

NIST SP 800-171 Rev. 2 / CMMC Level 2

How Rio router features relate to the 110 security requirements.

Version 3, October 2026 · riorouter.com

This document maps the features of the Rio router to the 110 security requirements (controls) in NIST SP 800-171 Rev. 2, the technical basis of CMMC Level 2. Rio is a home and small-office router. It helps with practices at the network layer: a firewall at the internet boundary, isolated network segments, and admin approval of devices. It does not replace the policy, documentation, endpoint, identity, and encryption controls a complete program needs.

Rio does not make any organization CMMC compliant or certified. Your assessor decides whether a requirement is met in your environment. CMMC Phase 2 begins November 10, 2026. Have this mapping reviewed by a CMMC Registered Practitioner or Registered Practitioner Organization (RPO) before you use it in a System Security Plan (SSP).

2 SUPPORTS A Rio feature directly supports this requirement at the network layer. You configure and document it; your assessor decides.	13 PARTIAL A Rio feature covers part of this requirement. Other tools, policies, or procedures are needed for the rest.	95 NOT ADDRESSED Rio does not address this requirement. It must be met by other systems, policies, or procedures.
--	--	--

How Segmentation Can Help With Assessment Scope

Under CMMC, assessment scope depends on which assets process, store, or transmit CUI and which assets protect them. On a flat network, where every device shares one segment, it is hard to show that other devices are separated from CUI. SecureRooms let you put CUI devices in their own isolated room, which can support a smaller, clearly defined CUI enclave.

For example, in a 10-person shop where 3 people handle CUI, keeping those devices in a dedicated room helps you show that the other devices are separated from CUI. Whether those other assets are out of scope is decided under the CMMC scoping guidance and by your assessor. Rio itself protects the enclave, so it is a Security Protection Asset and is in scope.

Where Rio helps most: network segmentation (3.13.5) and authorizing devices before they use your Wi-Fi (3.1.16). Rio also partly supports boundary protection (3.13.1), deny-by-default traffic rules (3.13.6), and wireless protection (3.1.17).

System & Communications Protection (SC)

16 controls · Supports: 1 · Partial: 3 · Not addressed: 12

CONTROL	STATUS	RIO FEATURE	WHAT RIO DOES AND DOES NOT DO
3.13.1 Boundary protection	PARTIAL	Firewall + SecureRooms + activity log	Rio sits at the internet boundary with a stateful firewall and NAT that block unsolicited inbound connections, and remote management of the router is off by default. SecureRooms create internal boundaries: devices in different rooms are isolated from each other. Monitoring is limited to the activity log of network events in the app. Deeper boundary monitoring (traffic analysis, intrusion detection, log retention) needs separate tools.
3.13.2 Security engineering	PARTIAL	SecureRooms + firewall	Rio's room segmentation and default blocking of inbound traffic can be part of a documented, segmented network design. This requirement covers architecture, development, and engineering practices across your whole CUI environment, which you define and document.
3.13.3 Role separation	NOT ADDRESSED	None	Separating user functions from system management functions is an operating system and application control. Network segmentation does not address it.
3.13.4 Shared resource control	NOT ADDRESSED	None	Preventing information transfer through shared system resources (such as shared memory) is an operating system control. Network segmentation does not address it.
3.13.5 Public-access subnetworks	SUPPORTS	SecureRooms	SecureRooms provide up to 16 isolated network segments on Rio's Wi-Fi networks, plus a wired LAN room. Devices in different rooms are isolated from each other, so guest or publicly accessible devices can be kept in a room separate from devices that handle CUI. Put CUI devices in a dedicated room and record the room layout in your SSP.
3.13.6 Deny by default	PARTIAL	Firewall + device approval	The firewall blocks unsolicited inbound traffic from the internet, and devices in different rooms are isolated from each other. Device approval can hold new devices in a Pending state until an admin approves them. Outbound internet traffic from approved devices is allowed by default. If your assessor expects outbound traffic to be denied by default as well, you will need additional controls.
3.13.7 Split tunneling	NOT ADDRESSED	None	Split tunneling concerns remote devices (such as a laptop at home) connected to your network through a remote-access VPN. Rio VPN is an outbound privacy VPN for the internet traffic of rooms you assign to a VPN tunnel. It does not provide remote access, so it cannot prevent split tunneling on remote devices. Use the settings of your remote-access solution for this requirement.

CONTROL	STATUS	RIO FEATURE	WHAT RIO DOES AND DOES NOT DO
3.13.8 Data in transit	NOT ADDRESSED	None	Rio VPN encrypts internet traffic from rooms assigned to a VPN tunnel, but only between the router and the VPN service, and Rio has not confirmed FIPS validation of its cryptographic module. Wi-Fi traffic is encrypted with WPA2 (AES) on the local wireless link only. Protecting CUI in transit requires FIPS-validated cryptography (see 3.13.11), so do not rely on Rio here. Use FIPS-validated encryption end to end, such as TLS in your CUI applications.
3.13.9 Connection termination	NOT ADDRESSED	None	This requirement ends network connections at the end of a session or after a set period of inactivity. Rio does not provide session-termination settings you can configure and document for this purpose. Use your remote-access, application, and operating system settings.
3.13.10 Key management	NOT ADDRESSED	None	Rio VPN keys are generated and managed automatically, not by you, and Rio VPN is not relied on for CUI (see 3.13.11). You set and can change the Wi-Fi passphrase in the Rio app; include it in your key management procedures. Establishing and managing cryptographic keys for your systems is your responsibility.
3.13.11 FIPS-validated cryptography	NOT ADDRESSED	None	Requires FIPS-validated cryptography wherever cryptography protects CUI. Rio has not confirmed FIPS 140-2 or 140-3 validation of Rio VPN's cryptographic module or of the router's Wi-Fi encryption. Do not rely on Rio VPN or Rio Wi-Fi encryption for this requirement or for any requirement that depends on it. Treat it as not addressed by Rio.
3.13.12 Collaborative devices	NOT ADDRESSED	None	Blocking remote activation of cameras and microphones is controlled on the endpoint device. A network device cannot address it.
3.13.13 Mobile code	NOT ADDRESSED	None	Mobile code (such as scripts and browser plug-ins) is controlled through endpoint and browser settings.
3.13.14 Voice over IP	NOT ADDRESSED	None	Controlling and monitoring VoIP is an application-layer control. Rio carries VoIP traffic like any other traffic but does not control or monitor VoIP specifically.
3.13.15 Session authenticity	NOT ADDRESSED	None	Protecting sessions against hijacking or false information comes from protocols such as TLS between endpoints and services. Rio VPN is not relied on (see 3.13.11), and device approval does not protect individual sessions.
3.13.16 Data at rest	NOT ADDRESSED	None	Protecting CUI at rest is a storage and endpoint control, such as full-disk encryption. Rio handles network traffic, not stored data.

Access Control (AC)

22 controls · Supports: 1 · Partial: 5 · Not addressed: 16

CONTROL	STATUS	RIO FEATURE	WHAT RIO DOES AND DOES NOT DO
3.1.1 Authorized access	PARTIAL	Device approval	Device approval lets an admin hold new devices in a Pending state, approve them in the Rio app, or block them. This limits which devices can join the network. Limiting access by user and by process requires identity and operating system controls.
3.1.2 Transactions and functions	NOT ADDRESSED	None	Limiting the transactions and functions a user may perform is an application and identity control.
3.1.3 Control CUI flow	PARTIAL	SecureRooms	Devices in different rooms are isolated from each other, so placing CUI devices in their own room limits where CUI can travel on your local network. Rio is not a data loss prevention tool. Controlling which information goes where (for example, to email or cloud services) requires endpoint, application, and data controls.
3.1.4 Separation of duties	NOT ADDRESSED	None	Separation of duties is an organizational and identity control.
3.1.5 Least privilege	NOT ADDRESSED	None	Least privilege for user accounts is an operating system and identity control.
3.1.6 Non-privileged accounts	NOT ADDRESSED	None	Using non-privileged accounts for everyday work is an operating system and identity control.
3.1.7 Privileged functions	NOT ADDRESSED	None	Preventing non-privileged users from running privileged functions, and logging those functions, is an operating system control.
3.1.8 Unsuccessful logons	NOT ADDRESSED	None	Limiting unsuccessful logon attempts on user accounts is an identity control.
3.1.9 Privacy and security notices	NOT ADDRESSED	None	Privacy and security notices (logon banners) are set on endpoints and applications.
3.1.10 Session lock	NOT ADDRESSED	None	Session lock with a pattern-hiding display is an endpoint operating system setting.
3.1.11 Session termination	NOT ADDRESSED	None	Automatically ending user sessions is set in operating systems and applications.
3.1.12 Monitor remote access	NOT ADDRESSED	None	Rio does not provide remote access into your network. Rio VPN is an outbound privacy VPN, not a remote-access VPN, so it does not monitor or control remote access sessions. If you allow remote access, use a separate remote-access solution that logs and controls sessions.

CONTROL	STATUS	RIO FEATURE	WHAT RIO DOES AND DOES NOT DO
3.1.13 Remote access encryption	NOT ADDRESSED	None	Rio does not provide remote access sessions, and Rio has not confirmed FIPS validation of Rio VPN's cryptographic module. FIPS-validated encryption of remote access sessions must come from your remote-access solution.
3.1.14 Remote access routing	NOT ADDRESSED	None	Rio does not provide or manage remote access. Remote management of the router is off by default and the firewall blocks unsolicited inbound connections, so Rio does not open a remote path into your network by itself. That can help you document a no-remote-access policy. If you permit remote access, routing it through managed access control points requires a separate remote-access solution.
3.1.15 Privileged remote access	NOT ADDRESSED	None	Authorizing remote execution of privileged commands is a policy, identity, and remote-access control. Rio does not provide remote access.
3.1.16 Authorize wireless access	SUPPORTS	Device approval	With device approval in use, new devices are held in a Pending state until an admin approves them in the Rio app, and devices can be blocked at any time. Joining Rio Wi-Fi also requires the WPA2 passphrase. Turn on device approval and document your approval process in your SSP.
3.1.17 Protect wireless access	PARTIAL	WPA2 Wi-Fi + device approval	Rio Wi-Fi uses WPA2 Personal with AES encryption, and device approval adds an admin check on each new device. WPA2 Personal uses one shared passphrase rather than individual credentials, and Rio has not confirmed FIPS validation of its Wi-Fi encryption. If CUI crosses Wi-Fi, protect it with FIPS-validated encryption on the endpoints or in the applications, or connect CUI devices by wire.
3.1.18 Mobile device connection	PARTIAL	Device approval	With device approval on, phones, tablets, and laptops must be approved before they can use the Rio network, and they can be blocked at any time. This requirement also covers how mobile devices are configured and used wherever they connect, which requires mobile device management (MDM) and policy.
3.1.19 Encrypt CUI on mobile	NOT ADDRESSED	None	Encrypting CUI stored on mobile devices is a device-level control, such as MDM or full-disk encryption. Rio does not address data at rest.
3.1.20 External connections	PARTIAL	Device approval + SecureRooms	Device approval and room isolation limit which outside devices (such as personal or visitor devices) can join your network, and keep them away from CUI devices. Verifying and limiting your use of external systems and services (cloud services, personal accounts, partner systems) is a policy and identity control that Rio does not address.

CONTROL	STATUS	RIO FEATURE	WHAT RIO DOES AND DOES NOT DO
3.1.21 Portable storage	NOT ADDRESSED	None	Limiting portable storage devices on external systems is an endpoint and policy control.
3.1.22 Publicly accessible content	NOT ADDRESSED	None	Controlling CUI on publicly accessible systems (such as websites) is a policy and content control.

Identification & Authentication (IA)

11 controls · Partial: 2 · Not addressed: 9 · 3 shown here, 8 in Remaining Families

CONTROL	STATUS	RIO FEATURE	WHAT RIO DOES AND DOES NOT DO
3.5.1 Identification	PARTIAL	Device list + device approval	The Rio app lists each device on the network by its hardware (MAC) address, and device approval records which devices an admin has approved. This identifies devices only. MAC addresses can be imitated, and identifying users and processes requires an identity system.
3.5.2 Authentication	PARTIAL	WPA2 passphrase + device approval	Joining Rio Wi-Fi requires the WPA2 passphrase, and device approval can require an admin to approve each new device. This is a shared passphrase plus admin approval by hardware address, not cryptographic authentication of individual devices or users. Authenticating users and processes requires an identity provider.
3.5.3 Multifactor authentication	NOT ADDRESSED	None	Multifactor authentication for user accounts comes from an identity provider or MFA product. Rio does not provide user MFA.

Audit & Accountability (AU)

9 controls · Partial: 1 · Not addressed: 8 · 1 shown here, 8 in Remaining Families

CONTROL	STATUS	RIO FEATURE	WHAT RIO DOES AND DOES NOT DO
3.3.1 System auditing	PARTIAL	Activity log	The Rio app keeps an activity log of network events, which gives you network-level records to review. Full audit logging (operating system, application, and user activity), log retention, and analysis require separate logging or SIEM tools.

Configuration Management (CM)

9 controls · Partial: 2 · Not addressed: 7 · 2 shown here, 7 in Remaining Families

CONTROL	STATUS	RIO FEATURE	WHAT RIO DOES AND DOES NOT DO
3.4.1 Baselines and inventory	PARTIAL	Device list	The device list in the Rio app shows the devices on your network and can feed your hardware inventory. Baseline configurations and inventories of hardware, software, firmware, and documentation require asset management tools and procedures.
3.4.2 Security configuration	PARTIAL	Router settings	Rio's security settings (rooms, device approval, remote management off by default, Wi-Fi passphrase) are set in the app and can be recorded in your SSP. Security settings for your computers, servers, and applications are outside Rio.

Remaining Control Families (Not Addressed by Rio)

These 66 requirements fall outside what a network router does. They must be met by other parts of your CMMC Level 2 program: policy, endpoint security, identity management, physical security, and documentation. Rio does not address them, but a well-defined CUI enclave can reduce the number of systems they apply to.

FAMILY	CODE	COUNT	WHY RIO DOES NOT ADDRESS IT
Awareness & Training	AT	3	Security awareness and training programs. Handled through personnel policy, not network equipment.
Audit & Accountability (remaining)	AU	8	Audit review, alerting, time stamps, log protection, and retention. Rio's activity log contributes network events; the rest needs logging infrastructure.
Configuration Management (remaining)	CM	7	Change control, least functionality, and software restrictions. Rio's own settings are one input; system-wide controls are outside Rio.
Identification & Authentication (remaining)	IA	8	Identifier management, password rules, replay-resistant authentication, and related user identity controls. Handled by an identity provider and operating system settings.
Incident Response	IR	3	Incident handling, reporting, and testing. Process and policy controls.
Maintenance	MA	6	System maintenance procedures and maintenance personnel access. Organizational controls.
Media Protection	MP	9	Physical media handling, sanitization, and transport. Not network-layer.
Personnel Security	PS	2	Personnel screening and termination procedures. Human resources controls.
Physical Protection	PE	6	Facility access, visitor controls, and physical monitoring. Physical security controls.
Risk Assessment	RA	3	Risk assessment and vulnerability scanning procedures.

FAMILY	CODE	COUNT	WHY RIO DOES NOT ADDRESS IT
Security Assessment	CA	4	Security assessment, plan of action, system security plan, and continuous monitoring procedures.
System & Information Integrity	SI	7	Flaw remediation, malicious code protection, and system monitoring. Endpoint and application-layer controls.

Important Notes

About Rio VPN

Rio VPN is an outbound privacy VPN (WireGuard, IKEv2, or OpenVPN through the WLVPN service). The router sends the internet traffic of each room you assign to a VPN tunnel through that tunnel; two tunnels are available. It is assigned per room, not applied to all traffic by default. It is not a remote-access VPN: it does not let remote employees connect into your office network, so it provides no remote-access session control. Rio VPN requires a subscription after the included first year. Because FIPS validation of its cryptographic module is not confirmed, this mapping does not credit Rio VPN for any requirement.

FIPS-Validated Cryptography (3.13.11)

Requirement 3.13.11 calls for FIPS-validated cryptography wherever cryptography protects the confidentiality of CUI. It carries 5 points in the DoD assessment scoring methodology, among the highest weights. Rio has not confirmed FIPS 140-2 or 140-3 validation of Rio VPN's cryptographic module or of the router's Wi-Fi encryption. Do not rely on Rio VPN or Rio Wi-Fi encryption for 3.13.11 or for requirements that depend on it, such as 3.13.8 and 3.1.13. Treat them as not addressed by Rio, and meet them with FIPS-validated encryption on your endpoints, in your applications, and in your remote-access solution.

What Rio Does Not Cover

Rio is not a complete CMMC solution. A Level 2 program also needs:

- **Remote access.** Rio provides no remote-access VPN or session control (3.1.12 to 3.1.15, 3.13.7).
- **FIPS-validated encryption of CUI**, in transit and at rest (3.13.8, 3.13.11, 3.13.16, 3.1.19).
- **User identity.** User accounts, password rules, and multifactor authentication (3.5.3 and most of IA).
- **Endpoint security.** Malware protection, patching, and secure configuration of computers and phones (SI, CM).
- **Audit logging.** Full audit records, log retention, and review (AU).
- **Data loss prevention.** Control over what information leaves your network.
- **Cloud email and file sharing for CUI** that meets FedRAMP Moderate or equivalent requirements (DFARS 252.204-7012).
- **Program work.** Policies, training, physical security, incident response, an SSP covering all 110 requirements, a POA&M where allowed, and the assessment itself.

A well-defined CUI enclave can reduce how many systems these controls apply to, but Rio does not perform them.

Rio Itself Is In Scope

As the device that protects your CUI enclave, Rio is a Security Protection Asset. Include it in your asset inventory, network diagram, and SSP. Install router firmware updates when Rio provides them, limit admin app access to authorized administrators, and leave remote management off unless you have a documented need.

Documentation Your Assessor Will Ask For

For each requirement Rio supports or partially supports, your SSP should record:

- Your room layout and which devices are in each room. Keep CUI devices in a dedicated room. Wired devices share the wired LAN room, so if CUI devices are wired, keep non-CUI devices off the wired LAN.
- Whether device approval is on, and who approves and blocks devices.
- That remote management of the router is off.
- Any rooms assigned to a VPN tunnel, noting that Rio VPN is not relied on to protect CUI.
- A network diagram showing the CUI enclave boundary.

Professional Review

This document is Rio's own technical analysis of how its features relate to NIST SP 800-171 requirements. It is not an assessment, a certification, or a guarantee. Before using it in an SSP, have it reviewed by a CMMC Registered Practitioner, an RPO, or another qualified advisor who knows your environment. Only your assessment determines your CMMC status.

Changes From Version 2

Version 3 corrects statements about Rio VPN, which is an outbound, per-room privacy VPN and not a remote-access VPN, and about FIPS validation, which Rio has not confirmed. Re-rated: 3.13.1, 3.13.6, 3.1.17, 3.1.18, and 3.1.20 (Addresses to Partial); 3.13.7 and 3.1.14 (Addresses to Not addressed); 3.13.8, 3.13.9, 3.13.10, 3.13.11, 3.13.15, 3.1.12, and 3.1.13 (Partial to Not addressed). The label Addresses is now Supports, and N/A is now Not addressed, because these requirements still apply to you. If your SSP cites Version 2, update it.

Questions about this mapping or Rio's role in your compliance program: contact Rio at riorouter.com.