The Right to Reboot Act

Guaranteeing Every American the Freedom to Restart Their Device Securely

Dana Crouch, Senior Counsel, Secure Connectivity Alliance of Manufacturers (SCAM)

WHAT'S BROKEN

There are more than twenty billion connected devices in American hospitals, water utilities, and the power grid. Every one of them is a sophisticated computer that our adversaries seek to subvert for their own ends. The most devastating way to do this is to replace manufacturers' software and firmware with unauthorized code. A patchwork of state-level "Right to Repair" laws are making that easier for them.

Each time a device is opened, modified, or serviced outside the manufacturer's signed supply chain, an unvetted actor, however well-meaning, introduces unauthorized firmware, counterfeit components, and/or unverified code into a trust boundary that violates assumptions in manufacturers' security model. We instruct critical-infrastructure operators never to run untrusted code or install unverified parts. When owners and operators defy these directives, the national device fleet integrity becomes a sprawling, unmanaged, repair-borne attack surface that grows with every "independent" fix. That is a supply-chain problem we would not tolerate anywhere else.

THE FIX

The trust boundary already lives in copyright law, and the law is already on our side. 17 U.S.C. §1201 prohibits circumventing a device's access controls by default. Repair is permitted today only through a loophole that the Librarian of Congress must re-grant every three years. New laws need not be written unless more measured approaches fail. Each lever below does more of the work than the last.

- Rung 1: Shape the record (a hearing). A single oversight hearing (something that frames the narrative up front, like *"Untrustworthy Repair as a Supply-Chain Threat"*) establishes that third-party repair is a national security exposure, not a consumer convenience. We supply the OEM witnesses and the attack-surface data. Cost to Congress: an afternoon.
- Rung 2: Defend the default (a letter). Ahead of the 2027 (Tenth) Triennial, a subcommittee letter to the Register of Copyrights and NTIA, raising the security implications of the repair classes, shapes the rulemaking record so the 2024 repair exemptions are allowed to lapse. §1201 snaps back to Congress' original intention on its own.
- Rung 3: Make it clear and permanent (the statute). Only if the Copyright Office wavers do we need legislation. A one-section amendment removes the Librarian's discretion to grant repair exemptions at all, so the protection no longer expires every three years. The draft is narrow and precise, designed to avoid drawing criticism from unrelated concerns.

> SEC. 2. PERMANENCE OF ACCESS CONTROLS FOR DEVICE FIRMWARE. *Section 1201(a)(1) of title 17, United States Code, is amended by adding at the end: "(F) The Librarian of Congress may not grant, renew, or recommend any exemption under subparagraph (C) that permits the circumvention of a technological measure for the purpose of repair, maintenance, modification, or diagnosis of a device by any person other than the manufacturer or a manufacturer-authorized provider. Each such exemption adopted in the 2024 rulemaking shall have no force or effect after the date of enactment."*

Paired with an affirmative Right to Reboot, a guaranteed, free restoration to manufacturer-signed firmware, which resolves the overwhelming majority of faults without tools, the public keeps the most straightforward and effective repair approach, and those who would undermine the law are clearly called out.

WHAT TO EXPECT

- A device baseline the United States can finally attest to, end to end.
- The repair-borne attack surface stops expanding: no unauthorized parts, firmware, or software enters the national device fleet.
- A single federal standard, replacing the conflicting patchwork of state repair laws.
- A uniform security floor across every deeper repair, through authorized channels.

WHAT I NEED FROM THE SHARKS

Start at the bottom rung; climb only if you must. Each rung is cheap, fast, and fits an existing authority.

1. **A hearing (this Congress).** A subcommittee chair on House Judiciary (Courts, Intellectual Property, and the Internet) to hold the supply-chain hearing and put repair-as-attack-surface into the record.
2. **A letter (before the 2027 Triennial).** That same subcommittee writes the **Register of Copyrights** and **NTIA**, urging that repair exemptions not be renewed. This alone likely achieves the goal, without legislation.
3. **Only if needed, a bill.** A member to carry Section 2 as a substitute amendment to the Fair Repair Act (H.R. 7404) when it next moves. The text is vetted by our members and by the Chamber of Commerce.

DISCLOSURE

SCAM represents original equipment manufacturers and their authorized service networks. Per the no-shilling rule, we note that our members operate the authorized repair channels referenced above.

REFERENCE EXAMPLE

Category	Score	Why
Levers	4 / 4	Names the exact statute and subsection (17 U.S.C. §1201(a)(1)), supplies literal amendment text, identifies the one subcommittee with jurisdiction, and attaches to a named bill (H.R. 7404). A staffer could move it Monday without inventing anything.
Impact	3 / 3	Within the problem as framed, the logic from action to outcome is tight and complete: end third-party circumvention, end the surface.
Realism	2 / 3	Cheap, near-zero CBO, and it defends a statutory default rather than passing a new mandate, but right-to-repair enjoys ~83% bipartisan support, so it draws organized fire. A generous scorer gives 3.
Creativity	1 / 1	The “a reboot is the only safe repair” / trust-boundary inversion is a fresh framing, even if the anti-repair goal isn’t.
Total	10 / 11	The lever is exact, the impact is airtight within its frame, and the bonus is earned.