HB 2395 A STAFF MEASURE SUMMARY

Carrier: Sen. Prozanski

Senate Committee On Judiciary

Action Date:	05/13/19
Action:	Do pass the A-Eng bill.
Vote:	4-0-0-3
Yeas:	4 - Fagan, Gelser, Manning Jr, Prozanski
Abs:	3 - Bentz, Linthicum, Thatcher
Fiscal:	Has minimal fiscal impact
Revenue:	No revenue impact
Prepared By:	Gillian Fischer, Counsel
Meeting Dates:	4/29, 5/13

WHAT THE MEASURE DOES:

Requires manufacturers of connected device to equip connected device with reasonable security features that protect information that connected device collects, contains, stores, or transmits from unauthorized access, destruction, modification, use, or disclosure. Exempts from regulation entities and individuals subject to the Health Insurance Portability and Accountability Act of 1996 (HIPAA) and devices subject to regulations promulgated by the Food and Drug Administration (FDA) relating to medical devices, including software. Defines connected device and manufacturer.

ISSUES DISCUSSED:

- Laws currently in place to prohibit unlawful data collection but no required protections in devices
- Modeled on California statute
- Internet of Things devises rising in popularity in homes
- Does not create a right of action
- Definition of manufacturer includes products made outside of Oregon

EFFECT OF AMENDMENT:

No amendment.

BACKGROUND:

According to a public service announcement published by the FBI in 2018, cyber actors actively search for and compromise vulnerable Internet of Things (IoT) devices for use as proxies or intermediaries for Internet requests to route malicious traffic for cyber-attacks and computer network exploitation. IoT devices, sometimes referred to as “smart” devices, are devices that communicate with the Internet to send or receive data. Examples of targeted IoT devices include: routers, wireless radio links, time clocks, audio/video streaming devices, Raspberry Pis, IP cameras, DVRs, satellite antenna equipment, smart garage door openers, and network-attached storage devices.

House Bill 2395 A requires a person who manufactures a device that is sold in Oregon to equip the connected device with reasonable security features. The features should protect information that the connected device collects, contains, stores, or transmits from access, destruction, modification, use, or disclosure that the consumer does not authorize. Failure to build in reasonable security would be a violation of Oregon’s consumer protection law enforced by the Attorney General.