GOVERNMENT OF PAKISTAN
NCERT
******

No.1-1/2026/DG (NCERT)/ 89

Islamabad, the 29th January , 2026

From

Dr Haider Abbas
DG -(nCERT)

To

1- Secretary, MONFSR, Islamabad
2- Parliamentary Secretary, MOC, Islamabad
3- Chief Information Officer, NADRA, Islamabad
4- Company Secretary, PRAL, Islamabad
5- Acting Chairman HEC, HEC, Islamabad
6- Cabinet Secretary, CAB, Islamabad
7- Chairman (SECP), SECP, Islamabad
8- Chairman NEPRA, NEPRA, Islamabad
9- Chairman OGRA, OGRA, Islamabad
10- Cheif Secretary AJK, Govt of Azad Jammu and Kashmir,
11- Chief Secretary (GB), CSGB, Barmas Gilgit
12- Chief Secretary Balochistan, Govt of Balochistan,
13- Chief Secretary GB, Govt of Gilgit Baltistan,
14- Chief Secretary KPK, Govt of Khyber Pakhtun Khawa,
15- Chief Secretary Punjab, Govt of Punjab,
16- Chief Secretary Sindh, Govt of Sindh,
17- Director General, PCAA, Karachi
18- Federal Secretary (MoCommunication), MOCM, Islamabad
19- Federal Secretary of MoNHS, MONHS, Islamabad
20- Foreign Secretary, MOFA, Islamabad
21- Secretary, MOEPWD, Islamabad
22- Secretary, TEOR, Islamabad

23- Secretary, MOWR, Islamabad
24- Secretary, REVDIV, Islamabad
25- Secretary, Information Technology Department Gilgit Baltistan Government of Gilgit Baltistan,
26- Secretary, NHCD, Islamabad
27- Secretary, Science and Technology Balochistan,
28- Secretary, NSD, Islamabad
29- Secretary, MOPNR, Islamabad
30- Secretary, MOHR, Islamabad
31- Secretary, MOD, Rawalpindi
32- Secretary (DP), MODP, Rawalpindi
33- Secretary (EAD), EAD, Islamabad
34- Secretary (Education), MOFEPT, Islamabad
35- Secretary (Railways), MOR, Islamabad
36- Secretary Climate Change, MOCC, Islamabad
37- Secretary Establishment Division, ESTAB, Islamabad
38- Secretary FPSC, FPSC, Islamabad.
39- Secretary Finance, MOF, Islamabad
40- Secretary Housing, MOHW, Islamabad
41- Secretary IPC, MOIPC, Islamabad
42- Secretary IT, MoIT, Islamabad
43- Secretary Industries & Production, MOIP, Islamabad
44- Secretary Information, Science and Technology Department Government of Sindh,
45- Secretary Kashmir Affair,Gilgit Baltistan & SAFRON, kagbsafron, Islamabad
46- Secretary LAW & Justice, MOLJ, Islamabad
47- Secretary Maritime Affairs, MOMA, Islamabad
48- Secretary Ministry of Parliamentary Affairs, MOPA, Islamabad
49- Secretary MoIBC, MOIBC, Islamabad
50- Secretary NTISB, CAB, Islamabad
51- Secretary Planning, PC, Islamabad
52- Secretary Privatisation Division, PRIDIV, Islamabad
53- Secretary Religious Affairs, MORA, Islamabad
54- Secretary SIFC, SIFC, Islamabad
55- Secretary Science and Technology, MOST, Islamabad
56- Secretary of Interior, MOINC, Islamabad

57- Secretary(MoPHRD), MOPHRD, Islamabad
58- Secretary, PA&SS Division, PASS, Islamabad

SUBJECT: CYBERSECURITY ADVISORY ON DEPLOYMENT OF CLOUD TECHNOLOGY PRODUCTS IN PAKISTAN

In view of ongoing national security, data sovereignty, and regulatory risks, the attached Advisory titled "NCA-23.270126 – National CERT Advisory –Cloud Technology Products in Pakistan" (Annexure) has been issued by the National Cyber Emergency Response Team (National CERT).

2. The advisory highlights the risks posed cloud services, including Zoho Corporation, which are deployed across private and public sectors in Pakistan. These platforms possess privileged administrative capabilities, host data in foreign jurisdictions, and may be exploited for surveillance, intelligence gathering, or strategic targeting.

3. The advisory calls for immediate identification of affected deployments, regulatory engagement, stakeholder sensitization, risk mitigation, and promotion of verified Pakistan-based SaaS alternatives. Particular attention is required where these services are deployed in sensitive, regulated, or nationally significant environments.

4. It is requested that the advisory be disseminated to all relevant entities under your administrative and regulatory purview, ensuring executive-level attention, designation of responsible officers, and compliance monitoring.

Annexure : NCA-23.290126 – National CERT Advisory –Cloud Technology Products in Pakistan

Imran Ali
Assistant-I (Coordination)
30 January , 2026, 09:31:28 AM

Dr Haider Abbas
DG -(nCERT)
Ph:03009634911

Annexure

NCA-23.290126 – National CERT Advisory – Deployment of Cloud Technology Products in Pakistan

1. INTRODUCTION

National CERT has discovered vulnerabilities in the deployment and active use of cloud-based technology products within Pakistan's IT infrastructure, both in government and private sectors. One prominent example is **M/S Zoho Corporation**, an IT services provider, present across education, IT, finance, SMEs, and other sectors in Pakistan.

The adoption and operational use of platforms introduces risks to national security, data sovereignty, and regulatory compliance. The advisory consolidates these concerns and provides actionable recommendations to mitigate strategic and operational exposure.

Threat Type: State-Sponsored Cloud Service Deployment / Data Sovereignty Risk
Severity: High
Attack Vector: Supply Chain / Third-Party Cloud Service Dependency
Authentication Required: Applicable (Authorized access to cloud services)
User Interaction: Voluntary adoption and operational use by organizations
CVSS (Contextual): 8.2 (High – Strategic Data Exposure and National Security Risk)

2. IMPACT

Deployment of these cloud services may enable unauthorized access, digital surveillance, and long-term exposure of sensitive data. Specific potential impacts include:

a. **Data Sovereignty Violations** – Storage and processing of Pakistani data under foreign jurisdictions (e.g., USA, UK, EU), making it subject to compelled disclosure or lawful interception.
b. **National Security Exposure** – Access to sensitive governmental, commercial, and contractor systems.
c. **Regulatory Non-Compliance** – Breach of local cybersecurity, data protection, and CII regulations.
d. **Digital Surveillance & Intelligence Risks** – Latent monitoring of communication metadata, financial flows, personnel, and procurement records.

e. **Privileged Administrative Exploitation** – Zoho SaaS and MDM tools allow remote access to microphones, cameras, location, files, and logs; CRM, HRM, and financial tools aggregate critical metadata.
f. **Critical Data Leakage** – Exposure of commercial, institutional, and operational datasets.
g. **Strategic Dependency** – Entrenchment of these platforms creates difficulty in transitioning to local alternatives.
h. **Service Disruption Risk** – Potential denial, throttling, or manipulation of services during geopolitical crises.
i. **Compliance and Audit Challenges** – Limited visibility into data handling, storage, and foreign legal obligations.
j. **Long-Term Exposure** – Aggregated metadata could enable adversaries to map networks, identify vulnerabilities, and plan targeted operations.

2.1 Identified Local Partners (Non-Exhaustive)

a. MyHosting.com.pk
a. **Address**: 10–12, Arfa Software Technology Park, Ferozepur Road, Lahore
b. aiitsolutions.com
a. **Address**: Office #1, 4th Floor, Mehtab Plaza, Chaklala Scheme-3, Rawalpindi
c. itenablersglobal.com.pk
a. **Address**: B 82, Central Government employees Cooperative Housing Society, Gulshan E iqbal block 10A, Karachi, Pakistan
d. fairchanceforcrm.com
a. **Address**: Lahore, Pakistan
e. hamdtechnologies.biz
a. **Address:** Suite # 401 Mustafa Center SB-40 Block 13 B Gulshan e Iqbal Opposite to bait ul mukarram masjid

These entities are reportedly providing implementation, customization, and support services for Zoho products within Pakistan.

2.2 Attack / Risk Characteristics

a. **Threat Vector:** Authorized use of foreign-hosted SaaS platforms and local deployment partners
b. **Attack Complexity:** Low
c. **Privileges Required:** Administrative SaaS or MDM access
d. **User Interaction:** Routine operations
e. **Risk Nature:** Strategic, systemic, and long-term

2.3 Exploitation Conditions

a. Use of SaaS with privileged admin capabilities
b. Cross-border data hosting and processing
c. Absence of data localization and regulatory oversight
d. Dependence on foreign sub-processors

3. INDICATORS OF RISK (IoRs)

Category	Indicator	Description	Action Required
Cloud Hosting	Data stored offshore	Loss of jurisdictional control	Regulatory review
Vendor Origin	Foreign Countries	Elevated intelligence risk	Risk assessment
Partner Activity	Local deployments	Expanded footprint	Audit deployments
Data Flows	Cross-border transfers	Potential exposure	Enforce localization
Compliance	Unregistered SaaS use	Regulatory breach	Notify regulators
Privileged Tools	Admin, MDM capabilities	Potential surveillance	Restrict access
Aggregated Metadata	CRM, HRM, financial systems	Network mapping / targeting	Data minimization / monitoring
Oversight	Limited visibility / audit	Trust-based reliance	Mandatory reporting
Persistence	Deep integration	Hard-to-exit dependency	Migration strategy

4. AFFECTED USERS / ENVIRONMENTS

a. Private and public sector organizations using foreign state SaaS platforms
b. Contractors linked with LEAs or critical government systems
c. Education, IT, finance, SMEs, and other regulated sectors
d. Entities handling sensitive, strategic, or classified data

5. RECOMMENDED ACTIONS

5.1 Stakeholder Sensitization (MANDATORY)

a. Disseminate advisory to all affected entities
b. Advise refraining from collaboration, installation, or use of foreign state AI/ICT products

c. Encourage adoption of Pakistan-based SaaS alternatives with verified data localization (via P@SHA / MoIT&T)

5.2 Regulatory & Risk Engagement

a. Immediate engagement of sector regulators to identify current deployments
b. Assess national security, data sovereignty, and regulatory risks
c. Require organizations to report usage of these services, including Zoho, HCL Tech, InPage, etc.

5.3 Risk & Compliance Assessment

a. Map all affected systems and data flows
b. Classify systems by sensitivity and exposure
c. Evaluate exit strategies and local alternatives

5.4 Coordination & Strategic Planning

a. Conduct stakeholder meetings to highlight urgency and sensitivity of the issue
b. Identify all government and contractor deployments
c. Track progress and compliance with mitigation directives

6. ACTION SUMMARY & RESPONSE PRIORITIES

Action Type	Specific Steps	Priority
Regulatory Engagement	Identify all foreign origin SaaS usage	MANDATORY
Stakeholder Sensitization	Disseminate advisory, briefing	HIGH
Risk Assessment	Map systems, classify, evaluate	HIGH
Mitigation Planning	Data localization, exit strategies	REQUIRED
Coordination	Meetings, follow-ups, progress tracking	HIGH

7. MONITORING & OVERSIGHT

Authorities and organizations should:

a. Continuously monitor adoption of foreign cloud services
b. Enable reporting to MoIT&T / P@SHA on alternative adoption
c. Require transparency on data hosting and access
d. Review contracts, SLAs, and privacy policies
e. Track geopolitical and legal developments affecting vendors

f. Maintain centralized oversight of cloud technology usage

8. CALL TO ACTION

National CERT urges all relevant authorities, regulators, and organizations to:

1. Immediately identify foreign cloud deployments within their control
2. Restrict privileged admin access for foreign SaaS and MDM tools
3. Engage regulators for compliance review and risk classification
4. Promote adoption of verified local alternatives
5. Conduct stakeholder meetings to highlight sensitivity and monitor progress
6. Treat the matter as **high priority**, given implications for national security, strategic data exposure, and regulatory compliance

Failure to act promptly may result in systemic compromise, unauthorized surveillance, data exfiltration, regulatory breaches, and long-term strategic dependencies.