January 27, 2020

Chair, Dereck Davis
House Committee on Economic Matters
Room 231
House Office Building
Annapolis, Maryland 21401

Dear Chairman Davis and members of the committee:

The Security Industry Association (SIA), headquartered in Silver Spring, is a nonprofit trade association representing businesses that provide a broad range of security products for government, commercial and residential users, including over 20 businesses with headquarters, employees, and operations in Maryland. Some of these security solutions include video cameras, carbon monoxide detectors, facial recognition software, and advanced locking mechanisms. Our member companies develop, manufacture, and integrate technologies that help keep people and property safe from fire, theft, and other hazards.

SIA's primary concerns include mandating original equipment manufacturers (OEM) to disclose proprietary source code, diagnostic, and repair information to independent repair providers; placing the security – and cybersecurity – condition of certain equipment into a precarious state; and jeopardizing warranty policies that have long-proven to benefit and protect consumers.

Due to the overly broad and vague definition of "digital electronic equipment," which seemingly encompasses all digital electronic products, our member companies would be forced to disclose proprietary diagnostic and reparation information to individuals who do not have the

requisite skills to fix any known defects and thus puts the security integrity of residential and commercial users' equipment at risk.

For example, what would happen if an independent repair provider "fixed" your home security system but then an individual broke into your house for criminal purposes? HB 84 does not sufficiently answer who would be liable in this instance, the OEM and their authorized partners, or the independent repair provider. This example can be replicated in other cases should a house catch fire, pipes leak carbon monoxide, or a person exposes easily identifiable security vulnerabilities on locks. Simple malfunctions can cause real, physical harm. We must incentivize OEMs to ensure the efficacy and integrity of their products.

Secondly, HB 84 requires OEMs to release embedded software and security patches to independent repair providers which could compromise the cyber security of electronic equipment connected to an IP network. HB 84 does not explicitly forbid independent repair providers from overtly publishing sensitive intellectual property to the public. In the scope of cyber security, this includes software updates, source code, and encryption keys. Publishing this sensitive information not only impacts OEMs, but it increases consumer risks to future malicious cyber-attacks.

While "Right to Repair" appears well-intentioned, there are several unintended consequences that will adversely impact the security industry and its loyal customers if HB 84 becomes public law. Rather than stifling growth in an industry that thrives on innovation, we hope the Committee will work with private sector stakeholders to ascertain how we can address these issues in a collaborative manner.

Thank you for your time and attention to this issue. Please let us know if SIA or its members can provide information or any other further assistance to you and your colleagues in the legislature.

Sincerely,

Don Erickson

Don Erickson
Chief Executive Officer
Security Industry Association

Staff contact: Drake Jamali, djamali@secuirtyindustry.org