securepairs.org
security professionals for a fixable future

Jan 29, 2026

Dear Chairman Joseph A Solomon, Jr,
Representative William W. O'Brien, 1st Vice Chair
Representative Justine A. Caldwell, 2nd Vice Chair
Members of the House Corporations Committee

I am writing to you today in support of H7180, "Digital Electronics Right to Repair". I write on behalf of the more than 400 members of https://securepairs.org/who-we-are/ a coalition of the country's most respected information ("cyber") security experts.

To help you understand our thinking, we would like to call a few important facts to your attention. We hope that these explanations help provide context for cybersecurity-focused arguments made in opposition to H7180.

1. There is no cyber risk in independent repair
2. Authorized repair is not more trustworthy or secure
3. Flaws in OEM software - not repair information - fuel cyber attacks
4. Cyber criminals already have access to vendor firmware.
5. A right to repair makes businesses more secure, not less

There is no cyber risk in independent repair

Tech industry lobbyists and representatives from large vendors have argued for years that making information like service manuals and schematic diagrams as well as tools such as diagnostic software available to customers and third party repair providers poses a security risk. The only information required under H7180 is already in circulation worldwide. OEMS know that they cannot fully trust thousands of their own employees to keep any secrets – which are carefully scrubbed from repair materials, training materials and websites.

Most of us have experienced "phishing" attempts on our own computers where websites and emails pretending to be our banks, insurance companies, and friends trying to collect personal information. This is a huge risk having nothing to do with replacing burnt out parts or re-connecting wires. If a hacker accidentally got a schematic diagram – that diagram would still be useless for finding personal data or secure access credentials.

Authorized repair is not more trustworthy or secure.

The sad fact is that handing over your digital device to a technician, OEM or independent, gives that technician physical access to everything stored. The real protections for owners are to make sure to use security tools such as encrypted backups or “security mode” to prevent unauthorized access. The FTC “Nixing the Fix” Report to Congress evaluated this statement and found that consumers are not better protected by OEMs than independent providers.

There is the 2016 incident in which an Oregon college student sent her iPhone to Apple’s authorized repair provider, Pegatron, for repair only to have two technicians working for a Pegatron subcontractor access sexually explicit photos and a video from her phone and then upload them to her Facebook account. Apple quietly paid a multimillion-dollar settlement and confirmed the incident. Or the 2021 incident in which Google acknowledged it was investigating a string of incidents in which customers who mailed Pixel smart phones to the company’s authorized repair provider similarly reported that sensitive photos and videos were accessed by repair technicians. Then, in November of last year, Encore Repair Services, a major provider of authorized repair for OEMs, acknowledged that it suffered a security breach in which the Play ransomware group compromised Encore’s network and stole data which was then uploaded to the dark-web.

Flaws in OEM software - not repair information - fuel cyber attacks

Cyber security products are driven by specialized software run on ordinary servers. These products roll off assembly lines and their software is shipped to customers rife with exploitable weaknesses, including decades-old software modules, known and exploitable software vulnerabilities, and vulnerable default configurations. Once deployed, these devices – and the companies that deploy them – are easy prey for cybercriminals and nation-state actors.

CISCO makes a tremendous effort keeping their servers patched, but patching has to be done at the physical location of the server at every possible location. Just a few unpatched items can remain open to network hacks. There is no perfect way to prevent access other than not connecting to the outside world. One of the reasons that nuclear power plants are highly secure is that most were built before the internet.

Consider, for example, the recent storm of attacks targeting Cisco Adaptive Security Appliances (ASA). Those attacks are connected to a China-sponsored advanced persistent threat (APT) that has exploited a long string of previously undiscovered (“zero day”) software flaws in the Cisco software running ASA devices, with the Chinese actors exploiting zero-day vulnerabilities to gain unauthenticated remote code execution [RCE] on ASAs. That’s a very familiar pattern, with no link whatsoever to repair information, documentation, parts or diagnostic software.

Cyber criminals already have access to vendor firmware.

Leading cyber security experts on the front lines defending corporations and the military can attest that cyber-adversaries *already have access* to firmware for the devices they seek to compromise. Firmware can be extracted and decompiled, stolen or purchased.   The recent alert from CISA shows there are hundreds or thousands of vendor-authorized repair providers that already have access to repair materials anti-R2R lobbyists assume are being kept secret but are not secret and should not be secret.

When vendors argue that opposing a right to repair devices is about protecting them from compromise, understand that “the horse has left the barn,” as the steady cadence of devastating attacks on leading enterprise devices (F5, Cisco, Ivanti) illustrates.https://federalnewsnetwork.com/cybersecurity/2025/10/cisa-directs-agencies-to-address-significant-cyber-threat/.

A right to repair makes businesses more secure, not less

The proposed language of H7180 is a cybersecurity win for Rhode Islanders. Most consumers and small businesses lack the staff to evaluate, test, and install security software updates. H7180 will allow more skilled technicians to offer their services to help consumers, businesses and farmers keep their devices safe from hackers. That will lead to a more secure and resilient IT ecosystem in your state.

We would be pleased to answer any questions you may have about the cyber impacts of the right to repair, or the ideas and issues raised in this letter.

Sincerely,

Paul Roberts
Founder, Secure Repairs