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

Feature mapping against the 110 security controls.

Version June 2026 · riorouter.com

This document maps Rio Router's native hardware features against the 110 security controls in NIST SP 800-171 Rev. 2, which forms the technical basis of CMMC 2.0 Level 2. Rio addresses the network infrastructure layer of a CMMC program and does not replace the policy, documentation, endpoint, or identity controls a complete program requires. Controls outside Rio's architectural scope are listed as Not Applicable and should be addressed through other parts of your compliance stack. This mapping should be reviewed by a CMMC Registered Practitioner or C3PAO before inclusion in a System Security Plan.

9	15	86
ADDRESSES	PARTIAL	N/A
Rio directly addresses the requirement at the network layer.	Rio contributes; additional controls are required for full coverage.	Outside Rio's architectural scope; addressed by policy, endpoint, or other systems.

How Rio Reduces Your Assessment Scope

Under NIST 800-171 and CMMC, compliance cost and assessment scope scale directly with the size of the CUI environment. A contractor with a flat network, where all devices share one segment, must apply controls across every in-scope device. Rio's SecureRoom VLAN segmentation creates a technically enforced boundary around the CUI enclave. The C3PAO assessor evaluates what is inside the boundary; everything outside is out of scope.

For a 10-person shop where 3 people handle CUI, the difference between a flat network and a Rio-segmented network can reduce in-scope assets from dozens to a handful. That reduction cascades to lower assessment fees, fewer remediation items, less documentation burden, and faster time to certification. The controls Rio addresses are also the infrastructure controls that are hardest to implement otherwise: network segmentation (3.13.5), deny-all access (3.13.6), no split tunneling (3.13.7), encryption in transit (3.13.8), and wireless device authorization (3.1.16 and 3.1.17).

System & Communications Protection (SC)

16 controls · 4 Addresses · 6 Partial · 6 N/A

CONTROL	STATUS	RIO FEATURE	TECHNICAL BASIS
3.13.1	ADDRESSES	**Rio Router + SecureRoom + VPN**	Rio is the external boundary device. It monitors all inbound and outbound traffic, controls access via allowlisting, and protects communications via VPN encryption. SecureRoom creates monitored internal boundaries between network segments.
3.13.2	PARTIAL	**Zero-Trust architecture**	Rio's network architecture follows Zero-Trust principles. Full satisfaction of this control requires documented systems engineering and architectural standards across the entire CUI environment, not only the network layer.
3.13.3	N/A	—	Separating user functionality from system management is an OS/UI-level control. Network VLAN segmentation does not address this.
3.13.4	N/A	—	Preventing information transfer via shared system resources (covert channels, shared memory) is an OS-level control. Network segmentation does not address this.
3.13.5	ADDRESSES	**SecureRoom (VLAN segmentation)**	SecureRoom creates up to 16 isolated VLAN subnetworks. CUI assets can be placed in a dedicated SecureRoom isolated from general business traffic and public-facing systems. Directly implements the required subnetwork separation.
3.13.6	ADDRESSES	**Zero-Trust Allowlisting**	Rio's core architecture is deny-all by default. Every device must be explicitly approved before gaining network access. This is the precise definition of 'deny all, permit by exception.'
3.13.7	ADDRESSES	**Always-on VPN**	Rio's always-on VPN eliminates split tunneling. All traffic from connected devices routes through the Rio VPN gateway. Remote devices cannot simultaneously maintain a direct connection to other networks.
3.13.8	PARTIAL	**Always-on VPN**	Rio's always-on VPN encrypts all data in transit. Full satisfaction is contingent on FIPS 140-2/140-3 validation of the cryptographic module (see 3.13.11). Pending FIPS verification.
3.13.9	PARTIAL	**Always-on VPN**	Rio VPN sessions can be configured with timeout parameters. Documentation of this configuration should be included in the SSP. Full satisfaction may require explicit policy documentation.
3.13.10	PARTIAL	**Always-on VPN**	Rio manages VPN cryptographic keys internally. Key management documentation should be included in the SSP. External key management practices are the organization's responsibility.

CONTROL	STATUS	RIO FEATURE	TECHNICAL BASIS
3.13.11	**PARTIAL**	**Always-on VPN**	Control requires FIPS 140-2 or 140-3 validated cryptographic modules. Rio customers should confirm the FIPS validation status of Rio's VPN implementation with Rio directly before claiming satisfaction in an SSP. This is a high-value control that cannot be addressed via POA&M.
3.13.12	N/A	—	Endpoint/device OS control (cameras, microphones). Network-layer device cannot address.
3.13.13	N/A	—	Endpoint security and browser control.
3.13.14	N/A	—	Application-layer control. Rio handles the network transport layer but does not inspect or control VoIP protocols specifically.
3.13.15	**PARTIAL**	**Always-on VPN + Allowlisting**	VPN encryption protects session authenticity in transit. Device allowlisting prevents unauthorized endpoints from initiating sessions. Application-layer session authentication is a separate control.
3.13.16	N/A	—	Encryption at rest is an endpoint/storage control. Rio handles data in transit only.

Access Control (AC)

22 controls · 5 Addresses · 4 Partial · 13 N/A

CONTROL	STATUS	RIO FEATURE	TECHNICAL BASIS
3.1.1	PARTIAL	**Zero-Trust Allowlisting**	Rio limits device access at the network layer via explicit admin approval. The control also requires limiting access by users and processes; user/process-level access management requires identity and OS controls.
3.1.2	N/A	—	Limiting the transactions and functions authorized users may execute is an application-layer authorization control. Not addressable by network hardware.
3.1.3	PARTIAL	**SecureRoom + Allowlisting**	Network segmentation physically constrains CUI data flows to the designated enclave. Inter-VLAN routing is blocked by default. Endpoint and application-layer controls are also required.
3.1.4	N/A	—	Duty separation is an organizational and identity management control. Not addressable by network hardware.
3.1.5	N/A	—	Least-privilege control of user account privileges is an OS and identity control. Not addressable by network hardware.
3.1.6	N/A	—	Account privilege management is an OS and identity control.
3.1.7	N/A	—	Endpoint and OS-level control.
3.1.8	N/A	—	Authentication management control.
3.1.9	N/A	—	Policy and UI control.
3.1.10	N/A	—	Endpoint OS control.
3.1.11	N/A	—	Session management control.
3.1.12	PARTIAL	**Always-on VPN**	All remote traffic is routed through Rio's always-on VPN tunnel. Rio controls whether remote connections are permitted and encrypts the session. Full monitoring requires additional logging or SIEM.
3.1.13	PARTIAL	**Always-on VPN**	Rio's always-on VPN encrypts all remote-access traffic. Full satisfaction is contingent on FIPS 140-2/140-3 validation of the cryptographic module (see 3.13.11). Pending FIPS verification.
3.1.14	ADDRESSES	**Always-on VPN + Allowlisting**	All remote traffic is routed through Rio, which serves as the single managed access control point. No split tunneling; all traffic passes through the controlled gateway.

CONTROL	STATUS	RIO FEATURE	TECHNICAL BASIS
3.1.15	N/A	—	Policy and endpoint control. Rio enforces that remote sessions go through the VPN, but authorization of specific privileged commands is a separate control.
3.1.16	ADDRESSES	**Zero-Trust Allowlisting**	Rio requires administrator approval before any wireless device joins the network. New devices are blocked by default until explicitly authorized through the mobile app.
3.1.17	ADDRESSES	**Allowlisting + Always-on VPN**	Wi-Fi authentication is enforced at the device level through allowlisting, and all wireless traffic is encrypted via the always-on VPN. Both authentication and encryption requirements are met.
3.1.18	ADDRESSES	**Zero-Trust Allowlisting**	Mobile devices must be explicitly approved before connecting to the Rio network. Applies to smartphones, tablets, and laptops. Unapproved mobile devices are denied network access.
3.1.19	N/A	—	This control requires encryption of CUI at rest on mobile devices, addressed via device-level controls such as MDM or full-disk encryption. Rio's in-transit VPN encryption does not satisfy at-rest requirements.
3.1.20	ADDRESSES	**Allowlisting + Always-on VPN**	Rio controls all connections leaving the network. The deny-by-default posture limits what external systems can be reached. VPN routes all external traffic through a controlled gateway.
3.1.21	N/A	—	Endpoint OS and hardware control.
3.1.22	N/A	—	Application and web content policy control.

Identification & Authentication (IA)

3 controls shown · 0 Addresses · 2 Partial · 1 N/A

CONTROL	STATUS	RIO FEATURE	TECHNICAL BASIS
3.5.1	PARTIAL	**Zero-Trust Allowlisting**	Rio identifies devices at the network layer (MAC address and device identity) before granting access. User-level identification requires additional identity management systems.
3.5.2	PARTIAL	**Zero-Trust Allowlisting**	Rio authenticates devices at the network layer. The control also covers authentication of users and processes, which requires an identity provider. Consistent with 3.5.1 scope.
3.5.3	N/A	—	MFA is a user authentication control (identity provider or MFA solution). Rio provides network-layer device authentication, not user-level MFA.

Audit & Accountability (AU)

1 control shown (Rio-relevant) · 1 Partial · remaining 8 out of scope

CONTROL	STATUS	RIO FEATURE	TECHNICAL BASIS
3.3.1	PARTIAL	**Rio Router (network logging)**	Rio logs network connection events, device approvals and rejections, and traffic. This provides network-layer audit data. Full audit log requirements (application, OS, user activity) require additional SIEM or logging tools.

Configuration Management (CM)

2 controls shown (Rio-relevant) · 2 Partial · remaining 7 out of scope

CONTROL	STATUS	RIO FEATURE	TECHNICAL BASIS
3.4.1	PARTIAL	**Allowlisting + Mobile App**	Rio maintains a record of all approved network devices (the allowlist). This constitutes a network device inventory. Broader system inventory (software, firmware) requires additional asset management tools.
3.4.2	PARTIAL	**Rio Router (managed configuration)**	Rio enforces network-layer security configurations (VLAN rules, VPN enforcement, access policies). Configuration of the Rio device itself should be documented in the SSP.

Remaining Control Families (Not Applicable)

The following control families fall outside the architectural scope of a network security device. They must be addressed by other parts of a complete CMMC Level 2 program: organizational policy, endpoint security, identity management, physical security, and documentation. Rio does not address these controls directly, but its enclave scoping can reduce the number of systems these controls must be applied to.

FAMILY	CODE	CONTROLS	WHY OUT OF SCOPE
Awareness & Training	**AT**	**3**	Organizational training programs. Addressed through personnel policy, not infrastructure.
Audit & Accountability (remaining)	**AU**	**8**	SIEM, application-layer logging, and log retention. Rio contributes network logs; other controls require additional logging infrastructure.
Configuration Management (remaining)	**CM**	**7**	Software inventory, configuration baselines, and change control. Rio addresses its own configuration; broader system controls are out of scope.
Incident Response	**IR**	**3**	Incident handling, reporting, and testing procedures. 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**	Organizational risk assessment and vulnerability scanning procedures.
Security Assessment	**CA**	**4**	Security assessment, plan of action, and continuous monitoring procedures.
System & Information Integrity	**SI**	**7**	Flaw remediation, malicious code protection, and monitoring. Endpoint and application-layer controls.

Important Notes

FIPS 140-2 / 140-3 Validation (Control 3.13.11)

Control 3.13.11 requires FIPS-validated cryptographic modules for CUI protection. It is one of the few NIST 800-171 controls that cannot be addressed via a Plan of Action & Milestones (POA&M); a failure can block certification. Rio customers should confirm the FIPS validation status of Rio's VPN implementation directly with Rio before claiming satisfaction in a System Security Plan.

Rio Is Not a Complete CMMC Solution

Rio addresses the network infrastructure layer. A complete CMMC Level 2 program also requires a FedRAMP-authorized email and file-sharing platform for CUI communications, endpoint protection and detection on CUI-handling devices, multi-factor authentication for user accounts, a System Security Plan documenting all 110 controls, and a C3PAO assessment. Rio reduces the scope and cost of each of these by shrinking the CUI enclave.

Documentation Requirements

For each control Rio addresses or partially addresses, the customer's System Security Plan must document the specific Rio configuration in use (VLAN setup, VPN enabled, allowlist active), network diagrams showing the CUI enclave boundary enforced by Rio, and the administrator responsible for managing device approvals. A CMMC assessor will ask for this evidence during the C3PAO assessment.

Professional Review

This document represents Rio's technical analysis of feature-to-control alignment. Before inclusion in any System Security Plan, customers are encouraged to have this mapping reviewed by a CMMC Registered Practitioner Organization (RPO) or C3PAO with knowledge of their specific environment.

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