Bid Clarification Document					
Sr. No	Section No.	Page No.	Existing Clause	Clarification / Query of the Bidder	NPS Trust Response
1	General Query	-	-	We would like to understand whether a CERT-In empanelled partner is also eligible to participate in the said bid	As per the eligibility criteria of the Bid, "The bidder should be empaneled with CERT-In under the Empanelment for Information Security Auditing Organizations by Cert-In."
2	Scope of Work	3	Conduct Vulnerability Assessment / Penetration Test of the NPS Trust's IT setup, website and network, wherever necessary.	Kindly provide the Detailed Asset information and count	Detailed asset inventory and counts shall be shared with the selected bidder during audit execution. For the purpose of proposal submission, bidders may consider a following count (+- 10%): Desktop - 49 Laptop - 72 Printer - 20 Switches - 7 Firewall - 2 NAS Device-01 Access Point-03
3	Scope of Work	3	Conduct Vulnerability Assessment / Penetration Test of the NPS Trust's IT setup, website and network, wherever necessary.	Kindly provide the Detailed information of the website, Mobile applications and Digital Compliance Monitoring System	Digital Compliance Monitoring System (DCMS) hosted on Google Cloud Platform (Front end - Liferay portal and Visual Analytics - SAS VA) Website https://npstrust.org.in/ - (hosted on NICSI cloud) NPS Trust Mobile App (Android, iOS)
4	Scope of Work		5. Scope of Work ii) Review of the following areas: a.Current IT infrastructure of NPS Trust b. Information security policies c.Human resource security d. Asset management e.Access control f. Physical and environmental security g.Operations security h. Communications/Network security i. Existing/Vendor/Service provider engagements j. Information security incident management k.Information security aspects of business continuity management l. Data security for alignment with the Digital Personal Data Protection Act, 2023 h. Review of NPS Trust existing IT and cyber security policies and Procedures and recommend suitable	a) What kind of assessment needs to be conducted in "Current IT infrastructure of NPS Trust" b) Please list all current policies/standards/SOPs and count. c) What kind of assessment needs to be conducted in "Human resource security" d) Please confirm existence of a centralized Asset/Register with owners, classification (CIA), location, and lifecycle details, and whether cloud assets (IaaS/PaaS/SaaS) are included.	a) Conduct Vulnerability Assessment / Penetration Test of the NPS Trust's IT setup, website and network, wherever necessary. Based on the findings, suggest corrective actions / redressals / mitigation of risks / non-conformities and provide a comprehensive roadmap to counter the assessed / potential vulnerabilities. b) NPS Trust Policy has policy such as Password Policy, Information Technology Policy, IT Asset Management Policy, Cloud Adoption Policy, Email Policy, Information and Cyber Security Policy and has SOP such as IT Asset Management SOP. Policy are to reviewed and changes to be suggested, if any. c) The outcome of the assessment shall include risk findings and recommendations to strengthen human-centric security controls as part of the overall cyber security audit. d)NPS Trust maintains a centralized IT Asset Register covering its IT infrastructure in line with the NPS Trust's IT Asset Management.

4	Scope of Work		5. Scope of Work ii) Review of the following areas: a.Current IT infrastructure of NPS Trust b. Information security policies c.Human resource security d. Asset management e.Access control f. Physical and environmental security g.Operations security h. Communications/Network security i. Existing/Vendor/Service provider engagements j. Information security incident management k.Information security aspects of business continuity management l. Data security for alignment with the Digital Personal Data Protection Act, 2023 h. Review of NPS Trust existing IT and cyber security policies and Procedures and recommend suitable	e) What IAM model is in place (RBAC/ABAC), and do privileged accounts follow segregation of duties, MFA, PAM, and periodic access reviews requirements? f) Which sites (offices, server/communication rooms, DC/DR facilities) are in scope for physical security review and what evidence (access logs, CCTV, visitor logs) can be provided? g) Do you expect a logging & monitoring assessment (SIEM/SOC coverage, retention, alerting, use cases) across on-prem, NIC, and cloud?	e) Existing controls are in place. The same may be reviewed during audit stage. f) The physical security review under this RFP shall cover the office premises of NPS Trust, including the following locations: B-302, Tower-B, World Trade Centre, Nauroji Nagar, New Delhi IFCI Tower, Nehru Place, New Delhi The selected auditor shall be provided access to appropriate evidence. The extent and form of evidence shall be subject to security, confidentiality, and operational considerations of NPS Trust and its service providers and will be facilitated during the audit execution phase. g) The scope of this RFP is to conduct a comprehensive cyber security audit, including identification of gaps and recommendation of suitable controls, as applicable. Accordingly, the selected auditor shall review the existing logging and monitoring mechanisms, if any, and assess the adequacy of such controls in line with CERT-In Cyber Security Audit Baseline Requirements and ISO 27001 / ISMS controls.
4	Scope of Work		5. Scope of Work ii) Review of the following areas: a.Current IT infrastructure of NPS Trust b. Information security policies c.Human resource security d. Asset management e.Access control f. Physical and environmental security g.Operations security h. Communications/Network security i. Existing/Vendor/Service provider engagements j. Information security incident management k.Information security aspects of business continuity management l. Data security for alignment with the Digital Personal Data Protection Act, 2023 h. Review of NPS Trust existing IT and cyber security policies and Procedures and recommend suitable	h) Please confirm availability of high-level network diagrams and security device inventories (firewalls, IDS/IPS, WAF, VPN). i) What kind of assessment needs to be conducted in "Existing/Vendor/Service provider engagements" j) Is there an existing Incident Response Plan and playbooks (ransomware, data breach, DDoS)? k) Please confirm if you have documented BCP for critical services. l) Kindly specify personal data categories processed (subscriber, employee, vendor), processing purposes, cross-border flows, and sharing with processors, to map lawful bases (consent/legitimate uses)	h) As part of the cyber security audit envisaged under Clause 5 (Scope of Work) of the RFP, the selected auditor shall be facilitated with relevant high-level network architecture documentation and security infrastructure information, where available, for the purpose of assessment. i)Vendor assessment shall be limited to review of governance, and oversight controls from NPS Trust's perspective and shall not include direct audit of vendor systems. j)Incident response preparedness shall be assessed during the audit and suitable frameworks and playbooks, wherever required, shall be recommended as part of the audit report. k)Business continuity preparedness shall be assessed during the audit and suitable recommendations shall be provided as part of the audit deliverables. l)NPS Trust does not store subscriber personal data.This is being done by central recordkeeping agencies the details of which can be referred from NPS Trust website https://npstrust.org.in/nps-architecture
			Section 2(i) : NPS Trust Website and Mobile App	Are separate privacy notices and consent mechanisms implemented within the app? How is user data stored and secured (on device, cloud, or backend servers)?	NPS Trust does not store subscriber personal data.This is being done by central recordkeeping agencies the details of which can be referred from NPS Trust website https://npstrust.org.in/nps-architecture Website https://npstrust.org.in/ - (hosted on NICSI cloud) NPS Trust Mobile App (Android, iOS)
			Section 2 (ii) Digital Compliance Monitoring System (DCMS)	For the DCMS hosted on Google Cloud, please confirm which regions/data centers are used and whether personal data is stored or processed in this application. Is there a defined data retention and deletion policy for compliance data?	DCMS is hosted on a google cloud environment which is MEITY empanalled and does not process subscriber personal data. Cloud hosting, data handling, retention, and deletion practices shall be reviewed during the audit for compliance with applicable policies and laws.

			Section 2 (iii) E-mail and e-office	Please clarify whether NIC's e-mail/e-office services involve storage or processing of personal data of subscribers/employees. Additionally, does NPS Trust (through NIC) have a defined data deletion mechanism in place.	NPS Trust has availed e-mail and e-office services provided by NIC for official communication and electronic file management . The data management is being done on NICSI managed platform.
			2(iv) Other IT infrastructure:	Please confirm whether leased line, Wi-Fi, firewall, and NAS devices are managed internally or through third-party vendors	Network and security devices are managed through a mix of in-house oversight and third-party support, including an AMC service provider and connectivity providers. Detailed arrangements shall be reviewed during the audit.
			5(ii) (l) Data security for alignment with the Digital Personal Data Protection Act, 2023	• Has NPS Trust appointed a Data Protection Officer (DPO) or equivalent role? • Is there a defined process for handling data subject rights requests (access, correction, deletion, consent withdrawal)? • Are there existing mechanisms for data breach notification to the Data Protection Board of India? • Is there a centralized consent management mechanism in place for collecting, verifying, and revoking consent? • Are formal privacy policies documented and implemented?	DPDP governance requirements shall be assessed during the audit and recommendations shall be provided.
			5. Scope of Work iii) Conduct Vulnerability Assessment / Penetration Test of the NPS Trust's IT setup, website and network, wherever necessary. Based on the findings, suggest corrective actions / redressals / mitigation of risks / non conformities and provide a comprehensive roadmap to counter the assessed / potential vulnerabilities	i) We request NPS Trust to clarify that this activity includes the application black, grey or white box security testing. Also, please specify the expected number of applications to be covered under the activity (internal/external) ii) Also, we request NPS Trust to clarify the count of all servers and network devices to be be covered under assessment (internal/external) iii) Are there any specific policy-driven restrictions on scanning, penetration testing, or log access that we should be aware of?	The application security testing approach may be in line with Cyber security audit Baseline Requirements.Also details of applications (internal) have already been shared in the RFP.
			5. Scope of Work iv) Submit detailed audit report containing security gap analysis based on which action would be taken by NPS Trust	i) Is there a prescribed format or template for the security gap analysis report that bidders must follow? Also any specific framework that we need to follow?	No fixed report template is prescribed. The auditor shall follow industry-accepted frameworks and submit reports in a format mutually agreed with NPS Trust.
			5. Scope of Work v) Conduct post audit compliance verification subsequently to ensure remediation action taken against all the observation points/gaps and submit a detailed report and analysis on the latest cyber security status of NPS Trust	i) How many rounds of compliance verification are included in the scope — one retest or multiple iterations?	There shall be only one instance of re-assessment. The entire process of audit should be completed within a perioid notexceeding 60 days.
			iii. Conduct post audit compliance verification subsequently to ensure remediation action taken against all the observation points/gaps and submit a detailed report and analysis on the mitigation measures undertaken by NPS Trust and provide the final certification on safe for hosting within 7 days from the date of receipt of reply from NPS Trust.	As the contract is for 60 days only and remediation/fix may take month(s). Post audit compliance verification may not be feasible it is suggestion to extend the contract period. Can we provide the complication certificate instead of safe to host, as zero-day vulnerability will not be covered.	The terms of RFP shall remain same.
			5. Scope of Work vi) Certify that the infrastructure / web applications as "Safe for Hosting" and provide the final certification	Please clarify the exact standard or guideline under which the "Safe for Hosting" certification must be issued (e.g., CERT-In, NSCS Baseline Security Requirements, ISO 27001 Annex A controls, OWASP ASVS).	"Safe for Hosting" shall be issued by a CERT-In empanelled auditor based on a risk-based assessment aligned with applicable government guidelines and industry best practices.

			5. Scope of Work viii) Review of NPS Trust existing IT and cyber security policies and Procedures and recommend suitable measures for adopting best practices in line with ISO 27001 and ISMS readiness.	i) Please list existing IT and cybersecurity guideline/policies, procedures, and guidelines currently in force at NPS Trust.	The policies/SOPs/procedures may be reviewed and suggestions may be provided.
			Annexure I : Bid Format	Can you list the name(s) and number(s) of audits/assessments.	NPS Trust has undertaken periodic IT and security-related assessments. Details of prior audits shall be shared with the selected auditor during engagement, as appropriate.
				E-Mail and E-Office: Please confirm the exact activities expected to be performed under E-Mail and E-Office. If VAPT is required, kindly confirm whether necessary permissions will be provided by NIC. If only a configuration audit is needed, please note that no benchmark is currently available, which may limit our ability to perform the audit without defined standards.	NIC e-Mail and e-Office shall be covered through governance and usage-level review only; intrusive testing or VAPT of NIC infrastructure is not in scope as they are being managed by NIC and we are availing their service.
				IT Infrastructure: Requesting detailed information regarding the count of laptop and desktop. Do we need to perform VAPT for laptops/desktops? If yes, please confirm whether these devices are located at a single site or across multiple locations. In case of multiple locations, please confirm if the systems are connected through VPN.	Endpoint devices shall be covered through configuration and control review from cyber security point of view only; A sample of desktop and laptop may be taken for VAPT, if required as per cyber security audit baseline requirements.