Dear Legislators and Committee Members,

My name is Todd Bone, and I am a 4-Year Past Chairman of the ITAD Association (Formerly ASCDI), a Former 10+ Year Board Member of the Service Industry Association (SIA), current Treasurer of Repair.org, and Secondary Market IT Consultant.

For more than 35 years, I have provided repair services to government-owned data centers, including DoD (now the Department of War), and obtained the first GSA 25-Year Contract Schedule for Refurbished IT Equipment. Many of the Government client locations could not be serviced by the OEM because the OEM deemed older models obsolete. But, the Government makes substantial investments in software, for example, the Air Force who continues to use IT equipment for longer than 15 years, for example the Mutually Assured Destruction Program (M.A.D.), where the Air Force runs Nuclear Warfare Simulations on Supercomputers, which include server, storage, and networking equipment; and the Global Hawk Drone flight and training systems, all of which my former company XSi was the only company in the world left to support these systems.

XSi was also one of the first companies to provide repair and support for Cisco equipment, repairing Cisco-deemed obsolete Routers when Naval Ships returned to port. We also repaired Cisco equipment for Fortune 500 companies.

So, I'm quite familiar with what the government deems "critical infrastructure".

In my experience, CISCO uses "critical infrastructure" to describe infrastructure important to an organization's operations, while DHS/CISA/NIST defines it as infrastructure whose failure would have debilitating consequences for the United States.

Sources:
https://www.cisco.com/c/en/us/solutions/critical-infrastructure.html
https://www.govinfo.gov/content/pkg/USCODE-2023-title42/html/USCODE-2023-title42-chap68-subchapIV-B-sec5195c.htm

Unlike our federal agencies, Cisco applies a broad, operational, and marketing-driven definition, whereas federal law applies a narrow, national-impact standard. This allows Cisco to label ordinary enterprise networking equipment as "critical infrastructure," even when it does not meet the legal threshold.

Sources:
https://www.cisco.com/c/en/us/solutions/critical-infrastructure.html
https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience

Therefore,

1. Cisco's own materials define 'critical' functionally, based on business importance—not based on national impact.
   Source: https://www.cisco.com/c/en/us/solutions/critical-infrastructure.html
2. Federal law requires a much higher bar: the system must be so vital that its failure would have debilitating consequences for the United States.

Source: https://www.govinfo.gov/content/pkg/USCODE-2023-title42/html/USCODE-2023-title42-chap68-subchapIV-B-sec5195c.htm

3. Important enterprise IT systems are not automatically 'critical infrastructure' under DHS/CISA definitions.
   Source: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors
4. Cybersecurity concerns do not expand the legal definition of critical infrastructure—they are risks to be managed within it.
   Source: https://www.nist.gov/publications/framework-improving-critical-infrastructure-cybersecurity

This massively intrusive and overly broad definition in SB90 creates a marketplace where only CISCO can play – in direct conflict with long-standing antitrust law prohibiting monopolization. CISCO enjoys not only a monopoly on repairs but also on product sales. SB90 is not an egalitarian, pro-business piece of legislation – it is a gift to CISCO with no corresponding benefit to Colorado, where the M.A.D. program is located.

Best regards,

Todd Bone
todd@bone.holdings

Bone Holdings, LLC.
IT Secondary Market Consultancy Firm
1640 Chambord Avenue
Frisco, TX 75034

1919 S. Eads St.
Arlington, VA 22202
703-907-7600
CTA.tech

April 24, 2026

Representative Jenny Willford, Chair
Representative Chad Clifford, Vice Chair
House State, Civic, Military, & Veterans Affairs
Colorado General Assembly
200 E. Colfax Avenue
Denver, CO 80203

Re: SB26 – 090 – Exempt Critical Infrastructure from Right to Repair - Support

Dear Chair Willford, Vice Chair Clifford, and Members of the House State, Civic, Military & Veterans Affairs:

On behalf of the Consumer Technology Association® ("CTA")[1], thank you for the opportunity to provide testimony on Senate Bill 26-090, (SB26-090), Exempt Critical Infrastructure from Right to Repair. CTA strongly supports this legislation to exempt information technology intended to be used in critical infrastructure from Colorado's right to repair law passed in 2024.[2]

CTA is the trade association representing the U.S. consumer technology industry. Our members are the world's leading innovators – from startups to global brands to retailers – helping support more than 18 million American consumer technology jobs. Our members include manufacturers of digital electronic equipment subject to the provisions of the existing right to repair law for digital electronic equipment.[3]

Right to repair laws exist in nine states in the U.S. and Colorado is the only state to include critical infrastructure technology in the provisions of its law.[4] All other states have recognized that information technology equipment intended to be used in critical infrastructure (e.g. internet infrastructure, data centers, etc.) raises significant security risks if information / documentation on how to access those devices along with the parts and tools are provided to any entity – including entities that may want to cause harm to the these systems. Enabling essentially universal access to critical infrastructure leaves these systems vulnerable to cybersecurity attacks and malicious intent. The inclusion of information technology equipment used in critical infrastructure in the right to repair provisions puts all Colorado residents and businesses at risk.

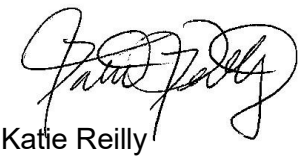
The exemption proposed in SB26-090 brings Colorado into alignment with the eight other state level repair laws. Critical infrastructure systems are the backbone of our water, transportation and communication infrastructure and these systems rely heavily on integrated information

[1] As North America's largest technology trade association, CTA® is the tech sector. CTA owns and produces CES®—the most powerful tech event in the world.
[2] Colo. Rev. Stat. §§ 6-1-1501 to 6-1-1505 (Consumer Right to Repair)
[3] Ibid
[4] Kansas's repair legislation became law earlier this month (April 2026) joining California, Colorado, Connecticut, Minnesota, New York, Oregon, Texas, and Washington.

technology. The Legislature recognized in 2024 the need to exclude other infrastructure systems from the requirements of the Colorado repair law including safety communications equipment and certain energy infrastructure. Many of these systems are interconnected with other critical infrastructure systems – especially in the communications sector – meaning an impact (e.g. malicious firmware, manipulated systems, etc.) in the communication sector could have a cascading effect on safety communications or the energy grid. Given the interconnectedness of our critical infrastructure systems, the same rationale should be given to all critical infrastructure systems that rely on information technology equipment, not just a select few.

CTA respectfully requests your support to pass this important legislation and protect Colorado residents and businesses. If you have any questions, please do not hesitate to contact me at kreilly@cta.tech.

Sincerely,



Katie Reilly
Vice President, Environmental Affairs and Industry Sustainability
Consumer Technology Association

SB26-090

Thank you Chairman and members of this panel. My name is Nilesh Patel and I am not only a repair professional but also an employee of the one of the largest Medical Device manufacturers in the world.

This bill is too broad in both its language and its approach. If it passes it will inevitably grant manufactures the ability to monopolize the repair industry. This will negatively impact quite literally every industry across the board. Fortune 500 companies, small businesses, schools, hospitals, libraries, governments, law enforcement, you name it…

As an employee of one of the largest medical device manufacturers in the world, I see this bill from the same lens as those companies who stand for this bill and from the lens of an IT repair professional that stand against it. From the lens of those who stand for it, they stand to gain monetarily. From the lens of those who stand against it, they stand to provide cheaper, faster, and safer solutions while extending the life of the hardware they own.

I get the privilege of working shoulder to shoulder with BioMedical Engineers, Clinicians, IT/IS professionals, and hospital executives that rely on these technologies to provide the highest level of medical care to patients across the entire globe.

As a hardware manufacturer, we supply medical devices to hospitals that in of themselves require, what is labeled as “critical infrastructure” to operate within a hospital’s environment. We supply the necessary tools for these hospitals to repair these devices on their own such that turn around times are quicker and reduce the impact on the patients they serve. Doing this offers greater patient safety, faster recovery times, reduces lengths of stay in hospitals, and allows for more patients to be served. The costs of healthcare are absurdly high already, allowing this bill to pass will inevitably increase healthcare costs, reduce turn around times, limit the patients they can serve, will cost people their jobs and unfortunately will cost lives.

It is a blatantly false premise that repair tools pose a security risk. As a hardware manufacturer we offer repair tools free of charge while also allowing the use of third-party repair tools and services to reduce costs and grant faster turn arounds. Our position is if they buy it, they own it.

Hospitals are one of the many places that purchase and use IT equipment. They also employ their own IT/IS and BioMedical engineers to support the repair of the equipment they purchased. We know in today’s world that technology moves fast and forcing customers to upgrade their perfectly operational equipment not only feeds into the e-waste pandemic but also limits their ability to comply to the latest security standards that are readily offered by third-party software and tools. This grants new life to old technology

without compromising security and reduces costs to both the hospitals and to the patients they serve. As a country, we have an broken healthcare system driven mainly by the already absurdly high costs associated to that healthcare.

By passing this bill, hospitals will have no choice but to pass these additional costs down to the patients, feed into the e-waste pandemic, and drive down healthcare.

The very people who were hired as the oil to keep the hospitals engine running will likely lose their jobs by turning over what they spent years training for, obtaining degrees for, and dedicating their lives for, to the companies that manufactured the hardware.

I strongly oppose this bill and hope everyone on the panel understands the risk to people's lives it will cause if it is passed.

Thank you,

Nilesh Patel

House State, Civic, Military, & Veterans Affairs

04/27/2026

SB26-090 Exempt Critical Infra from Right to Repair

Typed Text of Testimony Submitted

Name, Position, Representing	**Typed Text of Testimony**
Aaron Farrington Against themself	As a citizen of Colorado, and one who works in IT, I am opposed to the legislature attempting to remove our rights to repair our equipment for vague and non-specific "security" reasons. As school districts and other government entities face budgeting shortfalls due to the current economic and political environment, being able to repair and maintain pre-existing equipment is important to make sure that these entities are able to continue providing the services their communities need without overrunning their budgets. The idea that any singular "cyber security" incident would be caused by being able to repair equipment is honestly insulting, especially with how many issues are caused by companies outsourcing their software engineering to foreign entities and hallucination prone generative AI products. If anything, being allowed to repair equipment will decrease cyber security incidents as companies and organizations can hold off on upgrading until the new replacement equipment has proven to be secure over time and thorough testing.
Bennett Rutledge Against themself	Chair Willford, Major Clifford, and members of the committee, good afternoon, When I was a bureaucrat with the Federal Highway Administration, It was made plain to me that the reason we were to use standardized programming languages on our digital equipment of the day, such as COBOL and FORTRAN, rather than proprietary languages, was because we did not want to get locked in to digital equipment from a single vendor. If I could be sure that the Colorado Attorney General would have the experience with government contracts to understand that, at a deeper level, I would say that a judgment could be made on a case-by-case basis. But if the Attorney General does not have that specific background, it would be very dangerous, particularly with "enterprise critical" level infrastructure, to be locked into a relationship with a corporation already proven willing to force their clients to that level of dependency and exclusivity, when the inevitable crisis occurs.

	Please vote NO on SB26-090 - Exempt Critical Infra from Right to Repair, so that Colorado can use any repair personnel available in such a crisis.
Brian Louther Against themself	Iâ€™m a Colorado resident, and Iâ€™m here to oppose SB26-090. While â€œright to repairâ€ may sound appealing on the surface, this bill creates serious unintended consequences for small and local businesses across our state. It imposes broad mandates that shift costs, liability, and operational burdens onto manufacturers, distributors, and service providersâ€”many of which are small businesses themselves or rely on tightly managed supply chains to stay afloat. Forcing companies to open access to proprietary parts, tools, and diagnostic information undermines intellectual property protections and introduces real risks around safety, quality control, and cybersecurity. Not every repair environment is equipped to handle complex or sensitive systems safely, and when things go wrong, the accountability becomes unclear. That uncertainty hurts consumers and businesses alike. For small businesses in particular, this bill could be devastating. Many operate on thin margins and depend on authorized service networks or exclusive supplier relationships to remain viable. SB26-090 disrupts those models overnight, creating new compliance costs and exposing them to unfair competition from entities that are not held to the same standards. Instead of strengthening local economies, this bill risks destabilizing them. From a public policy standpoint, SB26-090 is overly broad, insufficiently targeted, and fails to balance consumer interests with the realities of maintaining safe, secure, and sustainable products and services. Good policy should solve problems without creating larger onesâ€”this bill does not meet that standard. I urge lawmakers to reject SB26-090. And I want to be clear: I will be paying close attention to how elected officials vote on this issue. I will not supportâ€”either in the primary or the general electionâ€”any candidate who votes in favor of this bill.

	Colorado deserves thoughtful, balanced legislation that protects consumers without harming the businesses that keep our communities running. SB26-090 falls short of that goal.
Chad MacDonald Against themself	Testimony Before the Colorado House of Representatives Opposition to the Antiâ€“Right to Repair Bill Good afternoon, Madam Speaker and members of the House. My name is Chad MacDonald. I am a Colorado resident and the owner of a small, oneâ€‘person IT company. I support small businesses across the state and also provide technology services for several county jails. I want to focus today on a core technical problem with this bill: the assumption that â€œcritical infrastructureâ€ uses fundamentally different equipment than what is found in a normal office environment. That assumption is incorrect. The routers, switches, firewalls, servers, backup power supplies, and network cabling used in a county jail, a 911 call center, or a hospital are often the same commercial, offâ€‘theâ€‘shelf devices used in small offices, schools, libraries, and local businesses. They are not exotic or specialized tools. What makes a system â€œcriticalâ€ is not the hardware itself, but the role it happens to be serving at that moment. A network switch does not know whether it is connecting a law firm or an emergency dispatcher. A battery backup does not distinguish between a dentistâ€™s office and a jail facility. Yet this bill treats identical equipment differently based on vague context, creating legal uncertainty for technicians performing routine, necessary repairs. This puts professionals like me in an impossible position. A simple, preventative actionâ€”such as replacing a failed power supply, battery, or network componentâ€”could suddenly be construed as unauthorized work on â€œcritical infrastructure,â€ even though it is the same repair I perform safely and competently every day.

	The practical result is delay. Instead of immediate repair, systems could remain down while waiting days or weeks for an authorized provider. In environments where uptime truly matters, that delay itself becomes the risk. Critical infrastructure depends on speed, flexibility, and local expertise, not artificial repair monopolies. This bill misunderstands how modern technology works and would make essential systems less resilient, not more. I respectfully urge you to oppose this legislation. Thank you for your time and service. Chad MacDonald
Erin Rosa Against themself	Hello, my name is Erin Rosa and Iâ€™m a resident of Colorado. I also work as a senior security consultant who has conducted multiple engagements to test cyber security controls for a diverse set of clients, including Fortune 500 companies. I have found and responsibly disclosed high severity vulnerabilities in core networking hardware and critical infrastructure. This bill doesnâ€™t make sense to me. Broadly limiting a government or businessâ€™s ability to repair critical hardware equipment they have already purchased does not help consumers or the economy. And as someone who works in cyber security, I can tell you that repair tools and allowing people to repair their own equipment is not the security threat proponents of this bill are claiming it is. If anything, limiting repair to a small strata of individuals erodes security transparency and creates a â€œsecurity through obscurityâ€ scenario that doesnâ€™t work to protect infrastructure. Please donâ€™t undermine the progress the legislature has already made with right-to-repair legislation.
Helen Ge Against	I am a computer engineering student and a longtime Colorado resident. This bill's broad definition of what counts as 'critical infrastructure' essentially limits access to repair tools / products across the board; as

themself	many consumer products can potentially qualify. Right to repair is important to guaranteeing competition and consumer freedom. Companies such as Apple use closed-off repair ecosystems to extract money from consumers and tether them to their products / services. Doing so does not meaningfully improve security, as it merely pushes the problem to 'authorised' parties which are just as likely to make a mistake. Further, limiting access interferes with the work of security researchers, who depend on the attainability of some parts / documentation in order to investigate potential problems, and make devices *more* secure. If this is not required of companies, security researchers will not be able to audit our critical infrastructure, while foreign adversaries who are not bound by this law can freely do such work.
Jon Daniel Against themself	Hello, I have several years of repair experience and am truly horrified that this bill is being considered. Please vote against it, for this bill represents large corporate interests and not end users otherwise known as the very people you, members of the legislature, represent. This bill that we are discussing has no definition of what "critical infrastructure" is. Any hardware that is used for any application could be argued as "critical infrastructure" with the current wording. This alone has enormous implications that I feel have not been considered. I understand that this bill has support that stem from fears of China and other adversaries' reverse engineering of hardware. Most if not all of this hardware is already manufactured outside of the USA. What secrets remain at the hardware level? Software configuration and hardening is where security does the protection work. Big tech corporations want the consumer and end user in metaphoric chains. They want long term support contracts and they want no competition when it comes to repairing and keeping hardware operating. Please see this for what it is, and vote no. This bill is a violation of equal rights and should be struck down as such. Thank you for your time and consideration.
Kim Kennedy Against themself	Blocking practitioners from the right to repair does not make anything more secure. This is simply a way for manufacturers to control future outcomes of their product by charging egregious cost for renewal fees, and maintenance. This has nothing to do with security and everything to do companies reoccurring revenue. A strongly oppose this bill as it

	wouldnâ€™t do nothing except hurt those who are protecting our community.
Lee Fife Against themself	I am writing to express strong opposition to SB26-090 which attempts to remove right to repair options for IT equipment under the guise of "increased security". I have been an IT professional throughout my career, involved in IT security for small and large organizations. This bill is a clear attempt by incumbent manufacturers to try to reduce competition and undermine any secondary market while providing absolutely no additional security. It is anti-competitive and hostile to individuals and to any other companies besides the incumbents. The bill is far too broad and will impact almost all computing equipment at small and large businesses as well as at libraries,hospitals, and local governments. If enacted, it will have huge negative impacts across the landscape. And it's being done purely to provide a titled playing field for the manufacturers where they can force customers, after purchase, to continue to use their services. It's a terrible idea and you should not be trying to undermine existing "right to repair" capabilities.
Matt Berninger Against themself	As 15+ veteran of the cybersecurity industry, having served in the federal government at DHS/ US-CERT, in the US Navy as a Cryptologic Warfare Officer, and in private industry for over a decade protecting critical infrastructure networks, I believe this bill is a bad idea. As a Coloradan living and raising a family in the Denver metro area, I believe it is has the potential to cause harm. For decades, attackers have been able to weaponize software weaknesses faster than defenders could patch them. A contributing factor is the sometimes slow cadence with which vendors make a patch available - if they do at all. This leaves an attack window open for a motivated attacker. The relative difficulty of developing these weaponized exploits, and the deterrent effect of avoiding armed conflict, have historically helped to shield US critical infrastructure from significant attack. However, an

	increasingly unstable geopolitical context and active shooting wars have made this deterrent less relevant. Recently, Iranian cyber teams have been engaged in destructive attacks against US critical infrastructure; where in the past they may have stopped at the door for fear of retaliation, they are now breaking in and flipping switches to see what they can break. After all, what do they have to lose? At the same time, the difficulty of developing these exploits has dramatically decreased due to advances in artificial intelligence. Thus it is no longer a handful of adversaries with this capability.; it is anyone with access to an AI model and the right motivations. Two of the main constraints mitigating serious attacks on US critical infrastructure are rapidly deteriorating. Left in all this is the critical infrastructure owner and operator. They operate technology which will inevitably have exploitable vulnerabilities. Those weaknesses are likely to be found - and now exploited - before the vendors can issue a proper patch. If this bill passes, that operator may have to decide between fixing a bug that poses real risk, or waiting for the vendor to give them permission. Put simply, we may be asking our critical infrastructure operators to choose between community safety or future business risk. Ideally, all vendors will be able to develop and release patches in time. History has proven otherwise. If they don't, our critical infrastructure owners and operators should be free to take actions to protect the Colorado communities they serve.
Rachel Cochran Against themself	I have worked in technology/information security for over 15 years, including for a company designated as a critical infrastructure provider in the US. As part of this work, I have dealt with a great deal of policy development and enforcement. SB26-090 is so exceedingly vague, it would be usable to gut Coloradoâ€™s right to repair on nearly every front. Any half decent lawyer could leverage the language in this bill to exempt their client companies from needing to support repair. And itâ€™s what will happen, as companies donâ€™t want spend the time and money to make things repairable. They make more money, the less you are able to repair existing equipment.
Rick SALTZMAN	Coloradoâ€™s right-to-repair law reflected a sound instinct: that operators should have meaningful ability to maintain and repair the

Against themself	systems they rely on. Senate Bill 90 would retreat from that principle in the environments where it matters most, in exchange for a security benefit the evidence does not support. If lawmakers want to improve cybersecurity outcomes in critical infrastructure, the focus should be on manufacturer accountability: secure defaults, vulnerability disclosure, lifecycle transparency and timely patching. These are the conditions that determine whether systems can withstand attack and recover when they fail. Senate Bill 90 does not move us in that direction. Legislators should direct their efforts toward the harder, more consequential work of holding manufacturers to a higher standard. In fact, we should be sure that products considered "Critical Infrastructure" should adhere to our right-repair laws. Imagine a situation where a battery needs to replaced on a product but only the manufacturer's service technician is able to do this repair. In a critical situation, the product should repairable by anyone, urgently without incurring the delay of a repair by the manufacturer's technician.
Sylvia Killinen Against themself	I am an information security professional, and I want to mark my opposition to SB26-090. Rather than defending the actual security of equipment used in Colorado, SB26-090 would instead prevent maintenance on any hardware a company can claim is critical. No piece of hardware can be considered critical infrastructure without knowing its context. The same monitor that sits on a school child's desk may be used in a data center handling critical processes. The school child should not be prevented from learning about their own equipment, and the child's family should not be prevented from repairing it, simply because an identical monitor may be used elsewhere. In addition, there is no security gain from preventing repair. It is completely unreasonable to assume that any hardware currently on the market is not already in an adversary's hands; all it does is force people who own equipment to replace, rather than repair. SB26-090 will only protect equipment manufacturers' bottom line, not security, and certainly not ordinary people.
Theresa Beazer Against themself	This bill doesnâ€™t help the infosec community. It helps big companies make more money. Understanding how things are made allows us to know when someone replaces a chip or bypasses a hardware control. The right to repair helps the environment by being able to affordably

	maintain infrastructure while not constantly paying large companies to maintain Infrastructure with their specialized up charges.
Wayne Seltzer Against themself	I am writing to urge you to reject "SB26-090 Exempt Critical Infrastructure from Right to Repair." This bill is clearly an attempt of Cisco, IBM, Oracle and other manufacturers to carve out right-to-repair exemptions for their products to protect their lucrative service contracts from 3rd parties. This bill will not benefit consumers and businesses! Only the manufacturers who support the bill. Even worse, the vague use of "Critical Infrastructure" could render all products exempt from our right-to-repair law. Colorado does not want that -- and neither should any other state. No doubt we all agree that products used in "Critical Infrastructure" applications need to have strong security. However, this bill suggests that there are products that are inherently "Critical Infrastructure." This is misleading -- a product is not itself "Critical Infrastructure." For example, if a cell phone or network router are used in a secure military facility, they may be "Critical Infrastructure." The idea that publishing service manuals compromises security of such products is incorrect. Security is a product design issue, not a right-to-repair issue. If security can be defeated by reading the information in "secret" repair documentation, the product is NOT secure. In fact, we should be sure that products considered "Critical Infrastructure" should adhere to our right-repair laws. Imagine a situation where a battery needs to replaced on a product but only the manufacturer's service technician is able to do this repair. In a critical situation, the product should repairable by anyone, urgently without incurring the delay of a repair by the manufacturer's technician.

	Please don't let that happen. If the manufacturers who are in support of this bill are interesting in obtaining an exemption to HB24-1121 for a specific list of products, I would reluctantly support such an amendment. Such products might be inherently insecure, as access to the service/repair manual would enable a bad actor to compromise some "critical infrastructure." In fact, such products should be improved so that "security by obscurity" did not apply. Please vote no on this over-reaching bill and maintain Colorado's right-to-repair law. Best Regards, Wayne Seltzer Boulder, CO founder of the Boulder U-Fix-It Clinic http://boulderufixitclinic.org
William Tiemann Against themself	It is a bad idea to give companies the right to override public policy by pretending something is critical that is not. this is a bad bill being taken forward in bad faith. Vote no on removing any right to repair.
. Lucky225 Against themself	Stop breaking right to repair. Critical infrastructure requires more access -- not less -- as contractors need to be able to perform repairs immediately during an emergency. Use simple logic you morons.