GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 239
TO BE ANSWERED ON: 21.07.2023

COWIN DATA BREACH

239. SHRI SYED NASIR HUSSAIN:
DR. AMEE YAJNIK:
SHRI VIVEK K. TANKHA:

Will the Minister of ELECTRONICS AND INFORMATION TECHNOLOGY be pleased to state:

(a) whether Government has a tangible plan to contain the leaked information from the CoWIN portal;
(b) whether the Indian Computer Emergency Response Team (CERT-In) has started investigation and identified those responsible for the breach;
(c) if so, the status of investigation thereof and if not, the reasons therefor; and
(d) the measures Government has taken to enhance safety protocols regarding such large databases, with the key focus of protecting private information of citizens and preventing unauthorized access to their database?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI RAJEEV CHANDRASEKHAR)

(a): As per the information provided by Ministry of Health & Family Welfare, Co-WIN portal of Ministry of Health & Family Welfare has complete security measures and adequate safeguards for data privacy with Web Application Firewall (WAF), Anti- Distributed Denial-of-Service (DDoS), Secure Sockets Layer(SSL)/Transport Layer Security(TLS), Identity & Access Management and regular vulnerability assessment.

(b) and (c): Taking cognizance of the cyber incident regarding CoWIN data in June 2023, CERT-In coordinated incident response measures with Ministry of Health & Family Welfare (MoHFW). The MoHFW has lodged a complaint and F.I.R has been registered by a law enforcement agency and CERT-In has provided inputs to facilitate investigation.

(d): Government has taken following measures to enhance the cyber security posture and prevent data breaches:

(i) On observing the reported data breaches, CERT-In notifies the affected organisations along with remedial actions to be taken. CERT-In coordinates incident response measures with affected organisations, service providers, respective sector regulators as well as Law Enforcement Agencies.
(ii) CERT-In issues alerts and advisories regarding latest cyber threats/vulnerabilities and countermeasures to protect computers, networks and data on an ongoing basis.
(iii) A special advisory on security practices to enhance resilience of health sector entities has been communicated by CERT-In to the Ministry of Health and Family Welfare, for sensitising health sector entities regarding latest cyber security threats in December 2022. The Ministry has been requested to disseminate the advisory among all authorised medical care entities / service providers in the country.
(iv) CERT-In is operates an automated cyber threat exchange platform for proactively collecting, analysing and sharing tailored alerts with organisations across sectors for proactive threat mitigation actions by them.
(v) CERT-In has issued guidelines on information security practices for government entities in June 2023 covering domains such as data security, network security,

identity and access management, application security, third-party outsourcing, hardening procedures, security monitoring, incident management and security auditing.

(vi) CERT-In has empanelled 150 security auditing organisations to support and audit implementation of Information Security Best Practices.

(vii) Government has formulated a Cyber Crisis Management Plan for countering cyber attacks and cyber terrorism for implementation by all Ministries/ Departments of Central Government, State Governments and their organizations and critical sectors.

(viii) Cyber security mock drills are conducted regularly to enable assessment of cyber security posture and preparedness of organisations in Government and critical sectors. 80 such drills have so far been conducted by CERT-In where 1062 organizations from different States and sectors participated.

(ix) CERT-In operates the Cyber Swachhta Kendra (Botnet Cleaning and Malware Analysis Centre) to detect malicious programs and free tools to remove the same and to provide cyber security tips and best practices for citizens and organisations

(x) CERT-In conducts regular training programmes for network / system administrators and Chief Information Security Officers (CISOs) of Government and critical sector organisations regarding securing the IT infrastructure and mitigating cyber attacks. A total of 42 training programmes have been conducted, covering 11,486 participants, during the years 2021 and 2022. In 2023, up to June, a total of 627 officials from Government, critical sectors, public and private sectors were trained in 6 training programs in the area of cyber security.

(xi) Security tips have been published for users to secure their desktops and mobile phones and to prevent phishing attacks.

(xii) CERT-In regularly disseminates information and shares security tips on cyber safety and security through its official social media handles and websites. CERT-In organised various events and activities for citizens during Safer Internet Day on 7 February 2023 and Cyber Security Awareness Month in October 2022, by posting security tips using posters and videos on social media platforms and websites. CERT-In, in association with Centre for Development of Advanced Computing, conducted an online awareness campaign for citizens, covering topics such as general online safety, social media risks and safety, mobile related frauds and safety, secure digital payment practices, etc., through videos and quizzes on the MyGov platform.

(xiii) CERT-In has set up the National Cyber Coordination Centre (NCCC) to generate necessary situational awareness of existing and potential cyber security threats.

(xiv) CERT-In co-operates, works and coordinates incident response measures with international CERTs, overseas organisations and service providers as well as law enforcement agencies.

(xv) The National Critical Information Infrastructure Protection Centre has been setup for the protection of critical information infrastructure and responding to cyber incidents pertaining to such infrastructure. The Centre provides near-real-time threat intelligence and situational awareness, based on which regular alerts and tailored advisories are sent to the entities concerned with such infrastructure.

(xvi) The Ministry of Electronics and Information Technology conducts programmes to generate information security awareness. Books, videos and online materials about information security are developed for general users, children and parents, and are disseminated through portals such as www.infosecawareness.in and www.csk.gov.in.

****