Dated 19.02.2025

OFFICE MEMORANDUM

Subject: Formation of a Cyber Security Team under CISO to Oversee Cyber Security Activities for the Ministry of New and Renewable Energy (MNRE)

As per directive from the Secretary, Ministry of Electronics and Information Technology (MeitY), vide letter **No. AA-14/28/2021-CSD dated 10th December 2024** regarding the formation of a dedicated Cyber Security team under the leadership of the Chief Information Security Officer (CISO) for the Ministry of New and Renewable Energy (MNRE), a Cyber Security Team in MNRE is constituted as follows:

Cyber Security Team of MNRE

Sl No	Designation	Current Officials	Email	Contact Number
1.	Chief Information Security Officer (CISO)	Dr. Arun K. Tripathi	aktripathi@nic.in	9810880378
2.	Deputy CISO	Mr. Mohd Shahid Hasnain	dciso-cstmonre@nic.in	9868220511
3.	Head of Department, NIC posted at MNRE	Mr. Adarsh Saiwal	adarsh.saiwal@nic.in	9810269560
4.	Director/Deputy Secretary of Admin Division of MNRE	Mr. Pankaj Gupta	pankaj.gupta66@nic.in	9868450773
5.	Director/Deputy Secretary or Scientist D of IT Division of MNRE	Ms. Priya	priya.mnre@nic.in,	8375975366

2.0   The objective is to streamline Cyber Security activities across MNRE and ensure that all associated digital and technology infrastructure remains secure, compliant, and resilient to emerging threats. In line with the growing importance of Cyber Security in the context of the Ministry's operations, including the increasing reliance on digital platforms, the rapid adoption of renewable energy technologies, and the shift towards digitization, it is imperative to establish a robust Cyber Security framework to safeguard critical data and resources.

3.0   **The specialized Cyber Security team will play a pivotal role in:**
   i.   Ensuring Compliance with national and international Cyber Security regulations and policies.
   ii. Defining Cyber Security Strategy for the Ministry to mitigate risks associated with cyber threats and attacks.
   iii. Implementing Cyber Security Frameworks that ensure the integrity, confidentiality, and availability of digital assets.
   iv. Monitoring and Responding to Cyber Incidents and potential threats that may compromise the functioning of MNRE.
   v.   Training and Awareness within the Ministry to cultivate a culture of Cyber Security.

4.0   **Scope of Work:**
   The Cyber Security team will have the following key responsibilities:

   i.   Risk Assessment: Conduct regular risk assessments of MNRE's IT infrastructure and technology deployments to ensure that potential threats are identified and mitigated.

ii. Implementation of Security Tools: Deploy state-of-the-art Cyber Security tools, including firewalls, endpoint protection, and threat intelligence platforms, to safeguard Ministry systems and networks.

iii. Incident Management: Establish protocols for reporting and managing Cyber Security incidents, minimizing the impact of any security breach, and restoring systems swiftly.

iv. Policy Development: Develop Cyber Security policies and frameworks tailored to MNRE's operations, ensuring the adoption of best practices across all digital initiatives.

v. Continuous Monitoring and Reporting: Implement a 24/7 monitoring system and provide regular reports to the senior leadership on the health of MNRE's Cyber Security posture.

5.0   The Cyber Security team under the CISO with roles and responsibilities of each team member will include but are not limited to the following:

Chief Information Security Officer (CISO): (Chairman) The team will be led by the CISO, who will be responsible for setting the overall Cyber Security strategy, ensuring compliance with MeitY directives, and reporting to the senior leadership of MNRE.

Deputy CISO: Deputy CISO with a dedicated team of Cyber Security analysts will be responsible for real-time monitoring of the Ministry's IT infrastructure and systems, identifying potential vulnerabilities, and responding to incidents promptly.
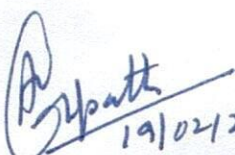
Head of Department, NIC posted at MNRE: HoD, NIC with the team will focus on securing the networks and communication systems within the Ministry, ensuring encryption, firewall management, intrusion detection, and prevention systems are in place. This team will also be responsible to handle security breaches, conduct forensics on cyber incidents, and assist in the investigation and remediation process.

Director/Deputy Secretary of Admin Division of MNRE: The Concerned officer will provide adequate resources to cyber cell of MNRE e.g office space, stationary materials, IT tools etc.

Director/Deputy Secretary or Scientist D of IT Division of MNRE (Secretary of the Cyber Cell): The Concerned officer will focus on ensuring adherence to national Cyber Security policies, MeitY guidelines, and international best practices, while assessing risks and managing potential impacts on the Ministry's operations. The officer will also be responsible for organising the meeting of the Cyber Security Team regularly.

6.0   The NIC cell of MNRE will also provide technical support to the Cyber Security Team. The Cyber Security Team of MNRE will work in close collaboration with MeitY's Cyber Security Division to ensure alignment with National Cyber Security standards and guidelines and for staying updated on evolving cyber threats and regulatory changes.

This issues with the approval of Secretary, MNRE

19/02/20:

Dr. Arun K. Tripathi
Adviser/Scientist 'G'

1. All Cyber Security team members
2. PPS to Secretary, MNRE
3. PPS to Secretary, MeitY
4. PPS to AS, MNRE
5. PS to AS & FA, MNRE
6. JS(Admin.)/Scientist G (SK)/Advisor (PS)
7. Director NIC (PB)/Scientist E NIC (AS) with request to upload on the Ministry's website.
8. Sanction folder