EAST CENTRAL RAILWAY

Office of the
Sr. EDP Manager
Hajipur
Ph-Rly-025-22222, 22116
Email id- sredpm@ecr.railnet.gov.in

No.ECR-HQ0ACCT(ADMN)/0127/2025-O/o Sr.EDPM/ACC/HQ/ECR Date:-22-10-2025

All Dy.FA&CAOs/ECR
All Sr.DFMs/ECR
All Sr.AFAs/ECR
All AFAs/ECR
All Concerned Officer/ECR

Sub:- National Cyber Security Awareness Month- Cyber Jagrit Bharat
Ref:- **Chairman & CEO, Railway Board's** Letter no 2012/CRIS/NDLS-HQ/I&S/INFO-SECU/0000/0014/PT-2 dated 01-10-2025.

<<<<>>>>

A copy of **Chairman & CEO, Railway Board** under his letter no- 2012/CRIS/NDLS-HQ/I&S/INFO-SECU/0000/0014/PT-2 dated 01-10-2025 regarding awareness about National Cyber Security and ensuring full fledge involvement in Cyber Security awareness programs in 2025 as **"National Cyber Security Awareness Month- Cyber Jagrit Bharat"** run by CRIS for all Officers and other officials associated with cyber security is enclosed herewith for information, wide circulation and necessary action please.

D.A-As Above

Sr. EDP Manager
EDP Centre/ECR/HJP.

चन्द्रशेखर आजाद स्नेही
Chandra Shekhar Azad Snehi
वरिष्ठ ई. डी. पी. मैनेजर
Sr. EDP Manager
पूर्व मध्य रेल, हाजीपुर
E.C. Railway, Hajipur

Copy to:-

(i) **PFA/ECR/HJP** - For kind information Please.
(ii) **PFA/CONS/MHX** - For kind information Please.
(iii)**All FA&CAOs/ECR** - For kind information Please.

22/10/25

Sr. EDP Manager
EDP Centre/ECR/HJP.

चन्द्रशेखर आजाद स्नेही
Chandra Shekhar Azad Snehi
वरिष्ठ ई. डी. पी. मैनेजर
Sr. EDP Manager
पूर्व मध्य रेल, हाजीपुर
E.C. Railway, Hajipur

GOVERNMENT OF INDIA
MINISTRY OF RAILWAYS
RAILWAY BOARD

06 OCT 2025
रेलवे बोर्ड का पत्र प्राप्ति सं०.....18

All PHODs
All DRMs

No.: 2012/CRIS/NDLS-HQ/I&S/INFO-SECU/0000/0014/PT-2 Dated : 01.10.2025

To

All GMs of Indian Railways
All GMs of Production Units
All DGs of Indian Railways
CMDs of All PSUs/CTIs and Autonomous Organizations under Ministry of Railways

Sub: National Cyber Security Awareness Month - Cyber Jagrit Bharat.

The **month of October** is being observed globally every year,both globally and in India as the NationalCyber Security Awareness Month (NCSAM). This year's, campaign theme set by the National Security Council Secretariat (MSCS) of Government of India is **"Cyber Jagrit Bharat"**,with focus on making cyber infrastructure of the country more secure through awareness amongst the people.

Enhancing the cybersecurity posture of Critical Sector Entities (CSEs), their respective Critical Information Infrastructure(CII)/Protected System is pivotal for safeguarding CSEs from the Cyber threats. Towards achieving this goal, it is imperative to spread basic awareness, amongst each & every employee and ensure that they follow cyber security hygiene, promote best practices and thereby stay safe online.

To achieve this objective, extensive initiatives on Cyber Security awareness need to be undertaken by all Zonal Railways, PUs, CTI's and PSUs/Autonomous organizations.The detailed programme is attached in **Annexure-1.**

The campaign comprises spreading awareness through quizzes; essay writing; poster creation;awareness sessions; conduct of exercises - Audit, patching, simulation, etc. as well as regular cyber drills.

Further, CRIS will also conduct Cyber Security awareness programmes for all PHODs, HODs, and other officials associated with Cyber Security as per **Annexures** enclosed.

All GMs/DGs/CMDs to ensure full-fledged involvement in making the campaign successful.

DA: Annexures-I, II, III

(Satish Kumar)
Chairman & CEO, Railway Board

Annexure-I

National Cyber Security Awareness Month

Cyber Jagrit Bharat

SN	Activities	Responsible Units	Suggested Dates	Details of Activities	Mode of Delivery
1	Conduct sector specific tailored awareness campaigns.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	07.10.2025 15:00 hrs	• **Activity 1:** CRIS will conduct Cyber Security Awareness Session for PHODs, HODs and other officials involved in Cyber Security. • CRIS shall share the VC Link.	VC
			08.10.2025	• **Activity 2:** Cyber security Awareness Art or Poster Contest on Cyber hygiene and cyber security best practices at Every Units.	Physical
			09.10.2025	• **Activity 3:** Cyber Security Awareness Essay writing competitionat Every units in Hindi/English/Regional Language.	Physical
2	Awareness Workshops / Webinars by CERT-In	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	06.10.2025 10.10.2025 15.10.2025 23.10.2025 29.10.2025	Encourage Employees to Attend Following Webinars being conducted by CERT-In :- • **6.10.2025:** Cybersecurity in Everyday Life: Simple Steps to Stay Safe • **10.10.2025:** The Human Firewall: Empowering Employees to Fight Cyber threats • **15.10.2025:** Keeping devices safe and clean • **23.10.2025:** Protecting from Malware infections • **29.10.2025:** Mobile and app Security The Sessions on all the days will be held from **11.30 AM to 12.30 PM**. Participants to enroll on below website:	VC

				https://faas.isea.app/formview/ncsam	
3	Organise cyber security awareness quizzes	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	13.10.2025	• Every Units shall conduct Cyber Security Awareness Quiz in their respective Units.(*CRIS shall share the question Bank with CISOs of ZR/PUs/CTIs*) • Appropriate rewards may be provisioned to encourage employee for maximum participation.	Physical
4	Carry out phishing simulation exercise	CRIS	14.10.2025 15:00 hrs	• CRIS will conduct live demo of Phishing Simulation Exercise for IR and awareness Session on various phishing Technique. • CRIS Shall share the VC link.	VC
5	Conduct cybersecurity leadership round tables to increase awareness of latest cyber security threats.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	15.10.2025	• CISOs of Every Units shall hold an Awareness Session on recent Cyber Security threats for their respective Leadership.	Physical
6	Run innovative social media campaigns regarding cyber hygiene and cyber security best practices to promote adoption by all stakeholders.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• CISOs of Every units shall run social media Campaign regarding Cyber Hygiene and Cyber Security Practices.	Online
7	Support campaigns of other Ministries/Departments on social media, where appropriate	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• Follow CERT-In, NCIIPC etc on social media and support Cyber Security Awareness Campaign on social media.	Online
8	Organise vulnerability patching competitions.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• **Activity 1:** All units shall encourage employees to update their End Points and associated Application and System Software.	Physical, Online

				• **Activity 2:** CRIS, RCIL and IRCTC shall run special campaign to encourage asset owner/Custodian to apply Security patches on Critical Servers. Employees/Units applying maximum Security patches should be appreciated for their efforts.	
9	Conduct cyber security drills to test response capabilities against latest and most prevalent threats.	CRIS, RCIL, IRCTC	16.10.2025	• All identified Units shall conduct a Cyber Security Drill to test response capabilities. • Cyber Security Drill report shall be prepared and learning from drill shall be shared across the Organisation.	Physical
10	Conduct drive to update inventory of all IT assets.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• **Activity 1:** All Zone, PUs, Divisions, CTIs including CRIS, IRCTC and RCIL shall update their asset Inventory for both i.e. Hardware and Software. • **Activity 2:** All Units shall identify End of Life and End of Support Software being used in their Units. • **Activity 3:** All Units shall define a strategy to replace/upgrade EoL or EoS Solutions.	Physical
11	Cyber Security best practice/slogan each day during login.	CRIS,IRCTC	Oct-2025	• CRIS shall create and display at least One Slogan/Cyber Security Practices on login Page of HRMS application and IR portal. • IRCTC shall also create and display Slogan/Cyber Security Practices on their website.	Online
12	Conduct drive to complete Cyber Security Audit of all unaudited	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• All Units shall identify unaudited Applications (Website/Web Portals /	Physical

	Applications (Websites/ Web Portals/ Mobile Apps etc.)/ Systems.			Mobile Application etc) in their respective Units. • All units shall plan audit of identified applications by CERT-In Empanelled Organization.	
13(a)	Rewarding people following best cyber security practices.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	31.10.2025	• Identify Top 3 Employees in every Zone/PUs/CTIs by their performance during various events being conducted in this Cyber Security Months.	Physical/VC
13(c)	Mandatory answering of one question related to cyber hygiene every week and a short quiz every quarter before 'Login' to check awareness of recent alerts/ advisories/ guidelines related to cyber security	CRIS	Oct-2025	• CRIS shall pop-up Cyber Security related questions during Login on HRMS etc. • CRIS shall share the Top 10 performer from every Zone/PUs/CTIs.	Online
13(d)	Activate multi-factor authentication wherever feasible.	CRIS, RCIL, IRCTC	Oct-2025	• All units shall identify applications without Multi Factor Authentication. • Implement Multi Factor Authentication on Identified Applications.	
13(e)	Cyber hygiene should be a priority for the top management, who should lead by example to further a culture of cyber hygiene.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• CISOs of Every Zone, PUs, CTIs etc shall have review meeting on Cyber Security Practices being followed in their Units and further improvement.	Physical/VC
13(f)	Clear segregation of personal and professional devices and implementation of proper SOPs for the same.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• Employees to be encouraged segregation of personal and professional devices.	Physical/ Online

13(g)	Incentivise cyber security incident reporting.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• All units should encourage employee to report every Cyber Security Incident. • Single Point of Contact should be identified and details of same should be advertised. • Concerned Officials should be rewarded for reporting Cyber Security Incidents.	Physical/ Online
13(h)	Introduce inter-department/vertical competitions within the organization and reward (for example - 'Best Cyber Hygiene Trophy') the department/ vertical having maximum cyber hygiene score.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• Reward the Units with Best Cyber Hygiene Trophy /Awards. • Suggested Criteria :- o Having Minimum No or No EoS or EoL System o Max No of Systems having latest update. o Any Other Criteria defined/Identified by respective Units.	Physical/VC
13(i)	Regular audit and assessment of cyber hygiene practices.	ZR, PUs, CTIs, CRIS, RCIL, IRCTC	Oct-2025	• Every Unit shall define and Implement Policy for having periodical VA-PT by CERT-In Empanelled Organization.	

- At the end of this month, Every Unit shall share summary report on improvements they have made and activities performed to improve Cyber Security awareness in their units.
- The Objective of above activity is to create a Cyber Security Aware culture and ensure that everyone should play their role in strengthening Cyber Security for Indian Railways.

V2-0 October 2025

Annexure-II

INDIAN RAILWAY SECURITY OPERATION CENTRE

(IRSOC)

Abbreviations

SN	Term	Expansion
1	IRSOC	Indian Railway Security Operation Centre
2	NCIIPC	National Critical Information Infrastructure Protection Centre
3	SOC	Security Operation Centre
4	MSSP	Managed Security Service Provider
5	KPI	Key Performance Indicator
6	SIEM	Security Information Event Management
7	EDR	End Point Detection and Response
8	NDR	Network Detection and Response
9	UEBA	User Entity Behavior Analytics
10	SOAR	Security Orchestration Automation & Response

1. **Background: -**

The Indian Railways (IR) is increasingly reliant on digital information and communication technologies (ICT) for operations, maintenance, production, and procurement of assets. As cybersecurity is a continuous process rather than a one-time solution, incidents are inevitable. Therefore, an effective Incident Response mechanism is crucial to minimize the impact of cyber incidents on railway operations, revenue, and management. The effectiveness of incident response is directly linked to timely detection, making monitoring user activities on organizational assets and networks a critical function.

The **Indian Railways Security Operation Centre (IRSOC)** has been conceptualized to address these challenges. IRSOC will collect logs and alerts from critical systems, servers, network devices, and other infrastructure components to detect malicious activities and enable appropriate responses.

Abstract Estimate of IRSOC amounting Rs 175Cr, was sanctioned in April-2022 for 3 Years. Detail Estimate amounting Rs 609Cr sanctioned in Oct-2024 for 8 Years.

2. **Objective: -**The IRSOC aims to

- Establish a centralized Security Operations Centre (SOC) for continuous monitoring of IT assets.
- Detect and respond to cybersecurity threats efficiently.
- Ensure compliance with government security guidelines (CERT-In, NCIIPC etc.).
- Improve incident response times and minimize downtime.
- Facilitate threat intelligence sharing among railway units.

3. **Stages of IRSOC Project and its associated Outcomes**

S.N	Project Stage	Work Type	Outcomes
1	Planning & Design	• Scope of Project • Threat Assessment • Business Impact Analysis • Identification of Use Case for SOC. • Selecting the Right SOC Model. • KPI for IRSOC.	• Identification of Assets to be integrated with SOC. • Identification of SOC Components. • Selection of Right SOC Model (DIY vs MSSP (On-premise) vs MSSP (Off Premise)
2	Implement	• Installation and Commissioning • Implementation and Validation of Use Cases • Training of Human Resources. • Creation of	• Integration of All identified Assets with IRSOC. • Upskilling/Training of Human Resource.

		Workflow/Automation.	
3	Operationalize	• Setting Up a baselines • Monitoring of Alerts • Incident Management • Coordination with NCIIPC and Cert-In.	• Central Log Analysis and early detection of Threats. • Faster compliance/Implementation of Cert-In/NCIIPC alerts/advisories across Zones/Units in IR. • Creation of Knowledge Management with respect to Incident Handling and Learning from them.
4	Continuous Improvement / Maintenance	• Monitoring of IRSOC Performance with respect to Identified KPIs. • Learnings from Security Incident and Implementation of Preventive /Corrective Security Controls.	• Improved MTTD and MTTR. • Less No of Incidents. • Increased Employee Awareness.

4. **Scope of IRSOC: -**
   - Integration of 1,20,000+ endpoints (Servers, Network Devices, Workstations etc.).
   - Deployment of **26 Sub-SOCs** across railway zones, production units, and research/training institutes.
   - Establishment of a **Central SOC** at the Railway Board.
   - Secure log collection and real-time monitoring from all Indian Railway units.
   - Collaboration with national cybersecurity agencies for intelligence sharing and compliance.
5. **Proposed Security Solutions in IRSOC**

   Proposed IRSOC shall have some major functionality which are listed below along with supported technology for respective functions:-

   A. Collection

   Functionality:

   The process of gathering security-relevant data from various sources, including network traffic, endpoints, logs, and cloud environments.

   Technologies:

   - **SIEM (Security Information and Event Management):** Aggregates and analyzes log data from multiple sources to identify potential security threats.

- **NDR (Network Detection and Response):** Monitors network traffic for suspicious activity and provides real-time threat detection.
- **EDR (Endpoint Detection and Response):** Focuses on monitoring and protecting endpoints (computers, servers, and mobile devices) from security threats.
- **UEBA (User and Entity Behaviour Analytics):** Uses machine learning to analyze user behaviour and detect anomalies that may indicate malicious activity.

B. Detection

Functionality:
Identifying potential security threats by analyzing collected data for anomalies, known attack patterns, or suspicious behaviour.

Technologies:
- **SIEM:** Correlates events from different sources and generates alerts for potential threats.
- **NDR:** Detects network-based threats and lateral movement of attackers.
- **EDR:** Identifies and responds to threats affecting endpoints.
- **UEBA:** Detects insider threats and compromised accounts by monitoring unusual user behaviour.
- **Threat Hunting:** Proactively searches for threats using advanced analytics and hypotheses rather than waiting for alerts.

C. *Triage*

Functionality:
Prioritizing security alerts based on severity, impact, and likelihood to minimize alert fatigue and ensure timely responses.

Technologies:
- **SOAR (Security Orchestration, Automation, and Response):** Automates response workflows to prioritize and handle incidents efficiently.
- **Threat Intelligence Platform:** Integrates with multiple sources to provide real-time threat intelligence, aiding in decision-making.

D. Investigation

Functionality:
Analyzing security incidents to determine their root cause, attack vector, impact, and possible mitigation strategies.

Technologies:
- **SOAR (Knowledge Management, Incident Management):** Provides a structured platform to document, investigate, and manage security incidents.
- **SIEM:** Helps in deep-dive analysis of logs and events to trace the attack path.
- **Threat Intelligence Platform:** Provides context on threat actors, Indicators of Compromise (IoCs), and malware behaviour.

E. Incident Response

Functionality:

Taking immediate actions to mitigate or contain security incidents and prevent further damage.

Technologies:

- **SOAR:** Automates incident response playbooks, integrates with security tools, and facilitates faster threat containment.

F. Auxiliary Functions

Functionality:

Supporting functions that enhance overall security posture and ensure continuous protection.

Technologies:

- **Vulnerability Management:** Identifies, assesses, and mitigates security vulnerabilities in the IT infrastructure.
- **Patch Management:** Ensures timely application of security patches to reduce exploitable weaknesses.
- **Forensics (On-Demand Service, Man-Days):** Conducts post-incident investigations to gather evidence and determine the full impact of attacks.

6. Major Security Solutions for IRSOC:



7. Salient Features of IRSOC:

- Proposed Security Solutions for IRSOC shall be implemented and configured at CRIS Private Cloud Chanakyapuri New Delhi and DR-DC Secunderabad.
- Propose Solution should provide and implement Disaster Recovery and Business Continuity Plan for IRSOC.Primarily IRSOC Services shall be made live from Primary DC(CRIS Chanakyapuri),In case of any exigencies Services should be made live from DR-DC Secunderabad.
- IR SOC shall be divided into 26 Sub-Security Operation Centre. These Sub-SOC shall be implemented at HQ of Each Zonal Railways, CRIS, Railway Board and Production Units.
- Each Sub-SOC shall have access to dashboard of VM, SIEM, Patch Management, Asset Discovery etc for assets of their respective Zones/Units. So that Sub-SOC can also monitor alerts and can take appropriate action in coordination with Central SOC.
- Proposed Solution shall ensure that there should not be more than 15 mins of delay in data transmission from Zone/PUs to CRIS Cloud Primary Site and DR-DC Site.
- Log Collector shall be placed on Sub-SOCs to collect logs from all Network devices & Servers under purview of respective Zones/Units.
- Log Collector should be able to collect logs from multiple divisions & CTIs in a Zone and forward it to Central Log Server at Central SOC for analysis and further action.
- In case of any issue in Network connectivity, Log Collector should have sufficient capacity to preserve logs for at least 2 Days and should be able to forward all logs to Central SOC as soon as connectivity issue gets resolved.
- Central SOC shall be implemented at Railway Board New Delhi and all correlation and analysis of logs shall occur from CRIS Private Cloud.
- The Proposed Solution shall enable both Central SOC and Sub-SOC to take remediation/response of any Security Incident/Threat as identified/reported by IRSOC Team.
- Each Sub-SOC Team should be able to analyse and review logs/alerts for their respective Units/Zones.
- Central SOC will have complete View of all alerts/activity/logs from all Zones/Production Units.
- Proposed Solution should enable IR to share and receive threat Intel feed from Cert-In /NCIIPC and other Law Enforcement Agency as and when mandated by GOI.
- Proposed Solution shall ensure secure transmission of logs/alerts/incidents etc from Zonal Railways and all Production Units of IR to CRIS Data Centre both Primary and DR-DC.

~~~~~ END ~~~~~
~~~~~

Annexure-III

References for Cyber Security Slogans and Posters

- **Cyber Security Slogans in English**
  - Protect what you connect."
  - "Security is everyone's business."
  - "Your data, your responsibility."
  - "Stay safe in cyberspace."
  - "Think security, act securely."
  - "Click with caution, surf without suspicion."
  - "Strong passwords, strong defenses."
  - "Patch your systems, or face the victims."
  - "An ounce of prevention is worth a pound of cyber cure."
  - "Cultivate a culture of cyber safety."
  - "Security starts with awareness."
  - "Don't wait for the breach to teach."
  - "Navigate safely, the cyber world is shady."
  - "Guard your data, secure your future."
  - "Embed security in Railway's DNA."
- **Cyber Security Slogans in Hindi**
  - "साइबर सुरक्षा – रेल की प्रगति का पहिया।"
  - "सुरक्षित रेल, सुरक्षित डेटा, सुरक्षित भारत।"
  - "साइबर खतरे से सतर्क रहें, रेल को सुरक्षित रखें।"
  - "एक क्लिक की लापरवाही, बढ़ा सकती है आपकी परेशानी।"
  - "साइबर सुरक्षा – रेलवे की जीवनरेखा।"
  - "पासवर्ड आपका कवच है, इसे मजबूत बनाएँ।"
  - "असली मेल पहचानें, फिशिंग जाल से बचें।"
  - "साइबर अनुशासन – हर रेलवे कर्मचारी की पहचान।"
  - "सोच-समझकर क्लिक करें, सुरक्षित रहें ।"
  - "लॉगिन करें सावधानी से, डेटा बचे जिम्मेदारी से।"
  - "डिजिटल रेल, सुरक्षित रेल।"
- References for Cyber Security Poster
  - https://www.cert-in.org.in/s2cMainServlet?pageid=Pre_Sec_Tips3
  - https://infosecawareness.in/nic-tip