SB-090

Matt Fussa

Vice President, Trust & Compliance Officer

As Cisco's Vice President, Trust & Compliance Officer, Matt Fussa leads a global team of technical and business professionals, including country cybersecurity officers and compliance experts. The Trust & Compliance Office partners with government cybersecurity agencies and customers to share security best practices and shape both cyber risk management and security regulations. Matt has responsibility for maintaining customer trust across SaaS, hardware, and data security compliance for Cisco.

With over two decades of leadership experience in the public and private sectors, Matt has made significant contributions to Cisco's success by leading efforts to enhance SaaS market access and obtaining essential certifications such as FedRAMP, ISO 27001, SOC 2, and EUCS. Other key accomplishments have included overseeing Cisco's focused strategy to combat counterfeiting and managing the response to government, law enforcement, and national security data demands.

Matt began his career at Cisco as lead legal counsel for the Global Government Solutions Group and eventually led legal support across the Americas regions, managing a large team of attorneys on business transactions, financing, regulatory compliance, acquisitions and integration, and the divestiture of legacy products from the Cisco portfolio. Following that success, he was selected to be the Cisco Scholar in Residence at the Woodrow Wilson International Center for Scholars in Washington, D.C., where he studied cybersecurity policy and worked closely with industry leaders and government officials. In his current role, he and his team are viewed as trusted advisors to Cisco's executive leadership team on matters of cybersecurity risk and regulatory compliance.

Matt is also a decorated U.S. Marine, where he served as a platoon and company commander, an international law specialist at the Pentagon, and held various senior legal leadership positions in the operating forces before retiring from the Marine Corps Reserves.

Testimony of Matt Fussa, Vice President and Trust Officer, Cisco Systems

Before the Colorado House State, Civic, Military, & Veterans Affairs Committee
Re: SB26-090 — Amendments to the Consumer Repair Bill of Rights Hearing: Monday, April 27, 2026

Chair Willford, Vice Chair Clifford, and members of the committee — thank you for the opportunity to testify today. My name is Matt Fussa. I serve as Vice President and Trust Officer at Cisco Systems, where I lead a global team that works with government agencies, regulators, and customers to help shape cybersecurity policy and manage cyber risk.

Cisco designs and builds the networking equipment — the routers, switches, and security infrastructure — that sits at the core of Colorado's critical infrastructure. We understand, as deeply as anyone, how consequential the security of those systems is.

Before I get into the substance of the bill, I want to share a quick observation from my trip here. I traveled this morning from Raleigh, North Carolina to be with you in Denver. Between the moment I left my house and the moment I walked into this hearing room, I relied — without thinking about it — on a remarkable chain of critical infrastructure. The air traffic control systems that safely guided my flight. The communications networks that kept the pilots, the tower, and the ground crews in sync. The train that carried me from Denver International Airport into the city. The traffic systems on the way to the Capitol. The electricity generation and distribution that lights this room. The water system. The financial networks that processed my coffee purchase this morning. It is very likely that Cisco technology was quietly at work in every single one of those systems. That is the reality of modern critical infrastructure — invisible when it works, catastrophic when it doesn't. And that is the reality this committee is legislating around today.

I want to be clear: Cisco supports the principle of right to repair. People and businesses should have fair, affordable options to repair the products they own. That principle is sound, and Colorado was right to advance it.

But repair policy must be written carefully. Not all digital technology is the same. A router used in a home is fundamentally different from the industrial-grade equipment used to manage a power grid, operate a

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Phone: 408 526-4000
Fax: 408 526-4100
www.cisco.com

hospital, or secure a state agency's confidential data. When a one-size-fits-all approach is applied to this kind of equipment, it can unintentionally grant unrestricted access to sensitive personal data, source code, encryption keys, and intellectual property. At a time when sophisticated nation-state actors are constantly evolving their tactics, the forced disclosure of proprietary technical information effectively creates a blueprint for cyberattacks against the systems Coloradans rely on every day.

This is why SB26-090, as amended by the Senate, matters. The amended bill addresses that gap through a structured exemption process — one that requires review by the Attorney General and limits eligibility to equipment sold under business-to-business or business-to-government contracts and genuinely intended for critical infrastructure use.

Colorado's existing framework already recognizes the need for targeted exemptions — for EV chargers, and medical devices. SB26-090 simply extends that same common-sense logic to the networking and telecommunications equipment that underpins our most sensitive systems. The bill is additive. It does not roll back consumer repair rights. It does not touch the devices people buy off a shelf.

What it does do is recognize that critical infrastructure requires specialized training, rigorous vetting, and carefully managed security controls. At Cisco, we recover more than 90% of our devices for proper refurbishment through authorized channels — proving that secure repair and sustainability go hand in hand.

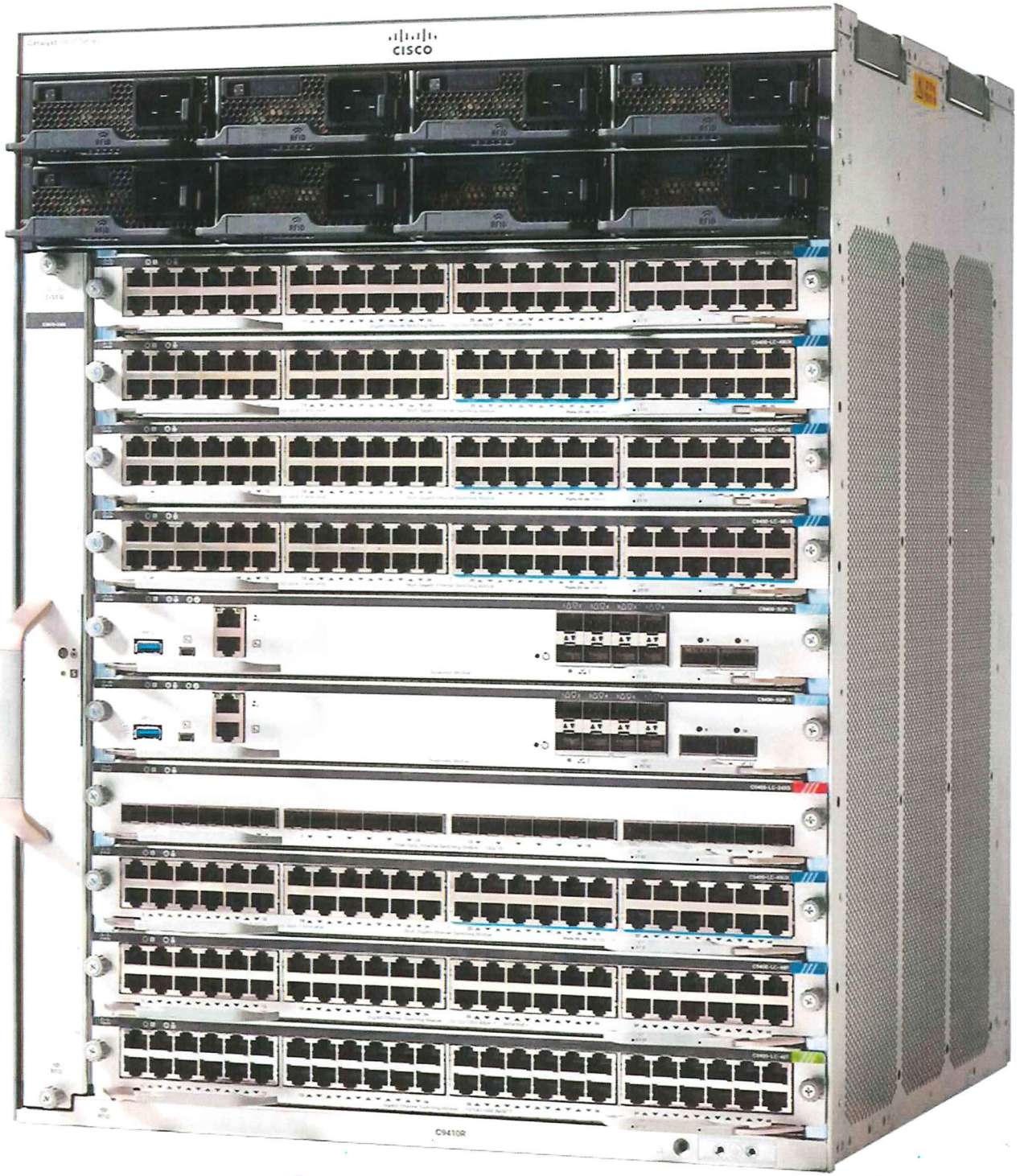
Colorado has an opportunity to show that repair access and security do not have to be in conflict. The amended SB26-090 protects consumer repair while safeguarding the services Coloradans depend on daily — their hospitals, utilities, transportation systems, and emergency services.

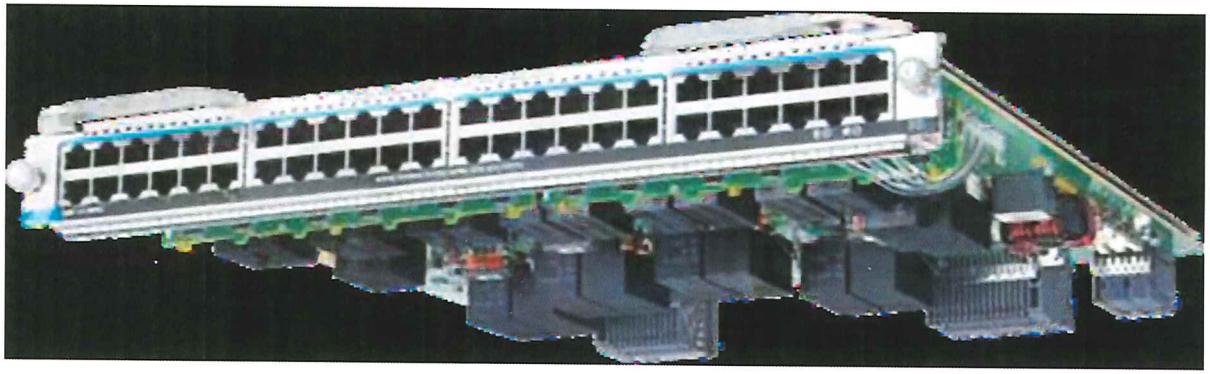
That is a responsible framework, and Cisco supports it. We respectfully ask the committee to advance the bill.

Thank you. I welcome any questions.

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706

Phone: 408 526-4000
Fax: 408 526-4100
www.cisco.com


cisco
C9410R



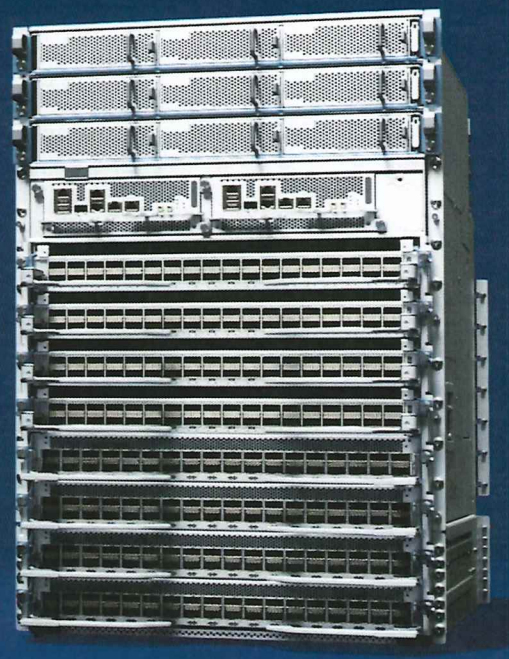
Cisco 8000 Series Routers

Get a network that grows with you

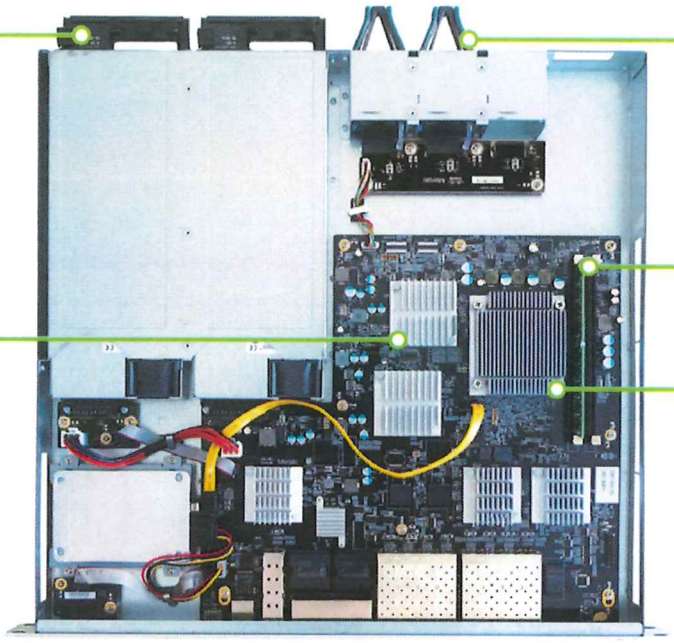
Get performance, functionality, and scalability you can count on with Cisco 8000 Series Routers powered by Cisco Silicon One ASICs.

Watch video

View models >



MX450 shown; interfaces and features vary by model and OS version



Redundant power

Reliable, energy-efficient design with field-replaceable power supplies

Cryptographic acceleration

Reduced load with hardware crypto assist

Modular fans

High-performance front-to-back cooling with field-replaceable fans

Additional memory

For high-performance content filtering

Enhanced CPU

Layer 3-7 firewall and traffic shaping

Front of the Cisco Meraki MX

MX450 shown; interfaces and features vary by model and OS version

Multicolor status LED

Monitor device status

Automatic cellular failover

Management interface

Local device access

Dual 10G WAN interfaces

Load balancing and SD-WAN

1G/10G Ethernet/SFP+ interfaces

10G SFP+ interfaces for high-speed LAN connectivity

Cisco Silicon One

The industry's only scalable and programmable unified networking architecture

Cisco Silicon One architecture delivers unmatched routing and switching capabilities for AI and networking needs for hyperscalers, data centers, service providers, and enterprises.

Watch video (01:48)

Contact us >