HYPERPORT

DATASHEET

NERC CIP-005-7 & 03-09 Remote Access Reference Alignment Guide

This reference guide demonstrates how Hyperport's secure access platform addresses the technical and procedural requirements of NERC CIP-005-7 (Electronic Security Perimeters and Remote Access Management) and CIP-003-09 (Security Management Controls for Low-Impact BES Cyber Systems). Designed for utility compliance teams and auditors, this document maps Hyperport's capabilities to specific requirement parts across both standards, including Electronic Security Perimeter (ESP) controls, Interactive Remote Access (IRA) management, Multi-Factor Authentication (MFA), vendor session governance, and malicious communication detection. By consolidating remote access through a single authenticated gateway with comprehensive audit logging and session recording, Hyperport enables Responsible Entities to streamline compliance, reduce operational complexity, and maintain audit-ready evidence for both medium- and low-impact BES Cyber Systems.

Hyperport Inc. | Tel: +1 (925) 472-6898 | info@hyperport.io

CIP-005-7 Cyber Security – Electronic Security Perimeters

R1 – Electronic Security Perimeter (ESP)

Relevant Requirements

R1: Implement documented processes that include each applicable part in CIP-005-7 Table R1 – Electronic Security Perimeter.

1.1 – 1.2: All Cyber Assets using routable protocols shall reside within a defined ESP, and all external routable connectivity must pass through an identified Electronic Access Point (EAP).

1.3: Require inbound/outbound access permissions with stated justification and deny all other access by default.

1.4: Where technically feasible, authenticate all Dial-up Connectivity.

1.5: Have one or more methods to detect known or suspected malicious communications for both inbound and outbound traffic.

Hyperport Capabilities

1.1-1.2: Defined ESP & EAP Control: Hyperport appliances are deployed at ESP boundaries as the authorized Electronic Access Points. All routable traffic to or from BES Cyber Systems is routed through the Hyperport gateway, creating a single policy enforcement point and facilitating complete ESP documentation and change control.

1.3: Deny-by-Default & Policy Justification: Hyperport's Role- and Policy-Based Access Control (RBAC/PBAC) model enforces explicit allow rules for specific users, roles, protocols, and targets while denying all else by default. Each policy entry includes purpose, approval record, and change metadata to support audit traceability.

1.4: Authenticated Dial-up: If modem or cellular paths exist, Hyperport provides an authenticated routing path into the ESP, ensuring all sessions are verified through MFA and central identity controls before connectivity is established.

1.5: Malicious Communication Event Detection: Hyperport does not perform inline packet inspection or signature-based IDS/IPS functions. Instead, it monitors for unauthorized or abnormal connection attempts at the platform level and forwards those security events to external SIEM or IDS tools for correlation and analysis. This approach satisfies R1.5 by providing real-time event generation and integration with the organization's broader threat-detection stack.

Central Visibility & Auditability: A real-time dashboard lists all active connections, user identities, source and destination systems, and session status. Administrators can search, filter, and export connection records for audit evidence and annual ESP review documentation.

Hyperport Inc. | Tel: +1 (925) 472-6898 | info@hyperport.io

R2 – Remote Access Management

Relevant Requirements

R2: Implement documented processes that include each applicable part in CIP-005-7 Table R2 – Remote Access Management.

2.1: All Interactive Remote Access (IRA) must utilize an Intermediate System (IS) so that the initiating device does not directly access the target.

2.2: Encryption for IRA must terminate at the IS.

2.3: Require Multi-Factor Authentication for all IRA sessions.

2.4: Have methods to determine active vendor remote access sessions (IRA and system-to-system).

2.5: Have methods to disable active vendor remote access (IRA and system-to-system).

Hyperport Capabilities

2.1: Intermediate System: Hyperport functions as the required Intermediate System by routing all Interactive Remote Access sessions through a controlled gateway environment. External devices never communicate directly with BES Cyber Systems; instead, traffic routes through Hyperport's secure routing engine, where session initiation, identity validation, and authorization occur.

2.2: Encryption Termination at IS: TLS or IPsec encryption is established between the user endpoint and the Hyperport appliance and is then re-encrypted on the internal segment toward the target system. This architecture meets CIP requirements for encryption termination and segmentation at the IS.

2.3: Multi-Factor Authentication: Every IRA session requires MFA before launch. Hyperport supports federated identity providers (SAML 2.0, AD, Okta, Ping, LDAP) and hardware or software token methods (TOTP, FIDO2), accommodating both connected and air-gapped environments.

2.4: Active Vendor Session Determination: Administrators and auditors can view all active vendor sessions in real time through the dashboard or API. Each record shows vendor identity, source address, target asset, start time, and access type. Hyperport also exposes connection metadata to external logging systems for automated inventory and compliance evidence.

2.5: Disable Vendor Access: Administrators can immediately terminate a vendor session from the dashboard or command interface and revoke the vendor's credential or token to prevent reconnection. Session termination, account disablement, and policy changes are individually logged with timestamp and user identity.

Supplemental Controls – Session Monitoring & Recording: All web-based RDP, SSH, VNC, and browser sessions are recorded as video and keystroke logs for non-repudiation. Authorized administrators can view sessions in real-time and terminate them on demand.

Supplemental Controls – File Transfer Governance: Hyperport's File Deck module enables controlled upload/download of configuration or firmware files with malware scanning and moderated approval workflows. Scanning applies only to files moved through File Decks and not to general network traffic.

R3 – Vendor Remote Access Management for EACMS & PACS

Relevant Requirements

R3: Implement documented processes that include each applicable part in CIP-005-7 Table R3 – Vendor Remote Access Management for EACMS & PACS.

3.1: Have method(s) to determine authenticated vendor-initiated remote connections.

3.2: Have method(s) to terminate authenticated vendor-initiated connections and control the ability to reconnect.

Hyperport Capabilities

3.1: Determine Authenticated Vendor Connections: Hyperport records and displays all authenticated vendor-initiated connections to Electronic Access Control or Monitoring Systems (EACMS) and Physical Access Control Systems (PACS). Logs capture user identity, authentication method, source, destination, and timestamps.

3.2: Terminate & Control Reconnection: Operators can end any active vendor session (application session or user session) and prevent reconnection by disabling accounts or tokens, blocking source IP ranges, or revoking certificates. All actions are audited and can be exported for evidence.

Enhanced Evidence & Verification: Hyperport maintains tamper-resistant session recordings and event logs that demonstrate termination and reconnection control, satisfying and often exceeding R3 expectations.

Hyperport Inc. | Tel: +1 (925) 472-6898 | info@hyperport.io

CIP-003-09 Security Management Controls (Low-Impact BES Cyber Systems)

Attachment 1§3 – Electronic Access Controls

Relevant Requirements

> **3.1:** Permit only necessary inbound and outbound routable electronic access between a low-impact BES Cyber System and external Cyber Assets.
>
> **3.2:** Authenticate all dial-up connectivity (per Cyber Asset capability) that provides access to low-impact BES Cyber Systems.

Hyperport Capabilities

> **3.1: Routable Access Control:** Hyperport enforces a deny-by-default policy for all routable communication. Only approved ports, services, and destinations defined in policy are routed through the appliance. Access rules can be time-limited and role-scoped to adhere to the principle of least privilege.
>
> **3.2: Authentication of Dial-Up Connectivity:** Where technically feasible, any dial-up or cellular access path is routed through Hyperport and authenticated using MFA and the same centralized identity provider used for routable access.

Central Visibility & Auditability: A real-time dashboard lists all active connections, user identities, source and destination systems, and session status. Administrators can search, filter, and export connection records for audit evidence and annual ESP review documentation. All routable sessions are captured in the central event log, which includes user, protocol, result, and timestamp, resulting in immutable audit records.

Hyperport Inc. | Tel: +1 (925) 472-6898 | info@hyperport.io

Attachment 1§6 – Vendor Electronic Remote Access Security Controls (VERA)

Relevant Requirements

When vendor electronic remote access (ERA) is permitted under Section 3.1, implement one or more methods to:

6.1: Determine active vendor ERA

6.2: Disable vendor ERA.

6.3: Detect known or suspicious malicious communications for vendor ERA.

Hyperport Capabilities

6.1: Determine Vendor ERA: Hyperport automatically labels vendor accounts and displays all active vendor sessions in real time. Audit logs capture session purpose, duration, and approving authority.

6.2: Disable Vendor ERA: Administrators can instantly terminate vendor sessions, vendor accounts, or vendor group accounts and apply auto-expiry for time-of-need access. Entire vendor user groups can be turned off with a single action, taking effect immediately to ensure access is only granted when authorized.

6.3: Malicious Communication Detection: Hyperport does not inspect network traffic for malicious content. Instead, it scans files transferred through its File Deck module for malware and records all session activity for post-event forensic review. Alerts on unauthorized logins or policy violations are forwarded to external monitoring systems for correlation and response.

Session Monitoring & Recording: Full session capture (video and keystroke) and alerting on vendor log-ons meet and often exceed the evidence examples in Attachment 2 for VERA controls.

Control Theme	Hyperport Capability Highlights
ESP Definition & Enforcement	Centralized routing gateway at ESP boundary; deny-by-default rules; event logging and SIEM integration (R1.1–1.5)
Interactive Remote Access	Intermediate System architecture with encryption termination and MFA (R2.1–R2.3)
Vendor Remote Access (BCS)	Determine and disable vendor IRA and system-to-system sessions (R2.4–R2.5)
Vendor Access (EACMS/PACS)	Determine and terminate authenticated vendor connections; control reconnect (R3.1–R3.2)
Dial-up Access	Authenticated and routed through Hyperport using MFA and central identity controls (R1.4, CIP-003-9 §3.2)
Malicious Comms Visibility	Security-event logging and SIEM forwarding; file-transfer malware scanning (no inline IDS) (R1.5, §6.3)
Governance & Auditability	Session recording, immutable logs, change tracking, SIEM integration, and automated approval workflows across all access methods

CONCLUSION

Hyperport's secure access platform maps directly to the technical and procedural requirements in **CIP-005-7 (R1 – R3)** and **CIP-003-9 (§3 & §6).** By routing all interactive and vendor remote connections through a single, authenticated, policy-enforced gateway and maintaining immutable session records and SIEM-integrated audit logs, Hyperport enables Responsible Entities to meet or exceed NERC CIP obligations for remote access control, authentication, monitoring, and vendor management while simplifying deployment, operations, and audit validation.