ICAR
भारतीय कृषि अनुसंधान परिषद
Indian Council of Agricultural Research
कृषि भवन, डॉ. राजेंद्र प्रसाद रोड, नई दिल्ली -110001
Krishi Bhawan, Dr. Rajendra Prasad Road, New Delhi – 110 001

F. No.: 4(2)/2025-ICT (e/file-356613) Dated the 4th November, 2026

To,

All ICAR Institutes / NRCs / Bureaux / ATARIs / CAUs

Subject: Comprehensive Advisory regarding Enforcement of Cybersecurity Protocols, ICT Infrastructure Governance, and GeM Procurement Compliance – reg.

Sir / Madam,

In pursuance of communication **No. F. No. 74-1/2026-Vig-I dated 01st October, 2026** *(copy enclosed)* from the Service Discipline Section, ICAR Headquarters, this advisory is issued for strict compliance across all ICAR Institutes and Hqrs. As mentioned in this letter recent GeM procurement processes have flagged security concerns. Unsecured Wi-Fi networks, absence of firewall log maintenance, non-archival of CCTV footage, and non-compliance with established CERT-In and MeitY directives are some of the issues to be taken care.

To mitigate digital vulnerabilities and prevent the recurrence of such procurement and security lapses, all ICAR Institutes and Units are hereby directed to strictly implement the following mandatory cybersecurity and procurement controls:

1. Compliance with CERT-In and MeitY Guidelines:

- **Mandatory Standards:** All ICT systems, networks, and digital infrastructure across the institute must strictly align with guidelines issued by CERT-In and MeitY.
- **Wireless Network Security:** All institutional Wi-Fi networks must be secured with mandatory password protection, robust encryption, and strict access controls to prevent unauthorized access. Unsecured or open Wi-Fi networks are strictly prohibited.

2. Enhanced Due Diligence in GeM Procurement:

- **IP Address Verification:** Technical Evaluation Committees (TEC) and Institute Purchase Committees must mandate and verify IP address logs during procurement stages to ensure that buyer and bidder sessions do not originate from common IP addresses.
- **Technical Comparative Statements:** Committees must prepare detailed technical comparative statements and conduct rigorous scrutiny of all bid submissions prior to contract awards.

3. Institutional Cybersecurity Governance & Nodal Appointments:

- **Deployment of Officers:** The Cyber Security Nodal Officers of each institute would also act as IT Nodal Officer and Institute's Chief Information Security Officer (CISO). However, we have not received nomination of Cyber Security Nodal Officers still from many ICAR institutes. It is requested to do the needful as early as possible.
- **Cadre Requirement:** The Institute's Cyber Security Nodal Officers or CISO should preferably be nominated from the Scientific / Technical cadre to ensure qualified ICT management and effective cybersecurity oversight.

Contd.../-

4. Firewall Upgradation & Centralized Log Retention:

- **Appliance Upgrades:** All firewall appliances must be upgraded to enable Central Firewall Reporting (CFR).
- **Log Archives:** Firewall log archives must be systematically generated, secured, and maintained for a minimum period of 6 to 12 months in full alignment with prescribed cybersecurity guidelines.

5. CCTV Surveillance & Video Archival:

- **Surveillance Coverage:** Proper CCTV surveillance must be maintained across all critical institutional infrastructure, server rooms, and procurement cells.
- **Recording Archival:** Video recordings must be systematically archived and retained for a reasonable period as per government norms.

6. System Audits, Network Monitoring, and Log Reviews:

- **Continuous Monitoring:** Routine monitoring and periodic security audits of all institutional ICT systems must be conducted.
- **Access Reviews:** Security personnel and IT officers must regularly review firewall logs, administrative access logs, and network connection records to detect anomalies promptly.

7. Capacity Building and Vigilance Training:

- **Staff Awareness:** Institutes must organize regular awareness and capacity-building programs for administrative, finance, and procurement personnel.
- **Focus Areas:** Training must emphasize compliance, procedural vigilance, cybersecurity hygiene, and accountability throughout GeM procurement workflows.

8. Additional Institutional Safeguards:

- **Extended Framework:** While the measures listed above provide the baseline framework, institute heads and Cyber Security Nodal Officers (CISOs) are empowered and required to incorporate additional institutional safeguards and security best practices as deemed necessary to fortify local digital assets.

Action Required & Compliance Timeline

1. Immediate Effect: The controls specified above take effect immediately across all ICAR establishments.

2. Compliance Report: An Action Taken Report (ATR) confirming the designation of Institute Cyber Security Nodal Officers / CISO / IT Nodal Officers, firewall log retention configuration, and TEC verification protocols must be submitted to the undersigned at the earliest.

This issues with the approval of the Competent Authority.

Yours faithfully,

04/11/2026

S.B. Lal, Pr. Scientist (ICT)
& CISO, DARE / ICAR
(eMail: ciso-icar@icar.org.in)

Encl. as above:

Copy for information and necessary action to:

1. US (SDS), ICAR Hqrs (with reference to letter No. F. No. 74-1/2026-Vig-I dated 01.10.2026).
2. PPS to Secretary, DARE and Director General, ICAR, Krishi Bhawan, New Delhi.
3. PPS to Addl. Secretary, DARE & Secretary, ICAR, Krishi Bhawan, New Delhi.
4. PPS to Addl. Secretary, DARE & Financial Adviser, DARE / ICAR, Krishi Bhawan, New Delhi.
5. eOffice Notice Board / Guard File.

भारतीय कृषि अनुसंधान परिषद
INDIAN COUNCIL OF AGRICULTURAL RESEARCH
कृषि भवन, डॉ राजेंद्र प्रसाद मार्ग, नई दिल्ली 110 001
Krishi Bhawan, Dr. Rajendra Prasad Road, New Delhi 110 001
E-mail –us.vigilance1@icar.org.in, Tel: - 91-11-23046619

No. F. No. 74-1/2026-Vig-I Dated: 01st October,2026

Service Discipline Section

Sub: - Issuance of suitable Advisory w.r.t Cybersecurity at ICAR Hqrs and its Institutes-reg.

Indian Council of Agricultural Research (ICAR), through various circulars and guidelines issued from time to time, has emphasized the need for strengthening cybersecurity measures across its Institutes and Headquarters :

2. However, recent instances have been observed during a preliminary enquiry regarding GeM procurement irregularities, in adherence to prescribed cybersecurity protocols. In certain cases, misuse of internet services, including instances of common IP addresses between buyer and bidder, has been flagged, raising serious vigilance concerns. These issues have largely arisen due to deficiencies such as unsecured Wi-Fi access, absence of firewall logs, lack of CCTV archival and non-compliance with CERT-In/MeitY guidelines.
3. The above observations underscore the need for immediate and strict compliance with established cybersecurity practices and strengthening of ICT infrastructure across ICAR institutes. It is, therefore, imperative to reiterate and reinforce adherence to cybersecurity measures to prevent recurrence of such lapses.
4. Accordingly, keeping in view the recommendations and instructions of Government of India/MeitY/CERT-In on cybersecurity matters, ICT Division, ICAR Headquarters, in consultation with CISO, ICAR, is requested to issue a comprehensive advisory to all Institutes.
5. While issuing such advisory, the following measures, inter alia, may be incorporated:

- Strict implementation of CERT-In and MeitY guidelines for all ICT systems, including Wi-Fi access control, firewall logging and CCTV data archival.
- Securing of network infrastructure, including mandatory password protection of Wi-Fi networks and restriction of unauthorized access.
- Due diligence in GeM procurement , wherein Technical Evaluation Committees (TEC) and Institute Purchase Committees ensure verification of IP addresses, preparation of technical comparative statements and thorough scrutiny prior to award of contracts.
- Deployment of dedicated IT Nodal Officer and Chief Information Security Officer (CISO) (preferably from Scientific/Technical cadre) at each institute for effective ICT management and cybersecurity oversight.
- Upgradation of firewall appliances to enable Central Firewall Reporting (CFR) and maintenance of log archives for a minimum period of 6–12 months, in line with prescribed guidelines.
- Ensuring proper CCTV surveillance and archival , with retention of recordings for a reasonable period as per norms.

- Regular monitoring and periodic audit of ICT systems , including review of firewall logs and network access.
- Awareness and capacity-building programmes for administrative and procurement staff to ensure compliance, vigilance and accountability in GeM procurement processes.

6. The above list is illustrative in nature. CISO, ICAR and ICT Division may incorporate additional safeguards and best practices, as deemed appropriate, to ensure a robust cybersecurity framework across all ICAR institutes.

Distribution –

1. ADG, ICT Division
2. CISO, ICAR

Regards,

01/10/2025

(Neeraj Tanwar)
Under Secretary (SDS)