;" "malware;" "white hat security research;" and "without authorization." The definition for "computer program" is removed.

Votes on Final Passage:

House	97	0	
Senate	46	1	(Senate amended)
House	96	0	(House concurred)

Effective: June 9, 2016