MOST IMPORTANT

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

File NO.2019/RBCC/7/7/Policy Implementation dated, 10/11/2020

The General Manager
The Directors General

Pr CAOs/CAOs

All Indian Railways, Production Units, CTIs

DMW, COFMOW, RWP, WPO

Managing Director
CRIS, New Delhi

Sub : National Cyber Security Strategy 2020
Ref : Hon'ble PM's directive.

Information & Communication Technology (ICT) has become the mainstay of normal working in most of the Organisations, including the GOI. The working of IR has also been increasingly shifting to ICT platform, more so in the Covid pandemic scenario. ICT, while providing a number of conveniences, efficiency & transparency, is also not bereft of its share of vulnerabilities & attacks by threat actors. Therefore, it is necessary to secure the ICT infrastructure in order to safeguard critical information. Keeping this in view, Board have already approved the IR ICT Security Policy 2019 which has been circulated to all Railway Units.

2. It has been observed that, in recent times, an alarming increase has been seen in the number of breaches/attempted breaches to ICT infrastructure of Govt Organisations. The Government of India, at the highest level, is also seized of the need for adequately and appropriately securing the ICT infrastructure. In keeping with this need, the Government has been working on the subject strategy.

3. Now, Hon'ble Prime Minister has given the following directions for action by all Ministries:

> ***"Every Ministry has some personnel with technical aptitudes. These are to be identified and trained in Cyber Security Courses within six months. These should then form the cyber security nucleus of that Ministry."***

4. A meeting was convened by Secretary (Security) in the Cabinet Secretariat recently to firm up the road-map for implementation of the directive. The MoM is attached for ready reference.

5 It has, therefore, been decided that certain strength of officials from each Railway Unit as per Annexure–II with aptitude in ICT hardware, software, networking and compliances may be identified for forming the group for that Unit, to begin with. This group would work under the overall supervision of the nominated CISO of the Railway Unit. The duties, as part of this security group, would be in addition to their regularly assigned responsibilities. Appropriate training, as and when formulated by MEITY, Govt. of India, would also be imparted to this core group.

5. Further, advanced training modules are also planned as indicated in para 11(ii) of the attached MoM.

6. Keeping in view the criticality, it is requested that urgent action to identify the personnel/officials may be undertaken and the details (as per Annexure-III) shared on the following email ie – ir-infosec@gov.in by 13.11.2020.

This issues with the approval of Board [M(O&BD)].

(Rajnesh Singh)
Director ME(C&IS)

Copy to: (i) ED/TD & EDF(X)-II – kindly provide nomination.
(ii) All CISOs of Railway Units- for information & necessary action please.

Receipt No : 761263/2020/ED(C&IS)

ANNEXURE-I

No.A-16/06/2020-SS
Cabinet Secretariat
Office of Secretary (Security)
226-A, North Block

Subject: National Cyber Security Strategy 2020 – matters regarding training of officers.

Secretary(Security) chaired a meeting on 20/10/2020 on the subject mentioned above. The meeting was held through video conference. The list of participants is attached.

2. Welcoming the participants Secretary(Security) gave a background for the meeting. It was re-called that during the presentation on National Cyber Security Strategy 2020 on 01/09/2020, HPM had directed that :-

"Every Ministry has some personnel with technical aptitudes. These are to be identified and trained in Cyber Security courses within six months. These should then form the cyber security nucleus for that Ministry".

3. Specific modalities are now required to be developed to implement the above directions. He thereafter invited comments of DG NIC & DG CERT-IN in the matter.

4. DG NIC noted that majority of Govt. officers now work in an IT enabled environment. Therefore every officer should have the knowledge of basic cyber security. Secretary(Security) suggested that MEITY should devise a general awareness training module of about 6 to 8 hrs duration with both theoretical and demonstration components. The module should be made available online. DG CERT-IN informed that Meity has a existing scheme for imparting training on cyber security. New Training modules are being designed by the Ministry in consultation with NIC, C-DAC & Cert-In. The content for this will be developed by C-DAC.

5. Secretary(Security) noted that every Ministry/Department has a NIC team associated with it. These NIC officers are technically qualified as well as highly experienced in dealing with cyber security matters. However in the present case, target audience for the proposed training will be from the Ministry/Departmental Officers who have basic/advanced degrees in science/technology or with an aptitude for technology. These officers are to be identified by respective Ministries/Departments and Meity may design a training programme on cyber security for them. The programme can consist of different modules and should be available partly online. The training module should focus on practical aspects of cyber security with hands on demonstration and practice to enable officers to troubleshoot. The module should clearly define training objectives and specifically achieve the objectives and skills sets required.

6. A certificate on completion of the training can also be given to the trainees.

Contd.....P/2

Receipt No : 761263/2020/ED(C&IS)

21

7. After successful completion of the training, these officers will form the nucleus of the cyber-security team of the Ministry/Department and will function under the overall leadership of the CISO of the Ministry/Department.

8. JS(DFS) suggested that roles and responsibilities of CISO need to be clearly defined for managing ICT operations. DG Cert-In noted that a detailed advisory dated 14/3/2017 has been issued by Meity in this regard which is also available at the website of the Ministry.

9. JS (M/O Power) enquired whether employees of subordinate officers and PSUs can be included in the proposed training. Secretary(Security) noted that requirements of subordinate offices/PSUs are different and the proposed training is primarily meant for officers of GOI and its attached offices. Another phase of training can be coordinated for subordinate offices'/PSUs'.

10. JS(NSCS) noted that the roles and responsibilities of the officers after successful completion of training should be clearly defined.

11. After detailed deliberations the following were recommended :-

(i) A Generic online training course of about 6-8 hrs duration with both theoretical and practical components should be developed by Meity for all officers, for basic cyber security.

(ii) For advanced training on cyber security, Meity may write to all Ministry/Departments for identifying officers who are technically qualified or with requisite aptitude in cyber security/IT. For this purpose, Meity may circulate appropriate communication. All Ministries/Departments should identify these officers within one week of receipt of the format. This exercise may be completed by 15.11.2020.

(iii) Meity to form a group of best trainers to design the module and content, the group may consist of trainers from NIC, Cert-In and CDAC and the content be based on competency approach. The training programme should commence from December 2020.

(iv) The successfully trained officer will then form the nucleus of a team to deal with cyber security matters (in addition to their assigned duties) and will work under the overall supervision of CISOs while dealing with cyber security issues.

(v) Secretary(Security) requested all concerned to strictly ensure that the timelines are adhered to. He also requested Meity to draw a timeline for completion of the training to all Ministries/Departments and to periodically apprise further progress in the matter.

The meeting ended with Vote of Thanks.

Annexure-II

Allotted Nomination Strength Railway Unit-wise

Sr No	Railway Unit	CISO	No of officials per Rly Unit for Generic Training	No of officials per Rly Unit for Adv. Training	Remark
1	Zonal Railways	1	8	4	**NR & WR have not nominated their CISOs.**
2	PUs & CTIs	1	4	2	
3	CRIS	1	20	10	
4	Rly Board	1	20	10	

Annexure-III

(A) Details sought for Generic Training

(Kindly provide data in Excel Sheet)

Name of Railway Unit: .....(Zonal Railway/PU/CTI etc).

CISO Shri _____

Sl No.	Name of Officer	Designation	Mobile No.	Email Id **	HQ/ Division	Brief area of working	Educational Qualification
				@@			

**** Email ID**: Kindly provide @gov.in / nic.in email ID, if available, as per instructions issued vide Office Order No. 42 of 2020.

(B) Details sought for Advanced Training

(Kindly provide data in Excel Sheet)

Name of Railway Unit: ..... (Zonal Railway/PU/CTI etc).

CISO Shri _____

Sl No.	Name of Officer	Designation	Mobile No.	Email Id **	HQ/ Division	Brief area of working	Educational Qualification
				@@			

**** Email ID**: Kindly provide @gov.in / nic.in email ID, if available, as per instructions issued vide Office Order No. 42 of 2020.