पूर्व मध्य रेल
(निर्माण संगठन)

कार्यालय
मुख्य प्रशासनिक अधिकारी/निर्माण
पूमरे/महेन्द्रूघाट, पटना
दिनांक–23.03.2026

सं. ECR/CAO/Con/E/Misc

सर्व संबंधित
निर्माण संगठन/पूमरे।

विषय–Implementation of IR SOC over Indian Railways.
संदर्भ–(1)महाप्रबंधक/संकेत एवं दूरसंचार/पूमरे/हाजीपुर का पत्र सं.–ECR-HQ0SnT(Tele)/1/2024 (260056) dt. 10.03.2026
(2) Rly BD letter no. 2022/RBCC/7/7/SOC dtd. 06.03.2026

विषयांकित के आलोक में संदर्भित पत्र की छायाप्रति सूचनार्थ एवं अग्रेत्तर आवश्यक कार्रवाई हेतु इस पत्र के साथ संलग्न कर प्रेषित की जा रही है।

भारतीय रेलवे में Indian Railways Security Operations Centre (IR-SOC) Project का Implementation किया जा रहा है। जिसके तहत एक Central SOC एवं Sub SOCs की स्थापना कमशः रेलवे बोर्ड तथा रेलवे यूनिटों में किया जायेगा। इसके अलावे Cyber Security Solutation को Install करने हेतु HRMS पर Downloading के निर्देशों के साथ लिंक उपलब्ध रहेगा।

सूचनार्थ एवं अग्रिम कार्रवाई हेतु सादर प्रेषित।

संलग्नक–यथोक्त।

23/3/26
(सौरभ सावर्ण)
वरिष्ठ कार्मिक अधिकारी/निर्माण
कृते मुख्य प्रशासनिक अधिकारी/निर्माण

प्रतिलिपि :– निम्नलिखित को सादर सूचनार्थ एवं आवश्यक कार्यवाही हेतु प्रेषित।

- सचिव CAO/Con/South को CAO/Con/South महोदय के सादर सूचनार्थ।
- सचिव CAO/Con/North को CAO/Con/North महोदय के सादर सूचनार्थ।
- PS-II, CAO/C/RSP, Patna को CAO/C/RSP, Patna महोदय के सादर सूचनार्थ।
- PS-II, CAO/GLP, DNR को CAO/GLP, DNR महोदय के सादर सूचनार्थ।
- सभी CE/Con/MHX
- CSTE/Con/South एवं North/MHX.
- CEE/Con/South एवं North/MHX.
- सभी Dy. CE, Dy. CSTE, Dy. CEE/Con/ECR.
- Dy. FA&CAO/Con/MHX.
- SMM/Con/MHX
- सभी CSWI/Con/MHX.
- CA/Personnel - for uploading on WEBSITE of Construction Organisation.
- Ch. OS/R & D/Pers/Con/MHX.
- Ch. OS/Bill/Con/MHX.
- नोटिस बोर्ड।

पूर्व मध्य रेल
East Central Railway

International Year 2025 of Cooperatives
Cooperatives Build a Better World

प्रधान मुख्य सिगनल एवं दूरसंचार इंजीनियर का कार्यालय
हाजीपुर – 844 101
Office of the Principal Chief Signal & Telecommunication Engineer
Hajipur - 844 101

eFile no. ECR-HQ0SnT(TELE)/1/2024 (260056) **Dated. 10.03.2026**

PHODs/CHODs
East Central Railway, Hajipur,
CAO/Con/N & CAO/Con/S,
CAO/WP & CAO/ (DLF & GELF)
DRMs, DNR, DDU, DHN, SPJ & SEE
East Central Railway

Sub.: Implementation of IR SOC over Indian Railways.
Ref.: Rly BD letter no. No. 2022/RBCC/7/7/SOC dtd. 06.03.2026.

Please find enclosed Rly Bd dated 06.03.2026 wherein Indian Railways Security Operations Centre (IR-SOC) project is being implemented to strengthen the cyber security posture of Indian Railways. Under this project, a Central SOC and Sub SOCs are being established at Railway Board and Railway units. CRIS is the executing agency of this project.

In this connection, the cyber security solutions need to be installed and configured at endpoints, including network devices of each Sub-SOC. This will ensure endpoint protection (Antivirus), log collection, real-time monitoring, asset discovery, incident detection, vulnerability management and patch management etc. Details of cyber security solutions are enclosed as Annexure.

In addition, link for installation of cyber security solutions will be available on HRMS, along with instructions for downloading.

In view of the above, it is requested that necessary instructions may be issued to concerned officials to facilitate the timely implementation of project by 27.03.2026.

DA: As above.

SPO/Confdl
For n/a plz.
18/03/2026.

10.03.26

(Rajesh Kumar Kushwaha)
Dy. Chief Information & Security Officer
East Central Railway, Hajipur

Copy to : CISO/ECR for kind information please.

Shri Rakesh Verma
19/3/26

भारत सरकार Government of India
रेल मंत्रालय Ministry of Railways
(रेलवे बोर्ड) (Railway Board)

No. 2022/RBCC/7/7/SOC

Dt. As signed

The General Managers/Director Generals
All Indian Railways, Production Units, RDSO and CTIs

Sub: Implementation of IR SOC over Indian Railways.

The Indian Railways Security Operations Centre (IR-SOC) project is being implemented to strengthen the cyber security posture of Indian Railways. Under this project, a Central SOC and Sub SOCs are being established at Railway Board and Railway units. CRIS is the executing agency of this project.

2. In this connection, the cyber security solutions need to be installed and configured at endpoints, including network devices of each Sub-SOC. This will ensure endpoint protection (Antivirus), log collection, real-time monitoring, asset discovery, incident detection, vulnerability management and patch management etc. Details of cyber security solutions are enclosed as Annexure. Installation of software solutions will require integration with the existing Network infra, Security Devices and Servers at the respective Zone/PU/CTI etc. The schedule for installation activity at all Sub SOC locations will be conveyed to respective CISOs. Representative of the M/s Bharti Airtel are being deputed at all Sub SOC locations for installation of above software.

3. In addition, link for installation of cyber security solutions will be available on HRMS, along with instructions for downloading.

4. In view of the above, it is requested that necessary instructions may be issued to concerned officials to facilitate the timely implementation of project by 27.03.2026.

This has the approval of competent authority.

Digitally signed by
Bharat Bhushan Harit
Date: 06-03-2026
22:39:46

DA: As above.

Director. ME(C&IS)
dircis@rb.railnet.gov.in

Copy to:

1. ED/TD, Railway Board
2. PCCMs, PCSTEs – All ZRs,
3. CISOs - ZRs, PUs, CTIs, and RDSO
4. DRMs - All Divisions, IR
5. MD/CRIS, CMD/RCIL, CAO/Systems/NR

for information and necessary action please

Annexure

S.No	Name of Solution	Purpose	Support needed from Sub-SOCs
1	Log Collector	• Collects logs from multiple sources within the network. • Normalizes and filters log data before forwarding. • Enable real-time monitoring, incident detection and forensic analysis	Inventory of Devices and their credentials for SIEM integration ▪ L3 Switch ▪ Firewall ▪ Servers ▪ Other Critical network and security devices
2	End Point Security	• Distributes EDR/AV signature updates and security patches to endpoints. • Reduces bandwidth consumption by preventing each endpoint from communicating directly with the central server. • Acts as a local distribution point for endpoints within a network segment.	• Required permission for all Resources for software roll-out on all end points. • Availability of Users/Access to endpoints for Roll-out of Software
3	ITSM for Asset Discovery, Inventory and Patch Management	• Supports asset discovery and inventory management. • Helps in software deployment and patch management.	• Required permission for all Resources for software roll-out on all end points. • Availability of Users /Access to endpoints for Roll-out of Software
4	Vulnerability Management	• Automated vulnerability scanning. • Identification of outdated software and misconfigurations. • Risk-based prioritization of vulnerabilities.	• Inventory of Network and Security Devices • Inventory of Servers