AN ACT relating to security of connected devices.

Be it enacted by the General Assembly of the Commonwealth of Kentucky:

➔Section 1. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

As used in Sections 1 to 3 of this Act:

(1) "Authentication" means a method of verifying the authority of a user, process, or device to access resources in an information system;

(2) "Connected device" means any device or other physical object that is capable of connecting to the Internet, directly or indirectly, and that is assigned an Internet Protocol address or Bluetooth address;

(3) "Consensus standards" means any standard promulgated by a nationally or industry-recognized standards development organization;

(4) "Manufacturer" means the person who manufactures, or contracts with another person to manufacture on the behalf of the person, connected devices that are sold or offered for sale in Kentucky. For purposes of this subsection, a contract with another person to manufacture on the behalf of the person does not include a contract only to purchase a connected device, or only to purchase and brand a connected device;

(5) "Reasonable security feature" means a security feature that is commensurate with the risk created by the level of connectivity of the product and accounting for the cost of the product, the cost to maintain the product, and the value of the product's services to the user;

(6) "Standards development organization" means any organization that plans, develops, establishes, or coordinates standards using agreed-upon procedures, which have the following attributes:

(a) Openness;

(b) Balance of interest;

(c) Due process;

(d) An appeals process; and

(e) A consensus agreement.

"Standards development organization" includes organizations recognized by the American National Standards Institute or other similar open consensus processes; and

(7) "Unauthorized access, destruction, use, modification, or disclosure" means access, destruction, use, modification, or disclosure that is not authorized by the owner or other authorized user.

➔Section 2. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) A manufacturer of a connected device shall equip the device with a reasonable security feature or features.

(2) To equip a device with a reasonable security feature, the manufacturer shall either:

(a) Equip the device with a reasonable security feature or features that are:

1. Appropriate to the nature and the function of the device;

2. Appropriate to the information it may collect, contain, or transmit; and

3. Designed to protect the device and any information contained therein from unauthorized access, destruction, use, modification, or disclosure; or

(b) Equip or reasonably be able to equip a connected product with a means to protect the product consistent with consensus standards that address commonly known or reasonably foreseeable vulnerabilities where such consensus standard is effective on the date of manufacture.

(3) Subject to the requirements set forth in subsections (1) and (2) of this section, a

connected device shall be deemed to have a reasonable security feature under subsections (1) and (2) of this section if:

(a) The device is equipped with a means for authentication outside a local area network;

(b) The preprogrammed password is unique to each device manufactured;

(c) The device contains a security feature that requires a user to generate a new means of authentication before access is granted to the device for the first time; or

(d) The device on the date of manufacture is or reasonably can be equipped with a means to protect the product consistent with consensus standards that address commonly known or reasonably foreseeable vulnerabilities.

(4) A manufacturer of a connected device shall not have liability to any user or owner of a connected device for any violation of this section if the owner or user of the connected device fails to connect in order to obtain available updates to the reasonable security features or otherwise does not avail himself or herself of any reasonable security feature available to the user or owner of the connected device.

➔Section 3. A NEW SECTION OF KRS CHAPTER 367 IS CREATED TO READ AS FOLLOWS:

(1) Sections 1 to 3 of this Act shall not be construed to:

(a) Impose any duty upon the manufacturer of a connected device related to unaffiliated third-party software or applications that a user chooses to add to or uses to interface with a connected device including software patches, updates, or downloads;

(b) Impose any duty upon a provider of an electronic store, gateway, marketplace, or other means of purchasing or downloading software or applications, to review or enforce compliance with Sections 1 to 3 of this

Act;

(c) Impose any duty upon the manufacturer of a connected device to prevent a user from having full control over a connected device, including the ability to modify the software or firmware running on the device at the discretion of the user;

(d) Provide a basis for a private right of action. The Attorney General, Commonwealth's attorney, or county attorney shall have the authority to enforce the provisions of Sections 1 to 3 this Act; or

(e) Limit the authority of a law enforcement agency to obtain connected device information from a manufacturer as authorized by law or pursuant to an order of a court of competent jurisdiction.

(2) Sections 1 to 3 of this Act shall not apply to any connected device the functionality of which is subject to security requirements under federal law, regulations, or guidance promulgated by a federal agency pursuant to its regulatory enforcement authority.

(3) When a consensus standard is used as the basis for determining that a connected product has been equipped or reasonably can be equipped with a reasonable security feature or features under Section 2 of this Act and that consensus standard is amended, a manufacturer shall be deemed to have equipped its connected product with a reasonable security feature or features under Section 2 of this Act so long as the reasonable security feature or features with which the product has been equipped conformed to the consensus standard in effect as of the date of the product's manufacture and the manufacturer has offered enhanced security features to the connected product when reasonably achievable.

(4) A covered entity, provider of health care, business associate, health care service plan, contractor, employer, or any other person subject to the federal Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, shall

not be subject to Sections 1 to 3 of this Act with respect to any activity regulated by that law.