भारतीय भूचुम्बकत्व संस्थान

Indian Institute of Geomagnetism

(एक स्वायत्त अनुसंधान संस्थान, विज्ञान और प्रौद्योगिकी विभाग, भारत सरकार)

(An Autonomous Research Institute, Department of Science and Technology, Government of India)

Telephone : 022 – 2748 4000
FAX : 022 – 2748 0762

Address: Plot No. 5, Sector-18, Kalamboli Highway, New Panvel, Navi Mumbai 410 218

Email : iig.pso.stores@iigm.res.in

Website: www.iigm.res.in

LIMITED TENDER ENQUIRY FOR IT SECURITY AUDIT OF IT INFRASTRUCTURE AT IIG HQ, ALL REGIONAL CENTERS AND OBSERVATORIES.

Tender No. IIG/TENDER/ 04/2023

TENDER DOCUMENT

AT

INDIAN INSTITUTE OF GEOMAGNETISM
(DEPARTMENT OF SCIENCE & TECHNOLOGY)
PLOT NO.5, SECTOR-18 KALAMBOLI HIGHWAY,
NEW PANVEL, NAVI MUMBAI 410 218

1. *Description of IT Audit Work at IIG:*

IIG would like to engage a third party firm to perform Information System audit services including a cyber-security audit, review of their existing IT policies, creation of IT policies in line CERT-In guidelines and ISMS readiness. The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs of quality standard IT policy, which includes the evaluation and gap analysis of the following with respect to CERT-IN guidelines:

- Current IT infrastructure of IIG
- Network and devices in use
- Operating systems and databases at Server level and User level
- Application packages and databases
- IT Policies including Operational Procedures in the current IT setup at IIG
- Identification of vulnerabilities, security flaws, gaps and loopholes
- Carry out ethical Internal and External Penetration Test for IIG IT setup and network

IIG would like to have the audit performed in a phased manner, wherein the

a) The **First Cyber Security Audit** exercise needs to be commenced within 15 business days of issuing the Work Order. This needs to be done at all offices Locations (IIG H.Q. and IIG regional Offices) and Departmental end users for all types of IT systems of IIG for Cyber Security. Report of Cyber Security Gaps along with the recommendations needs to be provided by the Bidder and based on the same security Gap analysis and action would be taken at IIG end. The First Phase of the Cyber Security Audit and its Reporting need to be completed within 20 business days of commencement. Creation of Policies, etc need to be completed within next 10 business days.

b) After the end of the First Phase of the Cyber Security Audit and Reporting thereof by the bidder, IIG would take some reasonable time to study the Gaps in Cyber Security and would attempt to bridge the gaps as much as possible. After the Gap bridging exercise by IIG has been completed, the bidder would be informed accordingly by concerned IIG representative, and thereafter the bidder should commence the Second Phase of Cyber Security Audit exercise. The time taken by IIG for bridging the Cyber Security Gap will not affect the bidder in any way as the bidder will not be held responsible for any delay in the same.

c) The **Second Cyber Security** Audit needs to be completed within 20 business days after concerned IIG representative gives the go ahead for the Second Phase exercise. The purpose of the Second Phase Audit exercise would be to review and ensure that remediation action has been taken against all the observation points/gaps. The Second phase audit exercise should also result in a Detailed Report and Analysis to be submitted for the current Cyber Security

status of IIG.

1. Project management

Project resources:

- The persons deployed should have suitable auditor qualification and certifications such as CISA / CISSP / ISO 27001 Assessor/ISA or any other formal IT security auditor qualifications etc. The details are required to be submitted as per format in Annexure #6 and Annexure #7.

The followings are the minimum Requirements of the Project Team:

1. Project Manager – 1 No.

a) The Project Manager must have completed minimum 5 IS Audit including one in Central/State Govt. / PSUs / Bank.

b) At least one IS Audit as Lead Auditor

2. Team Members – 2 Nos.

a) Both the Team Member must have completed minimum 2 IS Audit

Since the continuity of the project team is essential for the success of the project,

IIG expect the Successful Bidders to follow diligent process for ensuring this.

- Under any circumstances when the Resource Personnel are to be replaced or removed, Successful Bidder shall put forward the profiles of personnel being proposed as replacements. These profiles should be either equivalent or better than the ones being replaced. However whether these profiles are better or equivalent to the ones being replaced will be decided by IIG or its authorized representative. IIG or its authorized representative will have the right to accept or reject these substitute profiles.

Scope of Work

1 Background and Objective of the Assignment

IIG would like to engage a third party firm to perform services including a cyber-security audit, review of their existing IT policies, creation of IT policies in line with ISMS readiness. The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs, which includes the evaluation and gap analysis of the following with respect to CERT-IN guidelines:

- Current IT infrastructure of IIG
- Network and devices in use
- Operating systems and databases at Server level and User level
- Application packages and databases
- IT Policies including Operational Procedures in the current IT setup at IIG
- Identification of vulnerabilities, security flaws, gaps and loopholes
- Carry out ethical Internal and External Penetration Test for IIG IT setup and network.

IIG would like to have the audit performed in a phased manner, wherein the

a. The **First Cyber Security Audit** exercise needs to be commenced within 15 business days of issuing the Work Order. This needs to be done at all offices Locations (IIG H.Q. and IIG remote Offices) and Departmental end users for all types of IT systems of IIG for Cyber Security. Report of Cyber Security Gaps along with the recommendations needs to be provided by the Bidder and based on the same security Gap analysis and action would be taken at IIG end. The First Phase of the Cyber Security Audit and its Reporting need to be completed within 20 business days of commencement. Creation of Policies, etc need to be completed within next 10 business days.

b. After the end of the First Phase of the Cyber Security Audit and Reporting thereof by the bidder, IIG would take some reasonable time to study the Gaps in Cyber Security and would attempt to bridge the gaps as much as possible. After the Gap bridging exercise by IIG has been completed, the bidder would be informed accordingly by concerned IIG representative, and thereafter the bidder should commence the Second Phase of Cyber Security Audit exercise. The time taken by IIG for bridging the Cyber Security Gap will not affect the bidder in any way as the bidder will not be held responsible for any delay in the same.

c. The **Second Cyber Security** Audit needs to be completed within 20 business days after concerned IIG representative gives the go ahead for the Second Phase exercise. The purpose of the Second Phase Audit exercise would be to review and ensure that remediation action has been taken against all the observation points/gaps. The Second phase audit exercise should also result in a Detailed Report

and Analysis to be submitted for the current Cyber Security status of IIG.

2 Scope of Work:

The Scope of work for Cyber Security Audit would be as per the Guidelines of CERT-IN and would be under the following broad categories:

2.1 CSAF audit:

Audit has to be carried out as per the CERT-IN guidelines and the Cyber Security Assessment Framework (CSAF) Version-2. Audit will include compliance audit as per CSAF markers along with the technical sampling audit for evidence gathering.

The scope of work would cover the following areas:

- Assessment against CSAF markers and evidence collection
- Gap Analysis against CSAF
- Documented evidences
- Compliance Audits

2.2 Operating Systems and System Software such as Server Software, Domain controller Server, Server Hardware such as Blade/chassis Servers, Rack Servers, virtual servers, etc. The audit will include the server vulnerability assessment, pack and service patch updates, backdoor checks, default configuration.

2.3 Network connections of leased lines between Corporate and Port Office. Routers & Firewalls in IIG. Controls of Internet and other network access to various end-users by firewalls and anti-virus policies. The audit will include the network architecture review, network vulnerability assessment and network configuration review based on the vulnerability assessment. The bidder is supposed to analyze all reports, logs, etc. of the cyber security devices installed in IIG and provide input on cyber security policies for the same.

2.4 End user device audit: admin/user password control, license control, OS patches, updates, virus updates, shared folders access control, use of external devices, presence of unnecessary software.

2.5 Application audit

Audit has to be carried out on all the Software Applications and Packages that are exposed to Internet in IIG and also restrict any unauthorized software uses and installations, etc.

2.6 The overall purpose of the Cyber Security Audit exercise is to conform to the IT security needs of quality standard ISO 27001, which includes the evaluation and gap analysis of the following with respect to CERT-In guidelines :

a) Current IT infrastructure of IIG.
b) Network and devices in use.
c) Operating systems at Server level and User level.
d) Application packages and database.
e) Operational Procedures in the current IT setup at IIG.
f) Identification of vulnerabilities, security flaws, gaps and loopholes.
g) Carry out ethical Internal and External Penetration Test for IIG IT setup and network.

2.7 Review the current IT Security Policy and provide recommendations for a roadmap to provide cyber secure IT infrastructure to the end users including suggestions for best practices and procedures for IIG.

2.8 The Bidder should provide the below mentioned details at the starting of the Cyber Security Audit exercise:

a) Methodology in which the Cyber Security Audit activity to be done, this will include the time frame of each activity so as to organize the cyber audit activity for better control and monitoring.
b) Standards of Security and Quality that are to be followed during the Cyber Security Audit activity.
c) Tools and Software that may be used for the cyber security audit activity. All tools and software used by the bidder need to be licensed.
d) Any Additional and Mandatory standards of Cyber Audit regulation as required for CERT-IN Audit, should be made available and applicable by the Auditor.

2.9 Schedule of Conducting Cyber Security Audit:

Cyber Security Audit in IIG needs to be conducted Two Times for the sake of cross-checking the effective implementation of the recommendations provided during the first Audit exercise. The First Cyber Security Audit exercise needs to be commenced within 15 days of issuing the Work Order. This needs to be done at all offices Locations and Departmental end users for all types of IT systems of IIG for Cyber Security. Audit will include compliance audit as per CSAF markers along with the technical sampling audit for evidence gathering. Report of Cyber Security Gaps need to be provided by the Bidder and based on the same security Gap analysis and action would be taken at IIG end. The First Phase of the Cyber Security Audit and its Reporting need to be completed within 20 days of commencement.

a. After the end of the First Phase of the Cyber Security Audit and Reporting thereof by the bidder, IIG would take some reasonable time to study the Gaps in Cyber Security and would attempt to bridge the gaps as much as possible.

After the Gap bridging exercise by IIG has been completed, the bidder would be informed accordingly by concerned IIG representative, and thereafter the bidder should commence the Second Phase of Cyber Security Audit exercise. The time taken by IIG for bridging the Cyber Security Gap will not affect the bidder in any way as the bidder will not be held responsible for any delay in the same. The Report of the Gap Analysis of the First Phase of Cyber Security Audit should be made in such a way that it should help IIG in bridging the Gap.

b. The Second Cyber Security Audit need to be completed within 20 days after concerned IIG representative gives the go ahead for the Second Phase exercise. The purpose of the Second Phase Audit exercise would be to identify and specify whether the Security Gap Report Submitted in the First Phase exercise, still exists or the Cyber Security Gaps are plugged-in to make the IT system of IIG secure and as much foolproof as possible. The Second phase audit exercise should also result in a Detailed Report and Analysis to be submitted for the current Cyber Security status of IIG.

2.10 Reports required by IIG, during and at the end of the Cyber Security Audit exercise :

a) Audit Plan and proposed and actual progress in the Cyber Audit exercise on a weekly basis.
b) Dates and Locations of Proposed and Actual Cyber Audit exercise.
c) Summary of Cyber Audit findings, including identification tests and the results of the tests need to be shared with concerned IIG officials on a weekly basis and as and when required by IIG.
d) Analysis of vulnerabilities and issues of concern of Cyber Security needs to be reported on a weekly basis.
e) Recommendations in line with CERT-IN guidelines to make IIG's IT infrastructure CERT-IN compliant.
f) All the cyber security reports, device logs, etc. have to be shared with CERT-IN office representatives by the bidder. The purpose of the same is to keep CERT- IN informed about the perceived and possible cyber threat to IIG at present and in future.

2.11 Report Presentations Applicable to be submitted for Cyber Security Audit:

a) Summary of Cyber Security Audit findings including identification tests, tools used and results of tests performed, to be submitted to IIG on a weekly basis.
b) Analysis of the vulnerabilities and issues of concern in IIG's IT setup concerning Cyber Security to be reported on a weekly basis.
c) Recommendation for action to plug-in the Cyber Security gaps to be reported on a weekly basis.
d) Weekly progress reports to be submitted on the Cyber Security Audit activity to keep IIG informed about the status and completion of the

same.

e) Final Report of Cyber Security Audit in IIG across all locations and departments to be submitted immediately after the completion of the Audit activity.

f) Presentations on the Cyber Security Audit Report, its findings, conclusions, and recommendations for Gap Analysis and plugging, as per CERT-In guidelines, need to be made to the management of IIG as required.

2.12 The bidder will analyze all reports, logs etc. from the cyber security devices in IIG, which has to be shared with CERT-IN office representatives to keep IIG and CERT-IN informed about cyber threats at present and in future at IIG IT facilities. The bidder will identify current and future cyber threats to IIG IT facilities and propose take actions to mitigate such upcoming cyber threats and vulnerabilities so identified.

2.13 The bidder will develop and document Cyber Crisis Management Plan (CCMP) for IIG IT Facilities. The CCMP will be a separate document than the IT Security Policy of IIG and will contain strategy followed in case of a Cyber attack or threat in IIG. The CCMP will encompass all units of IIG as the cyber attack may happen at any branch location of IIG.

2.14 Details of the Authorized Contact person for the Cyber Security Audit Exercise need to be provided by the Bidder, designated for IIG, to be the single point of contact for the Bidder.

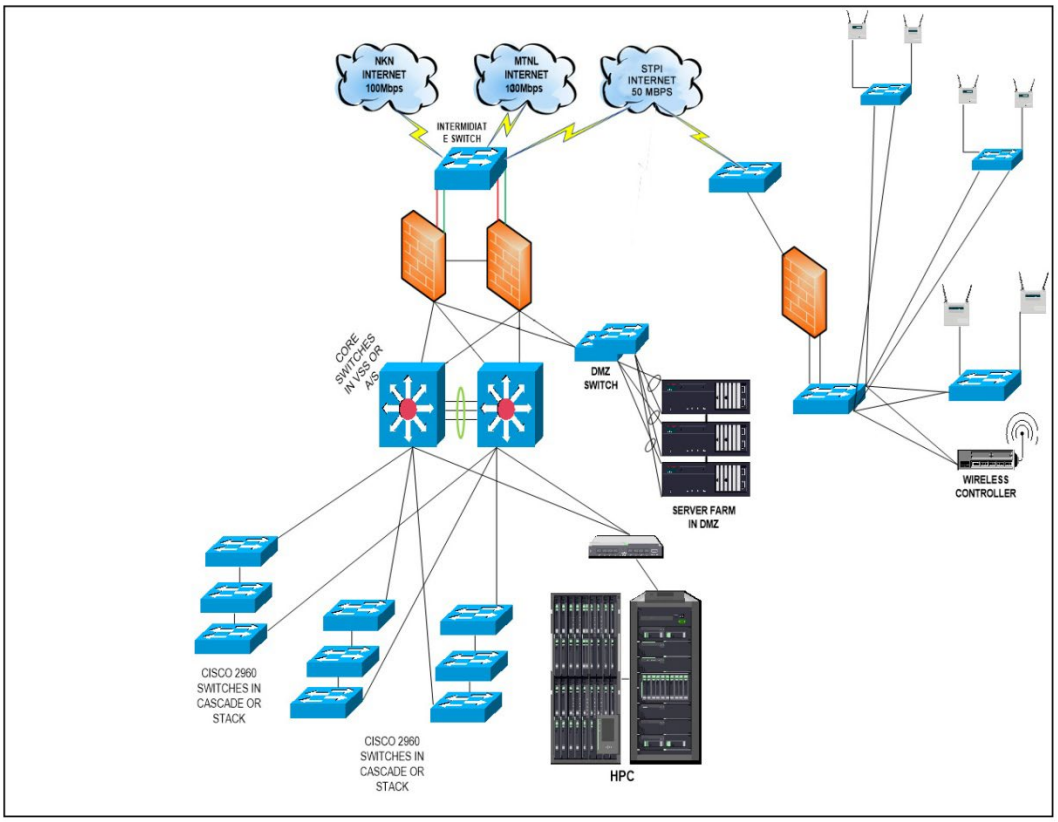
3. SCOPE OF IT INFRASTRUCTURE TO BE AUDITED:

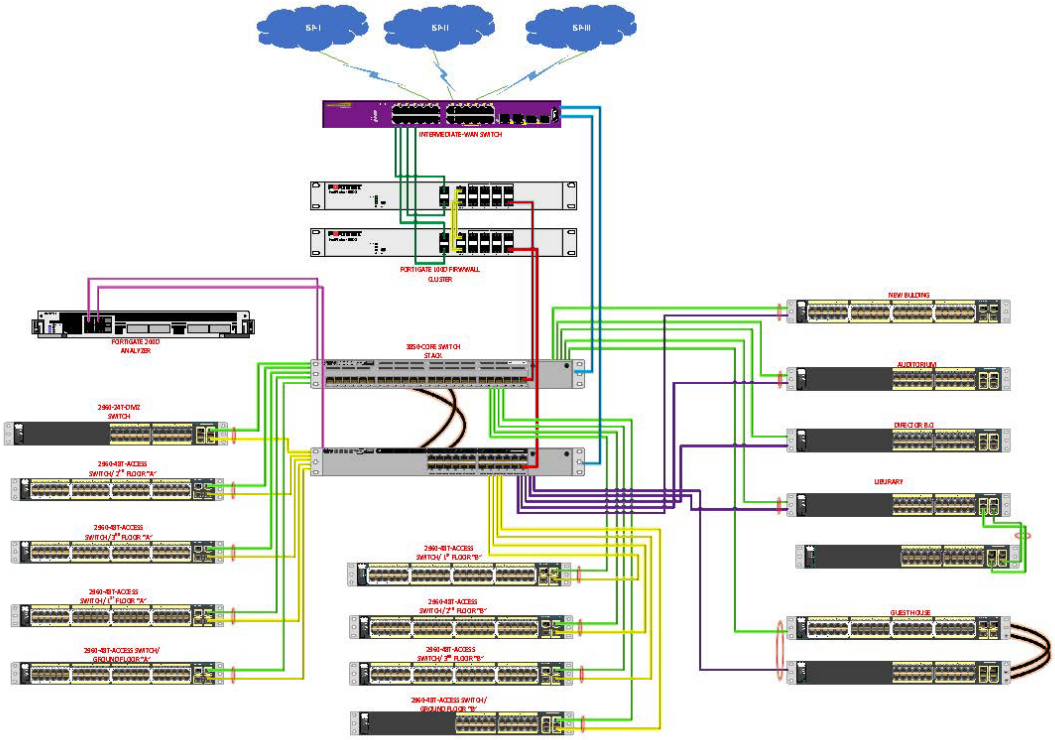
Sr. .	Parameters	**Description**
1	Organization locations	**1. IIG New Panvel campus.(IIG computer center site)** ***2.*** **IIG Colaba campus** ***3.*** **IIG regional centers (3 Nos.)** ***4.*** **IIG Observatories (9 Nos.)** ***5.*** **IIG Kolhapur Facility**
2	**Inter Connectivity tween H.Q. and remote ations IT setup**	IPSec VPN tunnel.
3	**No. of end user stations der Scope**	~150 in H.Q.; ~100 in Regional offices

5	**DR site**	At present we are hosting ERP System in IIG's Main Office. Recommendation for CCMP including DR Site is part of scope.
6	**No. of Servers**	8 rack servers + 1 chassis server with 4 blades in DC @ H.Q. 3 in Regional offices
7	**Operating systems:**	Linux / Windows/ Mac
8	**No. of Routers**	3 (H.Q.)
9	**No. of L2 Switches / ess switches**	20 + 1 core switch at H.Q.
10	**Firewall devices**	1+1 at H.Q. & 13 at regional Offices VM mode Analyzer and firewall manager
11	**No. of SAN/NAS Storage**	Fujitsu make Unified Storage – 1 No. VERITAS make Backup storage- 1 No. HPE Unified storage at NEGRL
12	**Information Security policy**	Reviewing the existing IT security policy and recommending updated policies, processes, procedures be put in place is part of scope of the audit exercise.
13	**Software Applications:**	Web enabled applications: ERP system, website with Intranet services RFID access control system Various scientific software applications, salary, library, inventory software applications
14	**Outsourced plications/servers**	1. IIG's Website with Content Management System is sted in NIC's Cloud. 2. RFID application server 3. Library management system. 4. Tally server 5. SARAL pay pack server, 6. Stores inventory software
15	**Online payment transactions**	1. ERP portal,

4. Network diagram

The IT network diagram of H.Q. (High - level) c o v e r e d under the audit is provided below:


NKN
INTERNET
100Mbps
MTNL
INTERNET
100Mbps
STPI
INTERNET
50 MBPS
INTERMIDIAT
E SWITCH
CORE
SWITCHES
IN VSS OR
A/S
DMZ
SWITCH
SERVER FARM
IN DMZ
WIRELESS
CONTROLLER
CISCO 2960
SWITCHES IN
CASCADE OR
STACK
CISCO 2960
SWITCHES IN
CASCADE OR
STACK
HPC


ISP-I
ISP-II
ISP-III
INTERMEDIATE-WAN SWITCH
FORTIGATE 3600
CLUSTER
FORTIGATE 2800
ANALYZER
3850-CORE SWITCH
STACK
2960-24T-DMZ
SWITCH
2960-48T-ACCESS
SWITCH/ 2ND FLOOR "A"
2960-48T-ACCESS
SWITCH/ 1ST FLOOR "A"
2960-48T-ACCESS SWITCH/
GROUNDFLOOR "A"
2960-48T-ACCESS
SWITCH/ 1ST FLOOR "B"
2960-48T-ACCESS
SWITCH/ 2ND FLOOR "B"
2960-48T-ACCESS
SWITCH/ 3RD FLOOR "B"
2960-48T-ACCESS SWITCH/
GROUNDFLOOR "B"
NEW BUILDING
AUDITORIUM
DIRECTOR BLG
LIBRARY
GUEST HOUSE

5. Deliverables of the Engagement - Reports and Schedule of Deliverables

5.1 Reports

Third Party Audit Firm will produce a report which should include the overall IT/Cyber security protection status considering people, process and technology. The IT/Cyber security assessment report/audit report should include expert recommendations which will make the IIG IT environment secure and sustainable. Report should include the following sections but not limited to:

1) Assessment report on the Information/IT Security Policy of IIG and provide recommendations for a roadmap to Secure IT infrastructure, including suggestions for best practices and procedures for IIG

2) Development of the Information Security/IT related Policies, as per ISMS (information security management system) which should include:

- Access control
- H/W and S/W Asset management
- Change Management
- Backup and Recovery
- IT System Operations security
- Network and Communications security
- System acquisition, development and maintenance
- IT Risk Management
- Information security incident management
- Information security aspects of business continuity management (BCM)
- Information and information related devices disposal policy
- Compliance and Regulatory requirements management
- Physical and environmental security

3) IT/Cyber Security Audit Report (along with recommendations) on IIG's IT environment, as per CERT IN guidelines which should include but not limited to:

- Access Control
- Network Security Management
- Database Management Process
- Backup & Restore Policy and Backup Plan
- Log management and monitoring policies for database, applications, router, firewall and operating systems
- Incident Management and resolution process of the incidents
- Patch update, bug fix and anti-Virus update process within IIG
- Report on Penetration Testing and Vulnerability scan

4) Drafting the Cyber Crisis Management Plan (CCMP) for IIG IT Facilities

5.2 Schedule of Deliverables

The duration of the assignment is about **50 Business days** *excluding* the time required for IIG to bridge the gaps as much as possible based on the finding of the **First IT/Cyber Security Audit** exercise.

Deliverable	**Tentative Duration / riodicity**
• Inception report including outline of IT/Cyber security requirements, audit Plan, Reporting Formats, work plan, documentation formats, dates and location of proposed IT/Cyber audit exercise	1 week
• Weekly Status Reports showing proposed vs actual progress, delays (if any), and support required, gaps identified till date etc.	Every Week
• Summary of IT/Cyber Audit findings, including identification tests and the results of the tests need to be shared with concerned IIG officials on a weekly basis and as and when required by IIG	Weekly/ As & when uested
• Prepare and submit a (i) draft Cyber security and IT audit report, (ii) draft Information/IT Security related policies (iii) Cyber Crisis Management Plan (CCMP) for IIG IT Facilities, and (iv) Expert Recommendations on the identified gaps . The audit report will have the following elements included in it: • Development of the Information Security/IT related Policies, which should include: • Access control • Asset management • Change Management • Backup and Recovery • IT System Operations security • Network and Communications security • System acquisition, development and maintenance • IT Risk management • Information security incident management • Information security aspects of business continuity management (BCM) • Information and information related devices disposal policy • Compliance and Regulatory requirements management • Physical and environmental security • Assessment Report (along with recommendations) on IIG's IT environment which should include but not limited to:	5 weeks

Deliverable	Tentative Duration eriodicity
• Access Control • Network Security Management • Database Management Process • Backup & Restore Policy and Backup Plan • Log management and monitoring policies for database, applications, router, firewall and operating systems • Incident Management and resolution process of the incidents o Patch update, bug fix and anti-Virus update process within IIG o Report on Penetration Testing and Vulnerability scan • Document Cyber Crisis Management Plan (CCMP) for IIG IT Facilities which will contain strategy followed in case of a Cyber-attack or threat in IIG. The CCPM will encompass all units of IIG as the cyber-attack may happen at any branch location of IIG	
• Share the reports and findings with IIG and relevant stakeholders only. • Presentations on the IT/Cyber Security Audit Report, its findings, conclusions, and recommendations for Gap Analysis and Plugging, as per CERT-In guidelines, need to be made to the management of IIG as required. Recommendations should also be given for implementation of NAC related activities and necessary steps to avoid uses of unauthorized software uses and installations in the office IT devices.	1 week
• Submission of final reports with required guidelines and documents	1 week

6. Audit Approach and Audit Considerations:

The independent IT/Cyber security audit will be undertaken through an evaluation of risk management by assessing total chain process of IT environment for operation integrity and operational management.

The Consultant shall sign a Confidentiality Agreement before starting the assignment, which will ensure the confidentiality and integrity of the content, data, applications, logics, structure, designs and other property of the Client, which should be shared, given access, and will be used by the Consultant during the execution of the assignment.

The Consultant should take care of the following considerations and details at the beginning of the IT/Cyber Security Audit exercise:

1. Approach and Methodology in which the IT/Cyber Security Audit activity is to be done, this will include the time frame of each activity so as to organize the IT/Cyber audit activity for better control and monitoring.
2. Standards of Security and Quality that are to be followed during the IT/Cyber Security Audit activity.
3. Tools and Software that may be used for the IT/Cyber security audit activity. All tools and software used by the bidder need to be licensed.
4. Any Additional and Mandatory standards of Cyber Audit regulation as required for

CERT-IN Audit should be made available and applicable by the Auditor.

5. All the IT/Cyber security reports, device logs, etc. have to be shared with CERT-IN office representatives by the bidder. The purpose of the same is to keep CERT-IN informed about the perceived and possible cyber threat to IIG at present and in future.

TERMS & CONDITIONS

01. General Conditions:

1. The tender should be properly sealed. Separate envelops should be used for technical and price bid and indication to their effect may please be super-scribed on the envelop.
2. The technical bid must contain an unpriced bill of material.
3. Service agreement shall be signed by the vendor as per annexure –II after awarding the contract.
4. The Price Bid Table to be filled only in the supplied format and shall be in a separate sealed cover and the guidelines and format to quote in the Price Bid is in Annexure I as given below.
5. Only cert-in empanelled agencies shall be eligible to participate in this tender.
6. Throughout the Tender document the term "CONRTRACTOR'' shall mean the successful Tenderer.
7. Institute reserves the right to accept or reject any tender offer without assigning any reason, whatsoever. The Institute is not bound to accept the lowest price offer.
8. The quoted rates should be inclusive of all taxes.
9. Quoted rates should be written both in figure and words and should be in whole rupees and followed by the word `only' written closely following the amount and not in the next line.
10. All corrections should be authenticated / signed.
11. Signature and rubber stamp of the bidder should be there in the bottom of every page of the bid.
12. Bids with blank quoted value will be rejected.
13. As mentioned in the Tender Notice **Sealed Tenders superscribed "**Limited tender Enquiry for IT security audit of IT infrastructure" **should be submitted at the Stores section, Room No.- 008, Indian Institute of Geomagnetism (IIG), Plot No. 5, Sector-18, Kalamboli Highway, New Panvel, Navi Mumbai - 410 218** up to **02.00 p.m.** On **10.10.2023** and the sealed cover for Technical Bid will be opened on **the same day at 03.00 p.m**. in the presence of attending tenderers. The date and time of opening of Price Bid will be intimated to the technically qualified bidders, tender not complying with above conditions are liable to rejections without any further reference. The tendered work if awarded is not transferable.
14. **Price Validity:** Four months from the date of opening of the price bid.
15. **Payment Schedule:** Bills for above work may be presented by the vendor after completion of work and work satisfactory certificate obtained from the In-charge Computer Section.

16. Any bid received by IIG NEW PANVEL after the deadline for submission of bids prescribed by IIG NEW PANVEL, will be summarily rejected and returned unopened to the Bidder. IIG NEW PANVEL shall not be responsible for any postal delay or non-receipt / non delivery of the documents. No further correspondence on this subject will be entertained.

Annexure - I

PRICE BID

Sr. No.	Items	Rate	GST	Total cost
01	• Access Control • Network Security Management • Database Management Process • Backup & Restore Policy and Backup Plan • Log management and monitoring policies for database, applications, router, firewall and operating systems • Incident Management and resolution process of the incidents • Patch update, bug fix and anti-Virus update process within IIG • Report on Penetration Testing and Vulnerability scan			
	Total of IT audit			
	GST			
	Grand Total			

(In words Rupees _____Only) It is certified that the information furnished above is correct.

a) We have gone through the terms and conditions stipulated in the Tender Document and confirm to abide by the same. Disagreement and solution proposed has been listed in a separate sheet and being attached with this Bid. A copy of the Tender Document with its each page signed, in token of acceptance of the Terms and Conditions, is enclosed.

b) We understand that the decision of the IIG to accept / reject "the points of disagreements and proposed solution provided by us" would be final and binding.

c) The signatory to this bid is authorized to sign such bids on behalf of the organization.

d) It is certified that our firm Contract has not been terminated/blacklisted by any other organizations.

Name and Signature of Company Representative With seal of the company.

Place:
Date

Annexure-II

Non discloser Agreement

(Between CERT-In empaneled Auditor & Auditee)

THIS NON-DISCLOSURE AGREEMENT is made on this …….. Day (date) of …… (Year)

By and between

In case of Central Government Ministry/ Departments #/State Government Departments

President of India/Governor of (name of state) acting through ……. (Name, Designation) of …….. (Name of Ministry/ Department) address …… hereinafter referred to as"Auditee" which expression shall unless repugnant to the context or meaning thereof , include its successors and assigns) of the first part.

In case of Autonomous Societies/ Not-for-profit companies/ Public sector Undertakings/Private sector

……. (Name of Company/ Society) incorporated /registered under the Companies Act, 1956/2013/ the societies registration Act, 1860 having its registered/corporate office at …… (Hereinafter referred to as"Auditee" which expression shall unless repugnant to the context or meaning thereof, includes its successors, administrators and permitted assigns) of the first part.

And

Name incorporated/registered under the…….. Name of the Act having its registered/corporate office at …… (herein referred to as "Auditor" whichexpression shall unless repugnant to the context or meaning thereof ,includes itssuccessors, assigns, administrators, liquidators and receivers)of the second part **WHEREAS**

A. Auditor is a services organization empaneled by the Indian Computer Emergency Response Team (hereinafter CERT-IN) under Department of Electronics & IT, for auditing, including vulnerability assessment and penetration testing of computer systems ,networks, computer resources & applications of various agencies or departments of the Government, critical infrastructure organizations and those in other sectors of Indian economy vide communication No……dated…….

B. Auditor as an empaneled Information Security Auditing organization has agreed to fully comply the "Guidelines for CERT-In Empaneled Information Security Auditing

Organizations, Terms & conditions of empanelment and Policy guidelines for handlingaudit related data" while conducting audits.

C. Auditee is also aware of the aforesaid Guidelines along with guidelines for Auditee Organizations published by CERT-In.

D. Both Auditor and Auditee have given their irrevocable consent to fully comply theaforesaid Guidelines and any amendments thereof without any reservations.

NOW, THEREFORE, in consideration of the foregoing and the covenants andagreements contained herein, the parties agree as follows:

1. **Definitions.** :

a) The term "Confidential Information" shall include, without limitation, allinformation and materials, furnished by either Party to the other in connectionwith Auditee products and services including information transmitted in writing, orally, visually, (e.g. video terminal display) or on magnetic media, and including all proprietary information, customer & prospect lists, trade secrets, trade namesor proposed trade names, methods and procedures of operation, business or marketing plans, licensed document know-how, ideas, concepts, designs, drawings, flow charts, diagrams, quality manuals, checklists, guidelines, processes, formulae, source code materials, specifications, programs, software packages, codes and other intellectual property relating to Auditee products and services. Results of any information security audits, tests, analysis, extracts or usages carried out by the Auditor in connection with the Auditee's productsand/or services, IT infrastructure, etc. shall also be considered Confidential Information.

b) The term "Auditee products" shall include all such products, goods, services, deliverables, which are subject to audit by the empaneled auditor under theAgreement.

2. **Protection of Confidential Information.** With respect to any Confidential Information disclosed to it or to which it has access, Auditor affirms that it shall:

a) Use the Confidential Information as necessary only in connection with scope of audit and in accordance with the terms and conditions contained herein;

b) Maintain the Confidential Information in strict confidence and take all reasonable steps to enforce the confidentiality obligations imposed hereunder, but in no event take less care with the Confidential Informationthat the parties take to protect the confidentiality of its own proprietary and confidential information and that of its other clients;

c) Not to make or retain copy of any details of products and/or services, prototypes, business or marketing plans, Client lists, Proposals developed by or originating from Auditee or any of the prospective clients of Auditee.

d) Not to make or retain copy of any details of results of any information security audits, tests,

analysis, extracts or usages carried out by the Auditor in connection with the Auditee's products and/or services, IT infrastructure, etc. without the express written consent of Auditee.

e) Not disclose or in any way assist or permit the disclosure of any Confidential Information to any other person or entity without the express written consent of the auditee ; and

f) Return to the auditee, or destroy, at auditee's discretion, any and all Confidential Information disclosed in a printed form or other permanent record, or in any other tangible form (including without limitation, all copies, notes, extracts, analyses, studies, summaries, records and reproductions thereof) immediately on (i) expiration or termination of this agreement, or (ii) the request of Auditee therefor.

g) Not to send Auditee's audit information or data and/or any such Confidential Information at any time outside India for the purpose of storage, processing, analysis or handling without the express written consent of the Auditee.

h) The auditor shall use only the best possible secure methodology to avoid confidentiality breach, while handling audit related data for the purpose of storage, processing, transit or analysis including sharing of information with auditee.

i) Not to engage or appoint any non-resident/foreigner to undertake any activity related to Information Security Audit. In case of information security audits for Government/ critical sector organization, only the man power declared to CERT-In shall be deployed to carry out such audit related activities.

j) Not to discuss with any member of public, media, press, any or any other person about the nature of arrangement entered between the Auditor and the Auditee or the nature of services to be provided by Auditor to the Auditee.

k) Make sure that all the employees and/or consultants engaged to undertake any audit on its behalf have signed the mandatory non-disclosure agreement.

3. **Onus.** Auditor shall have the burden of proving that any disclosure or use inconsistent with the terms and conditions hereof falls within any of the foregoingexceptions.

4. **Permitted disclosure of audit related information**:

The auditor may share audit information with CERT-In or similar Government entities mandated under the law as and when called upon to do so by suchagencies with prior written information to the auditee.

5. **Exceptions.** The Confidentiality obligations as enumerated in Article 2of this Agreement shall not apply in following cases:

a) Which is independently developed by Auditor or lawfully received fromanother source free of restriction and without breach of this Agreement; or

b) After it has become generally available to the public without breach of thisAgreement by Auditor; or

c) Which at the time of disclosure to Auditor was known to such party free ofrestriction and evidenced by documents in the possession of such party; or

d) Which Auditee agrees in writing is free of such restrictions.

e) Which is received from a third party not subject to the obligation ofconfidentiality with respect to such Information;

6. **Remedies.** Auditor acknowledges that any actual or threatened disclosure or use of the Confidential Information by Auditor would be a breach of this agreement and may cause immediate and irreparable harm to Auditee or to its clients;Auditor affirms that damages from such disclosure or use by it may be impossibleto measure accurately; and injury sustained by Auditee / its clients may be impossible to calculate and compensate fully. Therefore, Auditor acknowledges that in the event of such a breach, Auditee shall be entitled to specific performance by Auditor of its obligations contained in this Agreement. In addition Auditor shall compensate the Auditee for the loss or damages caused to the auditee actual and liquidated damages which may be demanded by Auditee. Liquidated damages not to exceed the Contract value. Moreover, Auditee shall be entitled to recover all costs of litigation including reasonable attorneys' feeswhich it or they may incur in connection with defending its interests and enforcement of contractual rights arising due to a breach of this agreement by Auditor. All rights and remedies hereunder are cumulative and in addition to any other rights or remedies under any applicable law, at equity, or under this Agreement, subject only to any limitations stated herein.

7. **Need to Know**. Auditor shall restrict disclosure of such Confidential Information to its employees and/or consultants with a need to know (and advise such employees and/or consultants of the obligations assumed herein), shall use the Confidential Information only for the purposes set forth in the Agreement, and shall not disclose such Confidential Information to any affiliates, subsidiaries, associates and/or third party without prior written approval of the Auditee. No information relating to auditee shall be hosted or taken outside the country in anycircumstances.

8. **Intellectual Property Rights Protection.** No license to a party, under any trademark, patent, copyright, design right, mask work protection right, or any other intellectual property right is either granted or implied by the conveying of Confidential Information to such party.

9. **No Conflict**. The parties represent and warrant that the performance of its obligations hereunder do not and shall not conflict with any other agreement or obligation of the respective parties to which they are a party or by which the respective parties are bound.

10. **Authority.** The parties represent and warrant that they have all necessary authority and power to enter into this Agreement and perform their obligations hereunder.

11. **Governing Law.** This Agreement shall be interpreted in accordance with and governed by the substantive and procedural laws of India and the parties hereby consent to the jurisdiction of Courts and/or Forums situated at < Name of the city>

12. **Entire Agreement.** This Agreement constitutes the entire understanding and agreement between the parties, and supersedes all previous or contemporaneous agreement or communications, both oral and written, representations and under standings among the parties with respect to the subject matter hereof.

13. **Amendments.** No amendment, modification and/or discharge of this Agreement shall be valid or binding on the parties unless made in writing and signed onbehalf of each of the parties by their respective duly authorized officers or representatives.

14. **Binding Agreement.** This Agreement shall be binding upon and inure to the benefit of the parties hereto and their respective successors and permitted assigns.

15. **Severability**. It is the intent of the parties that in case any one or more of the provisions contained in this Agreement shall be held to be invalid orunenforceable in any respect, such provision shall be modified to the extentnecessary to render it, as modified, valid and enforceable under applicable laws, and such invalidity or unenforceability shall not affect the other provisions of this Agreement.

16. **Waiver.** Waiver by either party of a breach of any provision of this Agreement, shall not be deemed to be waiver of any preceding or succeeding breach of the same or any other provision hereof.

17. **Survival.** Both parties agree that all of their obligations undertaken herein with respect to Confidential Information received pursuant to this Agreement shall survive till perpetuity even after expiration or termination of this Agreement.

18. **Non-solicitation.** During the term of this Agreement and thereafter for a furtherperiod of two (2) years Auditor shall not solicit or attempt to solicit Auditee's employees and/or consultants, for the purpose of hiring/contract or to proceed toconduct business similar to Auditee with any employee and/or consultant of the Auditee who has knowledge of the Confidential Information, without the prior written consent of Auditee.

19. This Agreement is governed by and shall be construed in accordance with the laws of India. In the event of dispute arises between the parties in connection withthe validity, interpretation, and implementation or alleged breach of any provision of this Agreement, the parties shall attempt to resolve the dispute in good faith by senior level negotiations. In case, any such difference or dispute is not amicably resolved within forty five (45) days of such referral for negotiations, it shall be resolved through arbitration process, wherein both the parties will appoint one arbitrator each and the third one will be appointed by the two arbitrators in accordance with the Arbitration and Conciliation Act, 1996. The venue of arbitration in India shall be (please choose the venue of dispute resolution as the city) or where the services are provided. The proceedings of arbitration shall be conducted in English language and the arbitration award shall be substantiated in writing and binding on the parties. The arbitration proceedings shall be completedwithin a period of one hundred and eighty (180) days from the date of referenceof the dispute to arbitration.

20. **Term.** This Agreement shall come into force on the date of its signing by both the parties and shall be valid up to …… year.

IN WITNESS HEREOF, and intending to be legally bound, the parties have executed thisAgreement to make it effective from the date and year first written above.

In case of auditee being Central Government Ministry/ Departments

For & on behalf of President of India
(Name and designation of authorized signatory)
……

<Name of Central Govt. Ministry/Department>

Or

In case of auditee being State Government Department

For & on behalf of Governor of ……. < State name>

……..

(Name and designation of authorized signatory)

<Name of State Department>

Or

In case of Autonomous Societies/Not-for-profit-company/Public sector undertaking ***/Private Sector #***

For <Name of organization> , <Name and designation of authorized signatory> duly authorized by rules & regulations / of <Name of society>/ vide resolution no. …. Dated ……. Of Board of Directors of ..... <Name of organization>.

(AUDITEE) **(AUDITOR)**

WITNESSES:

1.

3.