Submitter: Paul Roberts

On Behalf Of:

Committee: Senate Committee On Energy and Environment

Measure: SB1596

Chair Sollman, Vice-Chair Findley, and Members of the Committee:

My name is Paul Roberts and I am the founder of Secure Repairs (securepairs.org), an organization of more than 350 cyber security and information technology professionals who support the right to repair. I am writing to you today on behalf of our members to make clear that the fair access to repair materials sought by right to repair laws like Senate Bill 1596 does not increase cyber risk. In fact, it can contribute to healthier and more secure ecosystems of smart, connected devices.

No Cyber Risk In Repair

The proposed right to repair legislation, Oregon Senate Bill 1596, considered by this Committee simply asks manufacturers that already provide repair information and tools to their authorized repair providers to also provide them at a fair and reasonable price to the owners of the devices - and to third parties those owners may hire. By definition, the information covered by right to repair laws is not sensitive or protected, as evidenced by the fact that manufacturers distribute it widely to hundreds, thousands or tens of thousands of repair professionals working on behalf of their authorized providers. That includes everything from auto mechanics working at dealerships to hourly workers staffing the Geek Squad at Best Buy.

Hacked via schematics? Not a thing.

Also: we have yet to find- nor be presented with any evidence that the types of information covered by right to repair laws - schematic diagrams, service manuals, diagnostic software and replacement parts - act as a portal to cyber attacks. The vast majority of attacks on Internet connected devices - from broadband routers to home appliances and automobiles - exploit weak device configurations or vulnerabilities in embedded software produced and managed by the manufacturer. These security weaknesses are epidemic. A recent study of the security of IoT devices by Phosphorus Labs, a cybersecurity company, found that 68% of Internet of Things devices contained high-risk or critical software vulnerabilities.

Again: these hacks of connected devices take place without any access to repair materials. Nor is there any evidence that providing access to repair software will open doors to new attacks. As an example: a diagnostic routine that identifies a failed component or reveals the operating temperature of a device doesn’t provide access to the kinds of sensitive data that hackers are interested in.

A Right to Repair is key to a secure Internet of Things

As the Internet of Things ages and manufacturers gradually step away from their responsibility to support and maintain deployed products, new laws such as Senate Bill 1596 will foster a market based response: a diverse ecosystem of small, aftermarket service providers that step into the shoes of OEMs: supplying needed software updates and security patches, servicing and repairing deployed devices and so on. Passage of this law will foster a range of business and employment opportunities for Oregon residents and small businesses, fostering growth, investment and innovation up and down the economic ladder.

Repair: Pro-Consumer, Pro-Competition, Pro-Environment
To sum up: federal right to repair legislation like Oregon Senate Bill 1596 will greatly improve the quality of life for Michigan consumers, families, and communities, while promoting small businesses and reducing e-waste throughout the country. On behalf of our more than 350 members, I urge this committee to support the passage of this important right to repair legislation.

I or any of the cyber security experts who make up our group would be happy to meet with you and your staff answer any questions you may have about cybersecurity and the right to repair.

Sincerely,
Paul F. Roberts
Founder, Secure Repairs
paul@securepairs.org