

F. No j-30001(01)/4/2026-Fy (e- 28247)
Government of India
Ministry of Fisheries, Animal Husbandry and Dairying
Department of Fisheries

Krishi Bhawan, New Delhi-110001
Dated 14/10/2026

CIRCULAR

Subject: Inviting applications for rendering services as engagement of one Consultant Grade-II (Team Lead) and three Young Professionals on contract basis in the Department of Fisheries-reg.

The undersigned is directed to state that the Department of Fisheries, Ministry of Fisheries, Animal Husbandry & Dairying, proposes to engage four (04) Individual Consultants on contractual basis for providing specialized technical services in the areas of Cyber Security, Network Security Operations & Management and Application Support.

2. The details of the positions proposed to be engaged are enclosed as Annexure-I.
3. Interested and eligible applicants may submit their applications strictly in the prescribed format enclosed as Annexure-II, along with their CV/resume and supporting documents in respect of educational qualifications, professional certifications and relevant experience through email to the Department at: chandraprabhu.rajagopal@gov.in.
4. Applications shall be submitted on or before 28/10/2026 at 5:00 PM. Applications received after the prescribed closing date and time shall not be considered.

Encl.: As above.

Digitally signed
by
**Chandra
prabhu**
Date: 2026.10.14
16:53:06 +05'30'

(R.Chandraprabhu)
Deputy Director to the Govt of India
Tel:011 233710023

To:

- I. All attached/subordinate offices and organizations under the department of fisheries, Ministry of Fisheries, Animal Husbandry & Dairying.
- II. Director (CS Division), Department of Personnel & Training, Lok Nayak Bhawan, New Delhi – with a request to upload the Circular on the DoP&T website, as appropriate.
- III. NIC, Department of Fisheries – for uploading the Circular on the official website of the Department.

Annexure-I

Terms of Reference for engaging Young Professional and Consultant Grade -II for IT Infrastructure and Cyber Security Cell (Technical)

1.	Number of positions to be filled	Four (4)
2.	Job Location	Department of Fisheries, New Delhi
3.	Name of the position	Senior Cyber Security Consultant Grade-2 (Team Lead)
4.	Number of positions	One (1)
5.	Age	Up to 50 years
6.	Educational Qualification and Experience	Essential: B.Tech.(CSE/IT/EC) or MCA, with 8–10 years of relevant experience in Cyber Security. The candidate must possess at least one globally recognized professional certification, such as CEH, CISSP, or CISM, and must have a minimum of 3 years of relevant work experience in the Central Government and/or Central Public Sector Undertakings (CPSUs/PSUs). and I. Technical Administrator Course/Training Certificate (TM Apex Central/ Apex One/SC-200). II. Minimum 5 years of hands-on experience in deployment, administration, configuration, monitoring, troubleshooting, and management of Anti-APT (Advanced Persistent Threat) solutions, including Endpoint Detection and Response (EDR), Extended Detection and Response (XDR), threat intelligence integration, malware analysis, and incident response. III. Candidates possessing the CISO Deep Dive or Advanced CISO Deep Dive training certificates issued by the National e-Governance Division (NeGD), Ministry of Electronics and Information Technology (MeitY), Government of India, shall be given preference.

7.	Scope of work	The Senior Cyber Security Consultant responsible for planning, implementing, operating and continuously improving the cyber security posture of the Department of Fisheries. The consultant shall provide technical leadership in securing the Department's IT infrastructure, networks, applications, cloud services and digital assets in compliance with the guidelines issued by the Ministry of Electronics & Information Technology (MeitY), CERT-In, NCIIPC and other Government of India authorities. The consultant performs the following key functions: 1. Cyber Security Governance: Implement and periodically review cyber security policies, standards, SOPs and security architecture. • Ensure compliance with Government cyber security guidelines, advisories and regulatory requirements. • Recommend appropriate security controls to strengthen the Department's cyber resilience. 2. Security Operations & Monitoring: • Manage and monitor Security Operations Centre (SOC) activities. • Monitor security events through EDR, UEM, SIEM, SOAR and other security monitoring tools. • Investigate security alerts, analyse incidents and coordinate timely response and remediation. • Perform continuous threat monitoring and threat intelligence analysis. 3. Endpoint Detection & Response (EDR): • Monitor endpoints for malware, ransomware and suspicious activities.

	- Analyse process execution, registry modifications, network connections and user behaviour. - Conduct root cause analysis, threat containment and recovery activities. - Coordinate malware quarantine, endpoint isolation and restoration activities. 4. Malware Analysis & Threat Hunting: - Analyse Indicators of Compromise (IoCs) and Indicators of Attack (IoAs). 5. Digital Forensics & Incident Response (DFIR): - Conduct host, network and mobile forensic investigations. - Perform log analysis, evidence preservation and incident documentation. - Assist in cyber incident investigation and post-incident analysis. 6. Network Security: - Review and strengthen network security architecture. - Secure firewalls, VPNs, IDS/IPS, routers, switches and wireless infrastructure. - Assess network vulnerabilities and recommend mitigation measures. 7. Vulnerability Assessment & Security Review - security reviews of applications, servers and network infrastructure with the help of third-party Security Audit. - Coordinate penetration testing and closure of identified vulnerabilities. 8. Security Compliance - Ensure compliance with Cyber Crisis Management Plan (CCMP), Information Security Policies and MeitY/CERT-In advisories.
--	---

	• Assist in Cyber Security Audits, VAPT, ISO 27001, STQC, GIGW and other compliance activities. 9. Risk Management: • Identify cyber security risks affecting departmental systems. • Recommend risk mitigation strategies and monitor implementation. • Maintain risk registers and security documentation. 10. Capacity Building & Awareness: • Conduct cyber security awareness programmes for departmental officials with the help of NIC, Cert-In. • Provide technical guidance and hands-on support to IT teams. • Assist in developing cyber security best practices across the Department. 11. Reporting & Documentation: • Prepare monthly cyber security reports. • Maintain incident reports, audit reports, compliance reports and management dashboards. • Present security status of the websites. 12. Emerging Technologies: • Evaluate emerging cyber threats, AI-enabled attacks and new security technologies. • Recommend adoption of advanced security solutions for strengthening the Department's cyber security posture. 13. Critical Government Events & VIP Programme Support • Provide end-to-end cyber security and IT infrastructure support during high-level Government meetings, video conferences and national events involving the Prime Minister's Office (PMO), Cabinet Secretariat (CabSec),
--	--

		Ministry of Fisheries, Animal Husbandry & Dairying, MeitY, NITI Aayog and other Central Ministries/Departments. • Ensure secure and uninterrupted operation of IT infrastructure during PRAGATI, inter-ministerial review meetings, national conferences, and high-level review meetings chaired by Hon'ble Prime Minister, Hon'ble Ministers, Cabinet Secretary and other senior Government officials. • Coordinate with NIC, NICNET, CERT-In, MeitY and other Government agencies for ensuring secure connectivity and availability of departmental digital services during VIP events. • Ensure secure operation of video conferencing platforms, network connectivity, endpoint security and secure access for confidential Government meetings. • Provide immediate technical support for cyber security incidents, network failures and IT service disruptions during VIP programmes and mission-critical departmental activities. 15. Coordination with Government Agencies • certifying Authorities (CCA), National Cyber Coordination Centre (NCCC) and other Government organisations (CERT-In, NCIIPC, NIC) on cyber security advisories, audits, vulnerability remediation and compliance requirements. Deliverable / Expected Output: Refer Annexure -IV
8	Name of the position	Young Professional (Network)
9	Number of positions	One (1)
10	Age	Up to 32 Year
11	Educational Qualification and Experience	B.Tech.(CSE/IT/EC/EIC) or MCA, with 3 years of relevant experience in Network. The candidate must possess at least one globally recognized professional certification, such as CCNA, CCNP, and must have a minimum of 2 years of relevant work experience in the Central Government and/or

		Central Public Sector Undertakings (CPSUs/PSUs). Essential Technical Skills: The consultant should have hands-on experience in: • Cisco Enterprise Routers • Cisco Catalyst L2/L3 Switches • HP/Aruba Switches • Fortinet/Palo Alto/Checkpoint Firewalls • Proxy Solutions • Anti-DDoS Solutions • Enterprise Wi-Fi • Cisco Video Conferencing • TCP/IP, IPv4/IPv6 • OSPF, BGP, Static Routing • VLAN, QoS, ACL • VPN (IPSec/SSL) • DNS, DHCP • Network Monitoring Tools (SolarWinds, PRTG, Zabbix, etc.) • Network Automation (basic scripting preferred)
12	Scope of Work	1. Enterprise Network Administration • Design, implement, configure and manage the Department's enterprise network infrastructure. • Ensure high availability, reliability and performance of the departmental LAN, WAN, Wi-Fi and Internet connectivity.

	• Maintain updated network topology diagrams, IP addressing plans and network documentation. • Plan network expansion and modernization based on departmental requirements. 2. Router & Switch Administration • Install, configure and manage Layer-2 and Layer-3 switches. • Configure and manage enterprise routers. • Configure VLANs, Inter-VLAN Routing, ACLs, QoS, STP, EtherChannel and routing protocols. • Monitor bandwidth utilization and optimize network performance. • Perform firmware upgrades and preventive maintenance. 3. Firewall & Network Security: • Configure and manage Next Generation Firewalls. • Configure NAT, Security Policies, VPNs, IPS, IDS and URL Filtering. • Implement Zero Trust Network principles wherever applicable. • Review firewall policies periodically and remove obsolete rules. • Coordinate firewall changes with NIC and security teams. 4. Proxy Server Administration: • Configure and manage Proxy Servers. • Implement Internet access policies. • Configure URL filtering and web access control. • Monitor Internet usage and optimize bandwidth utilization. 5. Anti-DDoS Infrastructure:
--	--

	• Configure and monitor Anti-DDoS protection solutions. • Coordinate with NIC and ISP for mitigation of DDoS attacks. • Monitor network traffic anomalies. • Prepare mitigation reports and recommendations. 6. Wireless Network (Wi-Fi) Management • Install, configure and maintain Enterprise Wireless Access Points. • Implement secure wireless authentication. • Monitor wireless coverage and performance. • Troubleshoot wireless connectivity issues. 7. IP Device Administration Responsible for configuration, maintenance and troubleshooting of: • Enterprise Routers • Layer-2 Switches • Layer-3 Switches • Firewalls • Proxy Servers • Anti-DDoS Solutions • Wireless Controllers • Wireless Access Points • Enterprise Printers • Network Attached Storage (NAS) • Video Conferencing Systems • IP Phones (VoIP) • Network Monitoring Appliances • Internet Gateways
--	---

		• Load Balancers (wherever applicable) 8. Video Conferencing Infrastructure: • Install and maintain Video Conferencing infrastructure. • Configure VC endpoints. • Ensure uninterrupted VC services during high-level Government meetings. • Troubleshoot audio/video/network issues during VIP meetings. 10. Coordination with Government Agencies Coordinate with: • National Informatics Centre (NIC) • NICS • CERT-In • MeitY • NCIIPC • Internet Service Providers • OEM Support Teams • Telecom Service Providers • STQC • CCA • Data Centre Teams • Cloud Service Providers for: • Network Troubleshooting • Circuit Provisioning • NICNET Connectivity • Public IP Management • VPN Configuration • MPLS Connectivity
--	--	--

- Firewall Changes
- Security Compliance
- Network Upgradation

11. Government Network Connectivity

Manage:

- NICNET Connectivity
- MPLS Links
- Leased Line Connectivity
- Internet Redundancy
- VPN Connectivity
- Site-to-Site VPN
- Remote Access VPN
- Government Cloud Connectivity
- Data Centre Connectivity

12. Network Monitoring:

Monitor using enterprise tools:

- Switch Health
- Router Health
- Interface Utilization
- Link Availability
- Latency
- Packet Loss
- CPU & Memory
- Wireless Health
- Internet Utilization
- Bandwidth Reports

Generate:

- Weekly Reports
- Monthly Reports
- Incident Reports

13. Network Troubleshooting

Perform troubleshooting for:

- Routing Issues
- Switching Issues
- DNS
- DHCP
- NAT
- VPN
- Wireless
- VC Systems
- Printer Connectivity
- IP Address Conflicts
- Firewall Rules
- Proxy Configuration

14. Asset & Configuration Management

Maintain inventory and configuration backup of all network devices.

Maintain:

- Configuration Repository
- Firmware Repository
- License Records
- AMC Details
- Network Documentation

15. Documentation

		Prepare and maintain: • Network Architecture Diagram • Rack Diagram • IP Address Scheme • SOPs • Incident Reports • Change Management Documents • Configuration Backup Records 16. Compliance Ensure compliance with: • MeitY Guidelines • NIC Standards • CERT-In Directions • NCIIPC Guidelines • ISO 27001 Controls • GIGW • Government Security Policies • Departmental Information Security Policy 17. Vendor & Project Management • Coordinate with OEMs, vendors and System Integrators. • Verify installation and commissioning of network devices. • Review technical deliverables and service reports. • Assist in procurement, technical evaluation and acceptance testing of network equipment.
--	--	---

		Deliverable / Expected Output: Refer Annexure -IV
12	Name of the position	Young Professional (NIC Application Support)
13	Number of positions	Two (2)
14	Age	Up to 32 Year
15	Educational Qualification and Experience	B.Tech.(CSE/IT/EC/EIC) or MCA, with 3 years of relevant experience in the. The candidate must possess at least one globally recognized professional certification, such as CCNA, CCNP,
16	Scope of Work	1.NIC Applications Support Provide complete support for NIC hosted applications and services including • eOffice • eForms • Bharat VC • VC Scheduler • Video Conferencing Services • Email (@gov.in) • Secure Email Configuration • VPN Services • WiFi Portal Services • DNS Services • SMTP Gateway • Sandes • SewaK • Distribution List Services • MeghRaj Cloud Services • Domain Registration (gov.in) • SSL Certificate Management • Digital Signature (DSC)

- NIC Cloud Portal
- Organization Onboarding
- Mail Migration Support
- NIC Helpdesk Coordination

2. User Support & Helpdesk

Provide L1/L2 application support to

- Officers
- Divisions
- Attached Offices
- Regional Offices
- State Departments

Support includes

- Login issues
- Password reset
- User creation
- Role mapping
- Access permissions
- Functional issues
- Browser compatibility
- Digital Signature issues
- Printing issues
- Upload/download issues

3. Deployment Support

Support

- New application deployment
- Patch deployment
- Rollback
- Version control

		• Configuration management 4. Support during VIP Events Provide dedicated technical support during • PMO Reviews • Cabinet Secretariat Meetings • PRAGATI Meetings • Ministerial Meetings • Secretary Review Meetings • Parliament Sessions • National Conferences • VC with States/UTs • Video Conferences with PMO, Cabinet Secretariat, MeitY, NITI Aayog and other Ministries • Emergency Review Meetings Ensure • Zero downtime • VC readiness • Screen sharing • Presentation support • Digital document support • Connectivity troubleshooting • Real-time technical assistance 5.Deliverables The consultant shall deliver • Application uptime reports • Incident resolution reports • Monthly performance reports • User support logs • Change management records
--	--	---

		• Documentation updates • Compliance reports • Security coordination reports • Training reports • Dashboard reports • Knowledge repository updates 6.Essential Skills • Government e-Governance ecosystem • NIC Applications • eOffice • MeghRaj Cloud • Linux & Windows Server basics • Database (MySQL/PostgreSQL/MSSQL) • DNS & SSL Management • Digital Signature (DSC) • Government Cloud Operations Support • Application Deployment • ITIL Incident Management • Helpdesk Operations • Documentation • Basic Cyber Security Awareness • Coordination with Government agencies • All Type of IT Support of Applications
17	Method of Engagement	The Consultants shall be engaged on a short-term contractual basis through open advertisement and a duly constituted Consultancy Evaluation Committee (CEC), in accordance with the <i>"Procedure and Guidelines for Engagement of Senior Consultants/Consultants Grade-</i>

		II/Consultants Grade-I/Young Professionals in NITI Aayog, 2023." The initial engagement shall be for a period of two (02) years , extendable by one (01) additional year , subject to satisfactory performance, continued functional requirement, and approval of the Competent Authority.															
18	Period of contract	(i)The appointment on the above post will be purely on contract basis initially for a period of two (02) years (ii) Further extendable one (01) additional year subject to satisfactory performance and functional requirement of the Department. (iii) The performance of the consultants will be reviewed after every six months, and their contract shall be extended or discontinued (as the case may be) depending upon their performance. (iv) In no case the appointment shall be extended beyond three years from the initial date of appointment in the department. (v) The decision of the department shall be final in this regard. No right will be accrued in favour of the consultant regarding renewal of contract, absorption in service, etc.															
19	Remuneration (per month)	<table><tr><td>S.No</td><td>Name of Position</td><td>Remuneration (in Rs.)</td></tr><tr><td>1</td><td>Consultant Grade-2</td><td>1,45,000</td></tr><tr><td>2</td><td>Young Professional</td><td>70,000</td></tr></table>	S.No	Name of Position	Remuneration (in Rs.)	1	Consultant Grade-2	1,45,000	2	Young Professional	70,000	Necessary TDS may be deducted as per rules. No other allowance or benefit shall be provided. The remuneration of Individual Consultants will review after completion of one year on annual basis. The enhancement in remuneration will be based on their performance during the year after the recommendation of the Performance Review Committee to be constituted duly approved by the Competent Authority, as per the following criteria: <table><tr><td>Performance</td><td>Remuneration</td></tr><tr><td>Individual Consultants who made significant contribution in their domain and have shown exceptional</td><td>Up to 5% of remuneration with approval of Competent Authority.</td></tr></table>		Performance	Remuneration	Individual Consultants who made significant contribution in their domain and have shown exceptional	Up to 5% of remuneration with approval of Competent Authority.
S.No	Name of Position	Remuneration (in Rs.)															
1	Consultant Grade-2	1,45,000															
2	Young Professional	70,000															
Performance	Remuneration																
Individual Consultants who made significant contribution in their domain and have shown exceptional	Up to 5% of remuneration with approval of Competent Authority.																

		quality in providing the desired output as expected by higher authorities on the assigned/specific task. In exceptional cases, where any Individual Consultant has demonstrated exemplary performance in his/her domain and has made significant contribution in policy making and his or her articles have been published in reputed journals / magazine / newspaper or has authored books etc. NOTE: The criteria based on which 10% enhancement is recommended should be spelt out and brought out in the recommendations made by the Committee while evaluating the performance Of the Individual Consultants.	Up to 10% of remuneration with approval of Competent Authority
20	Other terms of engagement	(i) The Consultants will not be entitled for any separate monthly allowances including but not limited to conveyance allowance, HRA etc. However, in case, the consultant is required to travel outside Delhi in the context of the work/ assignment, the Department shall reimburse the actual cost of travel and daily allowance as per the Rules/regulation of the Central Government applicable to Group-B Non-Gazetted Officer. (ii) The Consultants will not be eligible for any other facilities such as residential telephone, residential accommodation, CGHS and Medical	

		reimbursement, personal support staff, transport facilities etc. (iii) The Consultant shall be entitled to leave at the rate of 1.5 days for each completed month of service, with no accumulation of leave beyond the calendar year, on a pro-rata basis. Accordingly, no remuneration shall be paid for any absence exceeding 18 days in a year (calculated on a pro-rata basis). Un-availed leave shall not be carried forward to the next year. (iv) The Consultant will be required to discharge the duties as assigned to him/her by the Department. In case a consultant leaves before completion of 6 months, he/she will not get any experience certificate. (v) The Income Tax or any other tax liable to be deducted, as per the prevailing rules will be deducted at source before effecting the payment for which the Ministry of will issue TDS Certificate. (vi) The consultant shall, in no case, work for or represent in court or before any other authority, tribunal etc. or give opinion/ advice to any person other than this Department in any matter during the period of his/ her engagement with Department of Fisheries. Further, in no case, the consultant shall act, or conduct anything with regard to any person or render any advice to the Department which is adverse to the interest of Department of Fisheries. (vii) The contract of consultant may be terminated, after giving one month notice, in following situations:- • If the Consultant is unable to do the assigned work. • Quality of the assigned works is not to the satisfaction of the Department. • If the consultant is absent from duty Without due authorization.
--	--	--

		• If the Department elects not to renew the contract of the consultant. • The contractual employee is found lacking in honesty and integrity or violates the confidentiality clause. (viii) The Department reserves the rights to terminate the contract without giving any explanation or whatsoever with immediate effect without any remuneration or notice period on the ground of proven misconducts. (ix) Termination shall be effected by written notice of 30 days served to the consultant. The termination will be without prejudice to either party's rights accrued before termination. (x) The Consultant is required to give 30 days' notice to the Department in case he/she opts to quit the assignment. (xi) Jurisdiction for legal disputes, if any arising during the period of the contract, will be in Delhi Courts only. (xii) The person who has worked as consultant shall not disclose the information received by him/her during the period of such engagement to any person other than this Department at any time whether during continuance of such engagement or after its severance. (xiii) Further, the consultant shall not represent, advice or work for any person against the interest of this Department for 02 years from the date of termination or contract end date in the matters related to the Department.
21.	Selection process	(a) Selection of the Consultant will be done on the basis of personal interview/talk by a Consultancy Evaluation Committee (CEC) (b) Only the short-listed candidates shall be called for the interview. (c) No TA or DA will be paid for attending the interview.

		(d) At the time of interview, the shortlisted candidates shall have to produce their bio-data and certificates, in original for verification. (e) The decision of the competent authority on selection of candidates will be final and no correspondence on this subject will be entertained.
22.	Attendance and working days	a) The working hours of the consultants shall be same as regular Govt. employees working in the Department. b) No extra remuneration shall be allowed for working beyond office hours or on Saturdays/ Sundays/ Gazetted Holidays. Compensatory leave in such cases shall be at the discretion of the competent authority. Note: The Support Staff (Network/VC/Application) shall attend the office and provide necessary support as and when required, including during various programmes/events of the Department and as per the requirement of the Department.
23.	Confidentiality and secrecy	(a) During the period of assignment with Department of Fisheries, the consultants would be subject to the provisions of India Official Secret Act, 1923 and will not divulge any information gathered during the period of his/ her assignment to anyone who is not authorized to know the same. (b) Selected candidates shall provide integrity certificates from 2 references known to them. (c) A self-undertaking shall be provided by the candidate to the effect that no criminal record or criminal case in any court is pending against him/her.

Annexure II

Department of Fisheries

Proforma for Inviting application

1.	Name	
2.	D.O.B.	
3.	Current Address	
4.	Permanent Address	
5.	Education Qualification	
6.	Experience	
7.	Certificate (International/Global and training)	
8.	Present Address	
9.	Contact No.	
10.	Email ID	
11.	Updated CV (World Bank Formats)	

Documents required:

1. Education Qualification
2. Experience Certificate
3. Aadhar Card
4. All Global/Training Certificates
5. Police Verification

Additional Terms and Conditions for Engagement of Individual Consultants

Consultancy Terms and Conditions:

1. Legal Status: The Individual Consultant shall have the legal status of an independent Consultant vis-à-vis the Department of Fisheries (DoF) and shall not be regarded, for any purpose, as being either a “staff” of DoF or an “official” of DoF. Accordingly, nothing within or relating to the Consultancy Contract shall establish the relationship of employer and employee, or of principal and agent, between the Department of Fisheries and the Individual Consultant.

2. Standards of Conduct:

2.1 General Conduct: The Individual Consultant shall neither seek nor accept instructions from any authority external to the Department of Fisheries in connection with the performance of his/her obligations under the Consultancy Contract. The Individual Consultant shall not take any action during the period of engagement, whether in respect of the performance of the Consultancy Contract or otherwise related to his/her obligations under the Contract, that may adversely affect the interests of the Department of Fisheries. The Individual Consultant shall perform his/her obligations under the Consultancy Contract with due regard to the interests of the Department of Fisheries and shall comply with all applicable laws, rules, regulations, Government instructions, cyber security policies and security requirements applicable to the performance of the consultancy services. Failure to comply with the applicable standards of conduct may constitute grounds for termination of the Consultancy Contract.

2.2 Confidentiality and Information Security

The Individual Consultant shall maintain strict confidentiality with respect to all information, data, documents, credentials, configurations, network architecture, security architecture, logs, vulnerability information, incident information and other material accessed during the course of the engagement.

The Consultant shall:

- Not disclose departmental information to any unauthorized person or organization.
- Not copy, transfer, store or transmit departmental information through unauthorized devices, applications, cloud services or communication channels.
- Follow the Department's Information Security Policy and applicable Government cyber security guidelines.

- Follow applicable directions/advisories issued by MeitY, CERT-In, NCIIPC, NIC and other competent Government authorities.
- Immediately report any suspected security incident, data leakage, unauthorized access or compromise of departmental information to the designated authority.
- Ensure that credentials, passwords, security keys, configuration files and other sensitive information are adequately protected.

The confidentiality obligations shall continue to remain applicable even after completion or termination of the Consultancy Contract.

2.3 Prohibition of Sexual Exploitation and Abuse / Workplace Conduct:

During the performance of the Consultancy Contract, the Individual Consultant shall comply with the Sexual Harassment of Women at Workplace (Prevention, Prohibition and Redressal) Act, 2013, and amendments thereto, and all applicable rules, regulations and Government instructions issued in this regard. Violation of applicable provisions may constitute a breach of the Consultancy Contract and may attract appropriate action, including termination of the contract, in accordance with applicable law and Government rules.

3. Title Rights, Copyrights, Patents and Other Proprietary Rights

3.1 Departmental Equipment:

Title to any equipment, devices, systems, software, documents, data, credentials, tools or other materials provided by the Department of Fisheries to the Individual Consultant for performance of the Consultancy Contract shall remain with the Department.

3.2 Intellectual Property Rights:

The Department of Fisheries shall be entitled to all intellectual property rights, including but not limited to copyrights, patents, designs, processes, inventions, methodologies, technical documents, reports, recommendations, scripts, configurations, documentation, dashboards and other materials developed specifically for the Department by the Individual Consultant during the course of the Consultancy Contract. The Individual Consultant shall not reproduce, publish, distribute, disclose, commercially exploit or otherwise use such materials without prior written permission of the Department.

4. Confidential Nature of Documents and Information:

The Individual Consultant shall maintain strict confidentiality of all official information, documents and data accessed during the consultancy engagement. The Consultant shall not, without the prior written approval of the Department of Fisheries:

- Publish any article, report or technical paper containing departmental information.
- Share departmental information through social media or other public platforms;
- Communicate departmental information to any newspaper, media organization or external agency;

- Share screenshots, photographs, network diagrams, configurations, security reports, vulnerability reports, incident details or other departmental information.
- Disclose any information relating to cyber security incidents, vulnerabilities, security controls, network architecture or IT infrastructure of the Department.

The Consultant shall not share any material or information received or generated during the consultancy engagement with any external agency, vendor, OEM, service provider or other person except where such sharing is specifically authorized by the Department.

In the event of premature termination or completion of the Consultancy Contract, all obligations relating to confidentiality and information security shall continue to remain effective.

5. Use of Name, Emblem or Official Seal of the Department of Fisheries:

The Individual Consultant shall not advertise or otherwise make public, for the purposes of commercial advantage or otherwise, that he/she has a contractual relationship with the Department of Fisheries.

The Consultant shall not use the name, emblem, logo, official seal or abbreviation of the Department of Fisheries or the Ministry of Fisheries, Animal Husbandry & Dairying, or represent himself/herself as an employee or official of the Government of India, without prior written permission of the Department.

The Individual Consultant shall not use his/her engagement with the Department for any commercial, promotional or professional representation without prior written approval of the competent authority.

6. Conflict of Interest

The Individual Consultant shall avoid any situation involving an actual, potential or perceived conflict of interest during the period of engagement.

The Consultant shall immediately disclose to the Department any circumstances that may give rise to a conflict of interest, including any professional or financial relationship with:

- Vendors;
- OEMs;
- System Integrators;
- Service Providers;
- Cyber Security Audit/VAPT agencies;
- Cloud Service Providers; or
- Any other organization dealing with the Department in matters related to the consultancy assignment.

The Individual Consultant shall not use information obtained during the consultancy for personal or commercial benefit.

7. Insurance:

The Individual Consultants shall be solely responsible for taking out and for maintaining adequate insurance required to meet any of their obligations under the Consultancy Contract, as well as for arranging, at their own expense, such as life, health and other forms of insurance as the Individual Consultant as they may consider appropriate to cover the period during which they are engaged.

8 Travel, Medical Clearance and Service incurred Death, Injury or Illness:

8.1 DoF may require the Individual Consultant to submit a Statement of Good Health from a registered physician prior to commencement of work in any offices or premises of DoF.

8.2 In the event of the death, injury or illness of any Individual Consultant which is attributable to the performance of engagement on behalf of DoF under the terms of the Consultancy Contract while the Individual Consultant is traveling at the expense of DoF or is performing any responsibilities under the Consultancy Contract in any offices or premises of DoF or Government of India, the Individual Consultant or the Individual Consultant's dependents, as appropriate, shall not be entitled to any compensation.

9 Force Majeure and other Conditions:

9.1 Force majeure as used herein means any unforeseeable and irresistible act of nature, any act of war (whether declared or not), invasion, revolution, insurrection, or any other acts of a similar nature or force, provided that such acts arise from causes beyond the control and without the fault or negligence of any Individual Consultant.

9.2 The Individual Consultants acknowledge and agree that, with respect to any obligations under the Consultancy Contract that they must perform in or for any areas in which DoF is engaged in, preparing to engage in, or disengaging from any peacekeeping, humanitarian or similar operations. Any delay or failure to perform such obligations arising from or relating to harsh conditions within such areas or to any incidents of civil unrest occurring in such areas shall not, in and of itself, constitute force majeure under the Consultancy Contract.

10 Termination:

The DoF can terminate the Consultancy Contract at any time without prior notice and without providing any reason for it. DoF reserves the right to terminate the services of an Individual Consultant at any stage, in the event of a serious failure in the performance of the assigned task or in the case of a failure. However, in the normal course, DoF will provide one month's notice to the Individual Consultant. The Individual Consultant can also seek for termination of the Consultancy Contract upon giving one month's notice to the DoF.

11 Audits and Investigations:

Each invoice paid by DoF shall be subject to a post-payment audit by auditors, whether internal or external, of DoF or by other authorized and qualified agents of DoF at any time during the term of the Consultancy Contract and for a period of two (2) years following the expiration or premature termination of the Consultancy Contract. DoF shall be entitled to a refund from the Individual Consultant for any amounts shown by such audits to have been paid by DoF other than in accordance with the terms and conditions of the Consultancy Contract. The Individual Consultant acknowledges and agrees that, from time to time, DoF may conduct investigations relating to any aspect of the Consultancy Contract or the award thereof, the obligations performed under the Consultancy Contract, and the operations of the Individual Consultant generally relating to performance of the Consultancy Contract. The right of DoF to conduct an investigation and the Individual Consultant's

obligation to comply with such an investigation shall not lapse upon expiration or premature termination of the Consultancy Contract. The Individual Consultant shall provide full and timely cooperation with such inspections, post-payment audits or investigations. Such cooperation shall include, but shall not be limited to, the Individual Consultant's obligation to make available such personal and any relevant documentation for such purposes at reasonable times and on reasonable conditions and to grant to DoF.

11 Settlement of Disputes:

DoF and the Individual Consultant shall use their best efforts to amicably settle any dispute, controversy or claim arising out of the Consultancy Contract or the breach, termination or invalidity thereof. Work related grievances, if any, should be processed as per the redressal mechanism established at DoF.

12 Governing Law: The Consultancy shall be governed by the laws of India and is subject to the exclusive jurisdiction of the Courts at Delhi.

13 Conflict of Interest: The Individual Consultants shall be expected to follow all the rules and regulations of the Government of India which are in force. They will be expected to display utmost honesty, secrecy of office and sincerity while discharging their duties. In case the services of any Individual Consultant are not found satisfactory or found in conflict with the interests of the DoF/Government of India, his/her engagement will be liable for discontinuation without assigning any reason.

Annexure IV

Deliverable / Expected Output: Senior Cyber Security Consultant Grade-2 (Team Lead)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
1	Cyber Security Governance	Review and update cyber security policies, SOPs, security standards and security architecture; prepare recommendations for strengthening cyber resilience.	Initial review within 90 days; thereafter Half-yearly/as required
2	Cyber Security Compliance	Maintain compliance tracker against applicable MeitY, CERT-In, NTRO/NCIIPC, CCMP and other Government cyber security advisories/directions.	Monthly / as and when advisory is issued
3	Security Operations	Monitor SOC activities and security events generated through EDR, UEM, SIEM, SOAR and other security tools; maintain security event and incident records.	Continuous; Monthly report
4	Security Incident Response	Analyse security alerts/incidents, coordinate containment, remediation and recovery, and document actions taken.	Critical incidents: immediate; Incident report within 24–48 hours of closure
5	EDR Monitoring	Monitor endpoints for malware, ransomware, suspicious processes, registry modifications, abnormal network connections and other malicious activities.	Continuous; Monthly summary

Deliverable / Expected Output: Senior Cyber Security Consultant Grade-2 (Team Lead)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
6	Threat Hunting	Analyse IoCs/IoAs and conduct threat-hunting activities for identified threats relevant to departmental infrastructure.	Monthly / threat-driven
7	Malware Analysis	Analyse suspicious files, processes and endpoint activities and recommend containment/remediation measures.	As required; incident-wise report
8	DFIR	Support host/network/mobile forensic investigation, log analysis, evidence preservation and post-incident analysis.	Incident-based
9	Network Security	Review firewall, VPN, IDS/IPS, router, switch and wireless security configurations and recommend hardening measures.	Quarterly / after major changes
10	Vulnerability Management	Coordinate security reviews/VAPT of applications, servers and network infrastructure with authorised third-party security auditors and track remediation.	As per audit/VAPT schedule
11	Vulnerability Closure	Maintain vulnerability register and monitor closure of identified vulnerabilities according to severity and approved remediation timelines.	Continuous; Monthly status
12	Security Audit & Compliance	Coordinate Cyber Security Audit, VAPT, ISO 27001, and other applicable compliance activities and maintain closure tracker.	As per audit schedule; Monthly status
13	Risk Management	Identify cyber security risks, maintain/update Cyber Security Risk Register and monitor implementation of mitigation measures.	Monthly / quarterly review
14	Security Awareness	Coordinate cyber security awareness programmes for departmental officials with NIC/CERT-In/other competent agencies and provide technical guidance to IT teams.	At least quarterly / as approved
15	Security Reporting	Submit consolidated Cyber Security Status Report covering incidents, vulnerabilities, EDR/SIEM alerts, compliance, risk, audit status and security posture of departmental websites/applications.	Monthly

Deliverable / Expected Output: Senior Cyber Security Consultant Grade-2 (Team Lead)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
16	Management Dashboard	Maintain/update management-level cyber security dashboard indicating security posture, major incidents, open vulnerabilities, compliance status and pending actions.	Monthly
17	Website Security	Present security status of departmental websites/applications, including security audit/VAPT status, vulnerabilities and remediation progress.	Monthly
18	Emerging Threats	Assess emerging cyber threats, AI/ML-enabled attacks and relevant security technologies and submit recommendations for appropriate security controls/solutions.	Quarterly / threat-based
19	Critical Government Events	Provide end-to-end cyber security and IT infrastructure support during PMO, Cabinet Secretariat, PRAGATI, Ministerial, inter-ministerial and other high-level Government programmes.	Event-based
20	VIP/VC Security	Ensure secure and uninterrupted operation of VC, network connectivity, endpoint security and secure access during critical Government/VIP meetings.	Event-based
21	Critical Incident Support	Provide immediate cyber security/technical coordination during cyber incidents, network failures or IT service disruption during mission-critical events.	Immediate / 24x7 during notified critical events
22	Government Agency Coordination	Coordinate with NIC, NICNET, CERT-In, NCIIPC, CCA, NCCC, MeitY and other competent Government agencies for advisories, audits, incidents, vulnerability remediation and compliance.	Continuous / as required
23	Documentation	Maintain updated security architecture, incident records, risk register, vulnerability register, audit records, compliance tracker, SOPs and other security documentation.	Continuous; monthly review
24	Quarterly Security Review	Conduct a consolidated review of the Department's cyber security posture and submit recommendations for improvement.	Quarterly

Deliverable / Expected Output: Senior Cyber Security Consultant Grade-2 (Team Lead)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
25	Annual Cyber Security Assessment	Prepare consolidated annual assessment of cyber security posture, major risks, incidents, compliance status and improvement roadmap.	Annually

Deliverable / Expected Output: Young Professional (Network)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
1	Enterprise Network Administration	Maintain secure, reliable and high-performing LAN, WAN, Wi-Fi and Internet infrastructure; identify capacity/performance issues and submit improvement recommendations.	Continuous; Monthly report
2	Network Architecture	Maintain updated network topology, logical/physical architecture diagrams, IP addressing plan, VLAN details and network documentation.	Initial within 30 days; update after every major change
3	Network Expansion & Modernization	Prepare technical assessment and recommendations for network expansion, modernization and capacity enhancement based on departmental requirements.	As required; proposal within 15 working days of requirement
4	Router Administration	Configure, monitor and maintain enterprise routers, routing protocols, NAT, ACLs and related configurations.	Continuous; configuration record after every change

Deliverable / Expected Output: Young Professional (Network)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
5	L2/L3 Switch Administration	Configure and maintain L2/L3 switches including VLAN, Inter-VLAN routing, STP, EtherChannel, QoS and ACL configurations.	Continuous; configuration backup monthly/after changes
6	Network Performance	Monitor bandwidth, interface utilisation, latency, packet loss, CPU/memory and link performance and recommend corrective measures.	Continuous; weekly monitoring and monthly report
7	Firmware & Preventive Maintenance	Maintain firmware/software version records and coordinate approved firmware upgrades and preventive maintenance of network devices.	Quarterly / as recommended by OEM
8	Firewall Administration	Configure and manage approved firewall policies, NAT, VPN, IDS/IPS, URL filtering and other network security controls in coordination with authorised security/NIC teams.	Continuous; monthly policy review
9	Firewall Rule Review	Review firewall rules and identify obsolete, duplicate or unnecessary rules for approval-based removal/modification.	Monthly / quarterly formal review
10	Proxy Administration	Maintain proxy configuration, Internet access policies and URL filtering/web access controls and monitor Internet usage/bandwidth.	Continuous; monthly report
11	Anti-DDoS	Monitor Anti-DDoS infrastructure and coordinate with NIC/ISP during suspected or confirmed DDoS events.	Continuous; immediate during incident
12	DDoS Incident Report	Prepare technical analysis, mitigation and post-incident report for DDoS/network traffic anomalies.	Within 48 hours of incident closure
13	Wi-Fi Management	Maintain enterprise wireless controllers/access points, secure authentication, coverage and performance.	Continuous; monthly health report
14	Wi-Fi Survey & Optimization	Identify coverage, capacity and connectivity issues and recommend corrective measures.	Quarterly / as required
15	IP Device Administration	Maintain configuration, connectivity and troubleshooting support for routers, switches,	Continuous

Deliverable / Expected Output: Young Professional (Network)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
		firewall, proxy, APs, printers, NAS, IP phones, VC systems, gateways and other network-connected devices.	
16	Video Conferencing	Ensure readiness, configuration and availability of VC infrastructure and endpoints for departmental and high-level Government meetings.	Event-based; readiness before each notified event
17	VIP/High-Level Meetings	Provide technical network/VC support for PMO, Cabinet Secretariat, PRAGATI, Ministerial, inter-ministerial and other critical Government meetings/events.	Event-based
18	Government Network Connectivity	Maintain NICNET, MPLS, leased line, Internet redundancy, VPN, site-to-site VPN, remote access VPN, Government Cloud and Data Centre connectivity.	Continuous; monthly availability report
19	Network Availability	Monitor network links and connectivity and coordinate timely restoration of outages with NIC, ISP, telecom and service-provider teams.	Continuous; immediate escalation for critical outage
20	Government Agency Coordination	Coordinate with NIC, NICS, CERT-In, MeitY, NCIIPC, ISPs, OEMs, telecom providers, STQC, CCA, Data Centre and Cloud Service Providers for network/security-related activities.	As required; action tracker monthly
21	Network Monitoring	Monitor switch/router health, interface utilisation, link availability, latency, packet loss, CPU/memory, Wi-Fi health and Internet utilisation through available enterprise monitoring tools.	Continuous
22	Network Monitoring Reports	Generate network health, availability, bandwidth and performance reports.	Weekly / Monthly
23	Network Troubleshooting	Diagnose and resolve/escalate routing, switching, DNS, DHCP, NAT, VPN, wireless, VC, printer connectivity, IP conflict, firewall and proxy issues.	Incident-based

Deliverable / Expected Output: Young Professional (Network)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
24	Incident Management	Maintain incident/ticket records, root cause, action taken, escalation and closure status for network incidents.	Incident-wise; critical incidents immediately
25	Asset Inventory	Maintain updated inventory of all routers, switches, firewalls, proxy servers, Anti-DDoS systems, wireless controllers/APs, printers, NAS, VC systems, IP phones, gateways and other network devices.	Continuous; formal monthly update
26	Configuration Management	Maintain configuration backups and a central configuration repository for network devices.	After every major change; monthly verification
27	Firmware & License Records	Maintain firmware, software, subscription and license records of network/security devices.	Monthly / whenever changed
28	AMC & Warranty	Maintain AMC/warranty records and coordinate preventive/corrective maintenance with OEM/vendor.	Monthly
29	Network Documentation	Maintain network architecture diagram, rack diagram, IP scheme, VLAN mapping, port mapping, SOPs, configuration records and change documentation.	Initial/update within 7 working days of major change
30	Change Management	Document and maintain records of approved network configuration changes, including pre-change and post-change status.	Change-wise
31	Compliance	Assist in ensuring network infrastructure compliance with applicable MeitY, NIC, CERT-In, NCIIPC, ISO 27001, GIGW and Departmental Information Security requirements.	Monthly/quarterly review
32	Security Hardening	Identify insecure network configurations and recommend/implement approved hardening measures for routers, switches, firewalls, proxy, Wi-Fi and other network devices.	Quarterly / risk-based
33	Audit Support	Provide technical information, configurations, diagrams and evidence required during security audits, VAPT, STQC and other authorised assessments.	Audit-wise

Deliverable / Expected Output: Young Professional (Network)			
Sl. No.	Area	Deliverable / Expected Output	Frequency / Timeline
34	Vendor/OEM Coordination	Coordinate with OEMs, System Integrators and vendors for installation, commissioning, troubleshooting, upgrades and maintenance of network infrastructure.	As required
35	Technical Verification	Verify installation, configuration, commissioning and performance of network equipment against approved technical specifications.	Project-wise
36	Procurement Support	Provide technical inputs for network equipment procurement, technical evaluation, testing and acceptance of supplied equipment.	Project/procurement-wise
37	Project Implementation	Assist in network upgrade, migration, expansion, commissioning and integration projects undertaken by the Department/NIC/other Government agencies.	Project-wise
38	Monthly Management Report	Submit consolidated report covering network availability, incidents, bandwidth, device health, security issues, pending actions, AMC, changes and recommendations.	By 5th working day of following month
39	Quarterly Network Review	Conduct comprehensive review of network performance, capacity, security configuration, availability and modernization requirements.	Quarterly
40	Annual Network Assessment	Prepare annual assessment of departmental network infrastructure and submit improvement/modernization roadmap.	Annually

