To: Senator Michael Sirotkin, Chair, Senate Committee on Economic Development, Housing, & General Affairs

From: Joe Hoellerer, Manager – Government Relations, Security Industry Association (SIA)

Date: Feb. 6, 2017

Re: SIA opposition to S. 180 (Pearson), an act relating to the Vermont Fair Repair Act

---

SIA is a non-profit, international trade association representing over 800 security and life safety solutions providers. Our member companies develop, manufacture, and integrate technologies that help keep people and property safe from fire, theft, and other hazards. Some of these security solutions include video cameras, carbon monoxide detectors, facial recognition software, and advanced locking mechanisms, to name a few. SIA represents industry leaders who constantly strive to introduce robust security solutions that keep families safe from nefarious individuals and ensure sensitive areas are secured from unauthorized entry. Due to the advent of interconnected sensors, networks, and ubiquitous smart technologies, use of these systems is growing in homes and businesses around the country.

On behalf of SIA, we must respectfully submit our **opposition to S. 180**, known as the Vermont Fair Repair Act.

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.

We understand the intention of this legislation is to provide consumers with the freedom and flexibility to fix everyday consumer devices, such as smartphones, tablets, televisions, and computers. However, due to the overly broad and vague definition of "equipment," which seemingly encompasses all digital electronic equipment, our member companies would be forced to comply with this burdensome legislation if enacted into law.

If an OEM of traditional security systems – e.g. video cameras, carbon monoxide detectors, fire alarms, alarm panels, and advanced locks – is forced to disclose proprietary diagnostic and reparation information, then residential and commercial users could be placing the security integrity of their equipment into the hands of individuals who do not have the requisite skills to fix any known defects. 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? S. 180 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, S. 180 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. S. 180 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. Once threat actors have access to this sensitive information, they can unleash a multitude of damaging cyber-attacks that potentially place consumers into an irreparable position.

Our membership prides itself on manufacturing and deploying technologically-advanced security solutions while providing consumers and end-users with multiple repair options outside of the OEM. In order to remain competitive in the security industry, companies understand it is imperative to certify authorized repair providers so customers receive flexibility when repairs are needed. SIA companies have certified multiple authorized repair providers and as a common business practice, OEMs certify repair providers through rigorous training to ensure these authorized partners are well-trained, knowledgeable, and qualified to meet the standards set forth by the OEM. By placing intricate repair information into the possession of uncertified independent repair providers, S. 180 is in fact, exposing consumers to more potential risk.

While “Right to Repair” appears well-intentioned, there are several unintended consequences that will adversely impact the security industry and its loyal customers if S. 180 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.

cc: Members of the Senate Committee on Economic Development, Housing and General Affairs & Senator Pearson

Senator Alison Clarkson, Vice Chair
Senator Philip Baruth
Senator Becca Balint
Senator David Soucy
Senator Christopher Pearson