GOVERNMENT OF INDIA
MINISTRY OF ELECTRONICS AND INFORMATION TECHNOLOGY
RAJYA SABHA
UNSTARRED QUESTION NO. 705
TO BE ANSWERED ON: 05.12.2025

OUTSOURCING OF GOVERNMENT EMAIL SERVICES TO A PRIVATE VENDOR

705. DR. JOHN BRITTAS:

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

(a) rationale behind outsourcing the management and hosting of Government's official Email services, including the email accounts of Members of Parliament, to a private vendor despite the existing in-house email infrastructure of National Informatics Centre (NIC);
(b) details of the safeguards in the contract to ensure data privacy including data localisation and security audits by Government agencies, etc;
(c) whether the operation of Government email system infrastructure by the private vendor comes under the ambit of Audit by C&AG; and
(d) whether the concerned private vendor will come under the purview of RTI Act in so far as its operation of Government email infrastructure is concerned?

ANSWER

MINISTER OF STATE FOR ELECTRONICS AND INFORMATION TECHNOLOGY
(SHRI JITIN PRASADA)

(a) to (d): Government of India recognizes email as an important mode of official communication. Government is upgrading the legacy e-mail system to a cloud based, secure and scalable system. This upgrade is being carried out through M/s Zoho Corporation Ltd., a reputed Indian software service provider, selected through an open competitive process.

This model ensures timely upgrades, quick scaling up, seamless migration of existing accounts, and the integration of modern office productivity tools–such as word processors, spreadsheets, and presentation software with email service.

The security architecture of the e-mail platform has been defined rigorously to protect critical government data. The solution mandates that all email data be encrypted both at rest and in transit, with specific requirements for end-to-end encryption using RSA 256 and TLS 1.3 standards.

The service provider is required to comply with rigorous control standards and certifications, including ISO 27001, ISO/IEC 27017, and ISO 27018. Key technical security requirements include the implementation of Multi-Factor Authentication (MFA) for user identities across all protocols (Web, IMAP, SMTP, POP, and Calendar), the application of Geo-fencing and IP-based restrictions, and the use of industry standards and policies to combat email spoofing.

The service is integrated with the NIC-CERT Security Information and Event Management (SIEM) system. Furthermore, the system requires Multi-Factor Authentication (MFA), mobile device management (MDM), and advanced threat protection mechanisms to prevent phishing, malware, and data loss (DLP).
The contract with the service provider ensures strict adherence to data sovereignty. The service provider has ensured that the cloud-based solution, including Primary and Disaster Recovery data centers, are physically located within India, and no data can be shared or replicated outside the country.

M/s Zoho is a registered Indian entity subject to Indian laws and jurisdiction. The contract emphasizes "Make in India" products, ensuring that the government's digital communication infrastructure is sovereign, with the government retaining full ownership of all data and intellectual property created during the contract.

The service is designed for high reliability, mandating a service availability uptime of at least 99.9% on a 24x7x365 basis.

To ensure high reliability, the service provider is required to maintain Disaster Recovery sites in different seismic zones at least 500 kilometres apart, with strict Recovery Time Objectives (RTO) and Recovery Point Objectives (RPO) to minimize data loss during contingencies.
The work awarded to M/s Zoho is a regular Government contract and is covered under the ambit of Comptroller and Auditor General of India. Government e-mail systems are the responsibility of National Informatics Centre (NIC), which comes under the purview of Right to Information as per extant provisions.

*****