# Request for Proposal for providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode):

**Published by:**

**NATIONAL POWER TRAINING INSTITUTE,**

**Sector-33, Faridabad-121003 HARYANA**

# Table of Contents

## Letter of Invitation

This document is for Request for Proposal for providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode).

Interested bidders may download the RFP document from the website (https://gem.gov.in/).The submission of the RFP document must be accompanied with the payment of tender processing fee of Rs. 5900/- (Rupees Five Thousand Nine Hundred only) and EMD of 3,00,000/- (Rupees Three Lakh only).
Last Date for Submission of Proposal: 16.05.2024 by 04:00 PM Interested bidders may contact Sh. Mukesh Kumar, Deputy Director, NPTI for any clarification.
Email: mukesh.npti@gov.in

**(E-Tendering Mode Only)**
**NATIONAL POWER TRAINING INSTITUTE**
**(Under ministry of Power, Govt. of India) NPTI Complex, Sector-33, Faridabad-121003**
**DOMESTIC COMPETITIVE BIDDING**
**(Through online open Tenders Through GEM)**

**TENDER NO. NPTI/HQ/Consultancy/RFP-2024/380 DATED: 25-04-2024**

## SECTION-1 NOTICE INVITING TENDER
### Critical Data Sheet

| | |
|---|---|
| Name of Work | Request for Proposal for providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode) |
| Tender Fees | Rs.5900/- |
| Earnest Money Deposit | Rs.3,00,000/- (Through NEFT/RTGS)<br>Bidders not paying EMD before tender submission end date and time will be summarily rejected. |
| Uploading/Publishing date of RFP on website | 25-04-2024 |
| Document Download Start date & Time | 25-04-2024, 03.00 PM |
| RFE Submission Start date & Time (through GEM Portal) | 25-04-2024, 03.00 PM |
| Pre-Bid Meeting | 01-05-2024, 03.00 PM, online link will be shared on the Portal |
| Last Date of submission of RFP | 16-05-2024, 04.00 PM |
| Time and Date of Opening of RFP | 16-05-2024, 04.30 PM |
| The tender documents can be downloaded from | https://gem.gov.in<br>www.npti.gov.in |
| Tender documents can be submitted at online | https://gem.gov.in |
| Contact Person | Sh.Mukesh Kumar<br>Dy. Director, NPTI Faridabad,<br>Ph-9810704004, Emaul-mukesh.npti@gov.in |

## Definitions

Following definitions will prevail throughout this RFP, unless in consistent with the subject matter or content.

- “RFP” means Request for Proposal for providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode).
- “Bidder”/ “Service Provider”/ “Vendor”/ “Tenderer/ Agency” means respondent to this RFE document
- “Selected Bidder” means the applicant who is declared successful after completion of the entire process of evaluation as defined under this RFE.
- “NEFT” means National Electronic Fund Transfer
- “RTGS” means Real Time Gross Settlement
- “GST” means Goods and Service Tax

## 1. About NPTI

National Power Training Institute (NPTI), an ISO 9001 & ISO 14001 organization under Ministry of Power, Government of India is a National Apex body for Training and Human Resources Development in Power Sector with its Corporate Office at Faridabad. NPTI had been providing its dedicated service for more than five decades.
NPTI has trained over 4,50,000 Power Professionals in regular Programs over the last 5 decades. NPTI is the world's leading integrated power training institute. NPTI is the only institute of its kind in the world with a wide geographical spread and covering a wide gamut of academic and training programs in Power Sector. NPTI's committed faculty is providing excellent training in the Power Sector, which is the most important sector among various infrastructure sectors. Thus, the training being provided by NPTI is having a cascading effect in the growth of GDP and economy of the country.
NPTI operates on an all-India basis through its eleven Institutes in different zones of the country as per details below:

**Northern Region**

- NPTI Corporate Office, Faridabad
- NPTI (Northern Region) Badarpur, New Delhi
- NPTI (Hydro Power Training Centre), Nangal

**Southern Region**

- NPTI (Power System Training Institute), Bengaluru
- NPTI (Hot Line Training Centre), Bengaluru
- NPTI (Southern Region), Neyveli
- NPTI, Alappuzha

**Eastern & North Eastern Region**

- NPTI (Eastern Region), Durgapur
- NPTI (North Eastern Region), Guwahati

**Western Region**

- NPTI (Western Region), Nagpur
- NPTI, Shivpuri

## 2. Cyber Security in Power Sector

Cyber intrusion attempts and Cyber-attacks in any critical sector are carried out with a malicious intent. In Power Sector it’s either to compromise the Power Supply System or to render the grid operation in-secure. Any such compromise may result in maloperations of equipment’s, equipment damages or even in a cascading grid brownout/blackout. Air gap myth between IT and OT Systems now diminishing. The artificial air gap created by deploying firewalls between any IT and OT System can be bypassed by any insider or an outsider.

Cyber-attacks are staged through malicious intent & techniques of Initial Access, Execution, Persistence, Privilege Escalation, defence Evasion, Command and Control, Ex- filtration. Unauthorized access inside the system through privilege escalation, the control of IT network and operations of OT systems can be taken remotely with adverse intent. The gain of sensitive operational data through such intrusions may help the Nation/State sponsored or non-sponsored adversaries and cyber attackers to design more threatening and advanced cyber-attacks.

### 2.1 Background

Central Electricity Authority (CEA) is mandated to prepare 'Guidelines on Cyber Security' in Power Sector under provision of regulation (10) of the Central Electricity Authority (Technical Standards for Connectivity to the Grid) (Amendment) Regulations, 2019. Guidelines on Cyber Security in Power Sector incorporating the cardinal principles have been prepared by CEA. In compliance to the provision of the above regulations, CEA (Cyber Security in Power Sector) Guidelines, 2021 are issued for compliance by all entities.

## 3. Scope of Work

To provide the experts/resource personnel to conduct the following Types of and Level of Training programs:

i. Basic Level Cyber Security Training and Certification Program (1 week) Offline Theory/Hands-on

ii. Basic Level Cyber Security Training and Certification Program Online (2 – weeks) (One week Theory and One week Hands-on)

iii. Intermediate Level Cyber Security Training and Certification Program (2 Weeks) * Hybrid Mode (Online/Offline)

iv. Advanced Level Cyber Security Training and Certification Program (2 Weeks) * Hybrid Mode (Online/Offline)

v. Cyber Security Training Program as desired by the industry on mutual consent basis.

* Hybrid Mode: The Agency has to conduct the sessions in Physical Mode with the provision of online access to the participants.

### 3.1. Terms & Condition

i. To conduct training as per course content for serial no. 1-4 as above, as per appendix 1 attached / approved course curriculum amended from time to time.

ii. To prepare and provide comprehensive training material on the subject in soft copies to all the participants.

iii. To arrange software / equipment / simulation tools used in the training environment for conducting the training courses with open source/legally sourced software.

iv. To create virtual Lab for conducting the Hands-on Training in online/offline mode.

v. To chalk out & submit the training schedule / time table in advance before commencement of the courses in consultation with NPTI.

vi. To conduct theory class and lab as per respective course curriculum.

vii. To prepare a question bank, conduct regular assessment test and submit the evaluation results to NPTI.

viii. To validate the list of nomination through online registration form, to create pre/post assessment template/feedback forms for the participants and submit the filled forms (E-copy) at the end of each program.

ix. To coordinate with NPTI for smooth conduction of training.

x. The agency/trainer should have fair knowledge of relevant international standards such as IS/ISO/IEC 17021, IS/ISO/IEC 27001, IS/ISO/IEC 27019, IEC 62443, ISO 31000 and any other applicable standards.

xi. The trainer should have adequate knowledge of subject areas defined in the course curriculum and fulfill all the learning objectives.

xii. The instructors/faculties shall have relevant industry experience and certifications.

xiii. To create engaging and interactive content, including simulations, case studies, and practical exercises to reinforce theoretical concepts.

xiv. Implement a secure online platform for training, incorporating encryption and access controls to safeguard sensitive information shared during the program.

xv. Integrate real-world scenarios and practical examples to enhance the participants' ability to apply theoretical knowledge in practical situations.

xvi. Conduct regular assessments & quizzes, both theory & hands-on.

xvii. Continuously update the training program to reflect the latest cybersecurity threats, technologies, and best practices commensurate with the amended guidelines.

xviii. Provide access to supplementary resources, such as reference materials, webinars, and forums, to support ongoing learning beyond the formal training sessions.

xix. Accommodate different learning styles and paces by offering flexible learning paths and options for participants to revisit specific modules based on their needs.

xx. Implement monitoring tools to track participants' progress and generate comprehensive reports for both individuals and organizational stakeholders.

xxi. Ensure the training program complies with relevant data protection and privacy regulations, reinforcing the importance of ethical conduct and confidentiality in cybersecurity practices.

xxii. The Agency shall ensure that no data related to the participants shall be used/shared/misused for any purpose other than the training conducted at NPTI. If any such instances come to the notice of NPTI, penalty @ Rupees Ten Lakh will be imposed for the first instance. Any subsequent incident will attract double the penalty amount followed by blacklisting of the Agency.

xxiii. Virtual lab will be designed as per the course curriculum on windows platform & hosted on MEITY empaneled cloud, for the programs

xxiv. Virtual lab should cater to demonstrate the cyber-attacks like phishing, DDos attack etc. And the virtual lab should have all the manual tools described in the course curriculum for the Hands-On training of the attack.

xxv. For hands-on training the lab shall be open for extra one week.

xxvi. The result should be compiled with the final status in percentage and grades providing the information whether the participant has successfully completed or has participated.

xxvii. The final result with complete details of the participants must be verified, signed and stamped by the empaneled agency and submitted to NPTI

xxviii. Compilation of Result with Marks/Grade and Fail Pass participated successfully completed

xxix. Provision shall be made for annual re-examination/re-test as per client’s requirement and special session shall be arranged for those participants who have not qualified the examination.

xxx. The agency should have LMS with dashboard with integrated virtual lab in the domain of cyber security for complete Training Program in all aspects.

xxxi. The agency must have its own cloud hosted lab for imparting various levels of training programs.

xxxii. Implement secure user authentication mechanisms to ensure only authorized participants list provided by NPTI to access the training program.

xxxiii. Enable real-time tracking of participant attendance, capturing logins, logouts, and participation in live sessions or activities.

xxxiv. Ensure accurate time stamping of attendance records, synchronizing with a reliable time source to prevent manipulation.

xxxv. Regularly back up attendance and other requisite records in a secure and encrypted manner to prevent data loss and facilitate recovery in case of system failures.

xxxvi. The Agency should provide the recorded sessions of all the training programs.

## 4. The Duration of the Empanelment

a) The Empanelment would be valid for three Years.

b) An Empanelment agreement shall come into force from the date on which the letter of intent is dispatched to the Bidder.

## 5. Language of the Bids

This bid should be submitted in English language only. Bills and compliance report should also be submitted in English language only. If any supporting documents submitted are in any language other than English, translation of the same in the English language is to be duly attested by the bidder and submitted. Any image files submitted in the bid document must be clear and have visible details; otherwise, it will not be accepted.

## 6. Queries

i. The Bidders must ensure that their queries (if any) are submitted in writing before/post the Pre- Bid meeting by 01.05.2024 at the mail-id: mukesh.npti@gov.in

ii. All the queries should necessarily be submitted in the following format in Excel:

| **Sr. No.** | **RFP Document Reference(s)** | | | | |
|---|---|---|---|---|---|
| | **Page No.** | **Section No.** | **Section Name** | **Section Details** | **Query by Bidder with proposed amendment/changes** |
| | | | | | |
| | | | | | |

## 7. Eligibility Criteria

i. The agency should be registered in India.

ii. The bidder should either be a company registered in India as per Company Act 1956/ 2013 or a partnership firm registered under partnership act 1932/ a Limited Liability Partnership under the Limited Liability Partnership Act 2008 or an organization registered under

Societies Act or an academic institution duly registered under applicable law.

iii. The agency should be in existence for last 3 years from the date of issuance of this RFP

iv. Joint Venture of organizations is not allowed to bid

v. If proceedings for suspension or cancellation of registration or for blacklisting or for termination of contract due to poor performance by the Consultants/Organizations/Agency's has been started by any Department / Undertaking of Government of Government/Semi Government/PSU in India before the issue date of this EOI and the same is subsisting on the last date of submission of bid, the bidder cannot participate in bidding process. A self-declaration regarding blacklist/debarment by State Govt./Central Govt./PSU in India has to be submitted.

vi. Average turnover since last three year (2020-21 to 2022-23) should be more than Rs 2.00 Crores. Annual turnover should be duly certified by Chartered Accountant with UDIN Number.

vii. It would be desirable to have academic tie ups of delivering quality cyber security education to eminent government institutions, e.g. IITs, IIMs, & other government institutions.

viii. The Agency must have its own Learning Management System with integrated virtual labs in the domain of cyber security.

ix. The Agency must have its own cloud hosted labs for imparting various levels of cyber security training.

x. It is desirable that the agency should have its own cyber range for conduction of attack defence simulation.

xi. It is also desirable that the bidder should have the ability to train using its own threat intelligence platform e.g. honey pots, decoys etc.

xii. Reference check to be arranged from any eminent institution confirming the training competence of the company

## 8. Evaluation

The evaluation of the bidders will be done as below:

a) They must possess the eligibility defined under clause 7 of this RFP document.

b) The evaluation will be done based on the document submitted.

c) The qualifying score will be 75 marks out of 100. Agency that qualifies in the evaluation will be ranked accordingly and they only shall be considered for opening of financial bid.

d) This ranking will be used once again at the time of first allotment of the trainees to the bidders where the agency will be allocated the training based on their ranking. The bigger batches will be allocated to the agency having higher ranks and vice a versa.

**Evaluation criteria:**

| S.No | Parameter | Maximum Marks |
|---|---|---|
| 1 | The bidder should have handled at least 5 assignments/ Services related to cyber security trainings/awareness sessions and content development to Training /Academic Govt PSU institutions in India during last three financial years [i.e.2022-23,2021-22 and 2020-21].<br>• more than 12 assignments/services 25 marks<br>• 8 to12 assignments/services 20 marks<br>• 5 to 7 assignments/services -10 marks<br>• 3 to 4 assignments/services -5 marks | 25 |
| 2 | The bidder should have experience in handling training in at least 10 of the following areas:<br>Introduction to Cyber Security, IT/ OT Cyber Risk Management, Case Studies on Recent Cyber Security Breaches, Case Studies on Cyber Laws, Cyber Security Framework, Data Protection and Privacy, Vulnerability Management, Encryption and Cryptography, Third-Party Risk Management, Security Auditing, Network Security, Endpoint Security, Web Application Security, Threat Hunting and Intelligence, Wireless Security, Physical Security, ISO Certification Trainings, NIST Framework Guidelines, Cyber Security – Regulatory Measures, Cyber Fraud Investigation, Cyber Security Governance, ATM, SWIFT, Internet Banking, Mobile Banking, Payment Gateway.<br>• Greater than 20 areas/domain - 25 marks<br>• From 16 to 20 areas/domain - 20 marks<br>• From 11 to 16 areas/domain – 15 marks<br>• From 6 to 10 areas/domain – 10 marks<br>• From 1 to 5 areas/domain – 5 marks | 25 |
| 3 | The bidder shall have at least 10 full time permanent employees working with the entity as on date of bid submission.<br>Out of these at least 5 [Five] full time technical permanent employees shall meet the following criteria:<br>➢ They shall be M.Tech/Ph.D with 10 or more than 10 Years experience And they may possess at least any one of following certification/experience<br>▪ CISM Certified Information Security Manager<br>▪ CISA: Certified Information Security Auditor<br>▪ LPT: Licensed Penetration Tester<br>▪ CEH: Certified Ethical Hacker/<br>▪ CISA: Certified Network Associate/<br>▪ CISSP: Certified Information System Security Professionals/<br>▪ Certified ISO 27001 Lead Auditor Certification/ | 20 |

| | | |
|---|---|---|
| | ▪ Experience in Infrastructure deployment & Governance including securing IT/OT/IOT based systems<br>✓ Greater than 20 employees 20 marks<br>✓ From 10-14 employees 15 marks<br>✓ From 6-9 employees 10 marks<br>✓ From 3-5 employees 5 marks<br>✓ Less than 3 employees Zero marks | |
| 4 | Number of Years of Existence/Establishment in Information Security/Cyber Security related activities. Evidence of the assignments to been closed as a proof of Experience.<br>• Greater than 5 years- 15 marks<br>• 3 to 5 years- 10 marks<br>• 1-3 years- 5 Marks | 15 |
| 5 | Presence in at least one of the following cities- Delhi, Gurgram, Noida Gaziabad, Faridabad 12M<br>Head/Main office in Delhi, Gurgaon Gaziabad, Noida,Faridabad @□10 Marks<br>1[One] mark for every additional city/location[Max.15 Marks] | 15 |

## 9. Payments Terms

i. No advance payment will be released for the training programs.

ii. The bidder shall submit their invoice quarterly and NPTI, after receipt of the invoice duly complete in all respect from bidders shall release the payment within 15 days.

iii. The payments shall be processed upon completion of training program only and duly signed results submitted to NPTI.

iv. The payment for each training batch shall be released for actual numbers of successful participants.

v. There will be no liability of any taxes etc. of any nature whatsoever on NPTI and all statutory obligations due to these transactions shall be borne by the agencies.

## 10. Instruction to Bidders

### Procedure for Submission of Bids

a) The bids would be submitted through GEM portal only. The payment for EMD/Tender Fee to be done online and receipt be annexed in their bid towards proof. The bids submitted through any other electronic medium shall not be considered.

b) These bids would be valid for a period of 180 days from the date of opening.

c) NPTI will not be responsible for any delay on the part of the bidder in obtaining the terms and conditions of the tender notice or submission of the bids online beyond the bid submission end date & time as mentioned in schedule of RFP.
d) If any clarification is required, the agency may send the queries through email to NPTI within one week of publishing of e-Tenders.
e) Bids not submitted as per the specified format and nomenclature may be out rightly rejected.
f) Ambiguous/Incomplete/Illegible bids may be out rightly rejected.
g) NPTI at any time during the course of evaluation of the bids, may seek verbal or written clarifications from the bidders, which may be in the form of product demonstration, presentation, undertaking, declaration, reports, datasheets, etc., and if NPTI finds the information in the submitted bids to be insufficient/ambiguous/deviant or of any such nature that hinders NPTI from arriving at a clear decision, It will entirely be at NPTI discretion whether to seek clarifications or not, and what clarifications to seek, or take any other action as per the guidelines provided in the tender.
h) All the bids' documents must be duly signed and stamped by the authorized signatory of the company. In case the bid is signed by anyone other than the authorized signatory of the company, the bidder must enclose authorization letter from HR department of the company for the officer, who signed the bid. All pages of the bids must be sequentially numbered and an Index should be placed at starting of the bids clearly mentioning the referred documents as per eligibility criteria and Selection criteria.

## 11. Tender Processing Fees

The bidders should deposit a non-refundable bid processing fees of Rs.5900/- (Rupees Five Thousand and Nine Hundred Only) through NEFT/RTGS. Transaction reference copy should be enclosed in bid document and submit the same on or before the closing time. Bids received without processing fee will be rejected. The RFE document can be downloaded from the website-www.gem.gov.in.

Tender processing Fees to be paid through NEFT/RTGS in account mentioned below:

| | |
|---|---|
| Beneficiary Name | : National Power Training Institute |
| Account Number | : 10724879119 |
| IFSC code | : SBIN0003245 |
| Type of Account | : Current Account |

## 12. Earnest Money Deposit

An EMD of Rs. 3,00,000 (Rupees Three Lakh Rupees only) is to be deposited by the bidder through NEFT/RTGS. Transaction reference copy should be enclosed in bid document and submit the same on or before the closing time. Bids received without EMD will be rejected. MSMEs registered for providing Training are exempted to pay the EMD.

i. EMD will not carry any interest.

ii. EMD will be forfeited if:

   a. A bidder withdraws from the tender, or amends its tender, or impairs, or derogates from the tender in any respect within the validity period of his tender

   b. A bidder having been notified of the acceptance of his tender by NPTI during the period of its validity

   c. Fails to furnish the performance security within the specified period for the due performance of the contract, or Fails or refuses to accept / execute the contract

   d. EMD furnished by the unsuccessful bidders would be returned without any interest on completion of the tender process, i.e., after award of the contract. EMD of the successful bidder would be returned without any interest after receipt of the Performance Security as per the terms of the bids received without EMD will be rejected

EMD to be paid through NEFT/RTGS in account mentioned below:

| | |
|---|---|
| Beneficiary Name | : National Power Training Institute |
| Account Number | : 10724879119 |
| IFSC code | : SBIN0003245 |
| Type of Account | : Current Account |

## 13. Performance Security

The successful bidder would be required to deposit an amount equivalent to Rs.7,50,000/- (Rupees Seven Lakh and Fifty Thousand only). This may be furnished by the way of Banker’s Cheque or Demand Draft (drawn in favour of “National Power Training Institute”, payable at Faridabad) or Bank guarantee in favour of “National Power Training Institute” payable at Faridabad. Performance security shall remain valid for a period of ninety days (90 days) beyond the date of the completion of all contractual obligations of the successful bidder. The performance security will be returned after adjusting for penalties on account of deficiencies, if any, in the performance of the contract.

## 14. Authorized Signatory

The "Agency as used in the Proposal shall mean the one who has signed the Bid document forms. The authorized signatory should be the duly Authorized Representative of the Agency, for which a certificate of authority will be submitted. All certificates and documents (including any clarifications sought

and any subsequent correspondences) received hereby, shall, as far as possible, be furnished and signed by the Authorized Representative.
The power or authorization, or any other document consisting of adequate proof of the ability of the signatory to bind the agency shall be annexed to the Proposal. NPTI may reject outright any Proposal not supported by adequate proof of the signatory's authority.

## 15. Amendment of RFP

At any time prior to the last date for receipt of Proposals, NPTI may, for any reason, whether at its own initiative or in response to a clarification requested by a prospective Agency, modify the RFP by an amendment. In order to provide prospective Agency reasonable time in which to take the amendment into account in preparing their Proposals, NPTI may, at its discretion, extend the last date for the receipt of Proposals and/or make other changes in the requirements set out in the Invitation for Proposals.

## 16. Document Comprising Proposal

The Proposal prepared by the bidder shall comprise of the following components: Form 1: Letter Proforma
Form 2: Minimum Eligibility
Form 3: Prior Experience (Project completion certificates conforming the experience to be attached as relevant and work-orders)
Form 4: CVs of proposed faculty members
Form 5: Declaration Letter
Form 6: Work plan for the project with timelines
Form 7: Letter of Undertaking
Form 8: Financial proposal
-Bid processing fee of Rs 5,900/- (Rupees Five Thousand only)
-Registered Power of Attorney executed by the Agency in favor of the Principal Officer or the duly Authorized Representative, certifying him/her as an authorized signatory for the purpose of this RFP.
- Submission of EMD amounting to Rs. 3,00,000 (Rupees Three Lakh only)

## 17. Power of Attorney

Registered Power of Attorney executed by the agency in favor of the Principal Officer or the duly Authorized Representative, certifying him/her as an authorized signatory for the purpose of this Proposal. NPTI shall not be responsible for non- receipt/non-delivery of the Proposal due to any reason whatsoever. Bidders are advised to study the Proposal carefully. Submission of Proposal shall be deemed to have been done after careful study and examination of the Proposal with full understanding of its implications.

## 18. Penalty Clause

In case of delay from the prescribed time duration in any deliverable, 1% of penalty will be imposed each month on the stipulated payment against each delayed deliverable. The penalty will not be more than the 10% of the total project cost. If delay in allocated training quantity so happens that it has to be conducted in next financial year the Agency need to submit clarification/ justification for delay to NPTI. However, If such delay is found to be unjustified, unexplained and without reason such agency(ies) shall be de-empanelled and their bank guarantee will be enchased. NPTI decision in this regard shall be final and binding.

## 19. Award of Empanelment and award of Training Batches

i. L1 rate will be declared Course cum batch size wise.

ii. L1 rate for each such category would be offered to all the bidders.

iii. The bidders accepting the above L1 rate would be offered the letter of empanelment.

iv. A contract agreement would be signed with the successful bidder with a security deposit of Rs. 7,50,000/-

v. First award of training batches (after empanelment) would be done on the basis of ranking of the bidders. Bigger size batches would be offered to higher ranked agencies and vice a versa. If the forthcoming/proposed batches are of similar size, then the higher ranked agency would be offered the first batch and lower ranked agencies would be offered the subsequent batches. All the empanelled bidders would be awarded one batch each in first round.

vi. For subsequent batches, the feedback received from the participants (80% weightage) and ranking (20% weightage) would combine together to award a particular batch to the bidders in similar fashion with that of clause 19-vi.

vii. If a particular agency refuses to accept/conduct a particular training batch, the same would then be offered to other empanelled agency in order of their applicable ranking. The agency which refused to accept the training batch would be debarred for two rounds of batches allottment or for six months, whichever is earlier.

viii. If the average feedback of a particular agency is average or not good or below that, that empanelled agency will not be awarded any further batch till the suitable rectification has been done on the bidders end including replacement of faculty, improving the participants experience etc. The final decision in this regard would be of NPTI which will be binding to all concerned agencies.

ix. Notwithstanding anything stated above, NPTI reserves the right to award a particular batch to any empanelled agency it decides and the decision in this regard will be binding on all the empanelled agencies.

## 20. De-empanelment of Agencies

If the agency is found wanting toward their commitment as per the terms of this RFP Agreement, such agencies shall be de- empanelled with a notice period of 30 days. In case of the de-empanelment, their bank guarantee would be enchased and their allotted quota of training numbers will be divided among the rest of the empanelled agencies. Such re-distribution of training numbers shall be at the sole discretion of NPTI and will be binding on the agencies.

## 21.Contract Performance Guarantee & Signing of Agreement

In the event of the successful Bidder, within fifteen days of receipt of the Letter of Intent (LOI) from NPTI, will be required to arrange Performance Guarantee in the form of a Bank Guarantee (BG). The BG shall be as per proforma provided as part of the Draft Contract (Annexure-2 & Annexure-3).

Further, the successful Bidder shall be required to enter into a Contract Agreement with NPTI within 15 (Fifteen) days from the date of the Letter of Intent (LoI) or within such extended time as may be granted by NPTI. The duration of empanelment will be as per clause-4.

## Forms for the Proposal

Proposal is to be submitted in the following format along with the necessary documents as listed. The Proposal shall be liable for rejection in the absence of requisite supporting documents. Proposal should provide information against each of the applicable requirements. In absence of the same, the Proposal shall be liable for rejection.

## Form-1 : Letter of Performa

To
The Principal Director,
National Power Training Institute NPTI Complex, Sector-33 Faridabad -121003, Haryana India

Sub: Request for Proposal for providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode)

Sir,

The undersigned Agency, having read and examined in detail all the RFE documents in respect of appointment of an Agency for NPTI for the said project, do hereby express their interest to provide their Services as specified in the scope of work.

1. Correspondence Details

| | | |
|---|---|---|
| 1 | Name of the Agency | |
| 2 | Address of the Agency | |
| 3 | Name of the contact person to whom all references shall be made regarding this Tender | |
| 4 | Designation of the person to whom all references shall be made regarding this tender | |
| 5 | Address of the person to whom all references shall be made regarding this Tender | |
| 6 | Telephone (with STD code) | |
| 7 | E-mail of the contact person | |
| 8 | Fax No. (with STD code) | |

2. Document forming part of Proposal

   We have enclosed the following:

Form 1: Letter Proforma Form 2: Minimum Eligibility
Form 3: List of the Program Organized in Past (Completion certificates conforming the experience to be attached as relevant and work-orders)
Form 4: CVs of the proposed team members Form 5: Self Declaration for Training Facility
Form 6: Declaration for Non-Blacklisting and Non Debarment
Form 7: Financial proposal
-Bid processing fee of Rs 5,900/-
-Registered Power of Attorney executed by the Agency in favor of the Principal Officer or the duly Authorized Representative, certifying him/her as an authorized signatory for the purpose of this RFP.
- Submission of EMD amounting to Rs. 3,00,000(Three Lakh Rupees only)

3. Declaration
   We hereby declare that our Proposal is made in good faith and the information contained is true and correct to the best of our knowledge and belief.

Thanking you
Yours faithfully,

(Signature of the Officer)
Name :
Designation :
Seal :
Date :
Place :
Business Address:

**Form-2 : Minimum Eligibility**

| | | | |
|---|---|---|---|
| 2.1 | Name of the Agency | | |
| 2.2 | Year of Registration | | |
| | | | **Attached or Not attached** |
| 2.3 | Legal Entity | Copy of Certificate of establishment | |
| 2.4 | Manpower Strength | HR Certificate with stamped and signature of authorized signatory | |
| 2.5 | Agency experience | Copies of related workorders/MoUs/Agreements/LoIs/Work Completion Certificate/Sanction letters | |
| 2.6 | Blacklisting | Undertaking on agency letterhead by signed and stamped by Authorized signatory | |

(Signature of the Officer)

Name :
Designation :
Seal :
Date :
Place :
Business Address:

**Form-3: List of programs organized in the past**

| Sr. No. | Program name | Type of target institution | Level of participants | No. of participants | Duration | Location | Year |
|---|---|---|---|---|---|---|---|
| 1 | | | | | | | |
| 2 | | | | | | | |
| 3 | | | | | | | |
| 4 | | | | | | | |
| 5 | | | | | | | |
| 6 | | | | | | | |
| 7 | | | | | | | |
| 8 | | | | | | | |
| 9 | | | | | | | |
| 10 | | | | | | | |

**Please Note:**

a. For each program specified above, please provide the detailed writeup (in separate plain sheet) for each program. This will help in understanding the project at a glance.

b. Work Order along with Completion Certificate or in-progress certificate from the client shall be mandatorily attached along with Project Description Template in support of each project.

(Signature of the Officer)
Name :
Designation :
Seal :
Date :
Place :
Business Address:

### Form-4 List of proposed faculties& CV

| S.No. | Name of faculty | Type of faculty (on-roll/in-house, experience(yrs),subject matter expert or international trainer etc.) |
|---|---|---|
| 1 | | |
| 2 | | |
| 3 | | |
| 4 | | |
| 5 | | |
| 6 | | |

**Form-5: Self-declaration for Virtual facility**
**(To be furnished on the Agency letter head with seal)**

**To,**
**NATIONAL POWER TRAINING INSTITUTE**
**NPTI Complex, Sector-33, Faridabad-121003**
**Ph-0129-2274916,17**
**www.npti.gov.in**

We hereby confirm and declare that (Agency Name), has the required Virtual Lab Facility.

For _

Authorized Signatory
Name:
Date:

**Form-6: Declaration for Non-Blacklisting or Non-Debarment**
**(On company Letter Head)**

I, authorized representative of __________(Designation),of the firm/agency _______ do here by solemnly affirm that our firm/agency ________ has never been blacklisted/debarred Blacklisted or Debarred or, EMD forfeited for failure to comply with contract terms of any government undertaking/UT administration/ PSUs in as on date of issue of RFEin last 3 Years.

(Signature of Authorized Signatory)

Name:
Designation:
Date:
Place:

**Form-7 : Financial Proposal**

To
The Principal Director,
National Power Training Institute
NPTI Complex, Sector-33
Faridabad -121003,
Haryana India

Sub: Request for Proposal for providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode)

Sir,

In response to the above-mentioned subject, hereunder is our financial cost for the project:

I/we_______________ herewith enclose Financial Offer of Rs. _________ (in words) for selection of my/our Agency for providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode). The break-up of the above cost is given as below.

| **S. No.** | **Course Name** | **Maximum Price per candidate (In INR Including GST)** | **Offered price per Candidate by Agency (In INR Including GST)** | | |
|---|---|---|---|---|---|
| | | | **Batch size less then equal to 50** | **Batch Size from 51 to 100** | **Batch Size More than 100** |
| 1 | Two Weeks Basic Level Cyber Security Training and Certification Program (Online Mode) | 18408 | | | |
| 2 | One Week Basic Level Cyber Security Training and Certification Program (Offline Mode) | 14160 | | | |
| 3 | Two weeks Intermediate Level Cyber Security Training and Certification Program (Hybrid Mode) | 23600 | | | |
| 4 | Two Weeks Advance Level Cyber Security Training and Certification Program (Hybrid Mode) | 30000 | | | |

We hereby declare that our Proposal is made in good faith and the information contained is true and correct to the best of our knowledge and belief.

Thanking you,

Yours faithfully

(Signature of the Officer)
Name :
Designation :
Seal :
Date :
Place :
Business Address:

## Annexure-2: FORM FOR CONTRACT PERFORMANCE GUARANTEE

Ref. No. : Date:

Bank Guarantee No.:

To,

NATIONAL POWER TRAINING INSTITUTE
NPTI Complex, Sector-33,
Faridabad-121003
Ph-0129-2274916,17
www.npti.gov.in

Dear Sirs,

1. In consideration of National Power Training Institute with its Registered Office at NPTI Complex, Sector 33, Faridabad – 121003, (hereinafter called the "Owner" which expression shall unless repugnant to the subject or context include its successors and assigns) having entered into a contract No. ____dated ______ (hereinafter called the Contract" which expression shall include all the amendments thereto) with M/s_______ having its registered /head office at ________(hereinafter referred to as the 'Contractor') which expression shall, unless repugnant to the context or meaning hereof include all its successors, administrators, executors and assignees) and NPTI having agreed that the Contractor shall furnish to NPTI a performance guarantee for Indian Rupees for the faithful performance of the entire contract.

2. We (name of the bank) ______ registered under the laws of _________ having head/registered office at __________ (hereinafter referred to as "the Bank" , which expression shall, unless repugnant to the context or meaning thereof, include all its successors, administrators, executors and permitted assignees) do hereby guarantee and undertake to pay immediately on first demand in writing any/all moneys to the extent of Indian Rs./ (in words) without any demur, reservation, contest or protest and/or protest and/or without any reference to the Contractor. Any such demand made by NPTI on the bank by serving a written notice shall be conclusive and binding, without any proof, on the bank as regards the amount due and payable, notwithstanding any dispute(s) pending before any Court, Tribunal, Arbitrator or any other matter or thing whatsoever, as liability under these presents being absolute and unequivocal and shall continue to be enforceable until it is discharged by NPTI in writing. This guarantee shall not be determined, discharged or affected by the liquidation, winding up, dissolution or insolvency of the Contractor and shall remain valid, binding and operative against the bank.

3. The Bank also agrees that NPTI at its option shall be entitled to enforce this Guarantee against the bank as a principal debtor, in the first instance, without proceeding against the Contractor and notwithstanding any security or other guarantee that NPTI may have in relation to the Contractor's liabilities.

4. The Bank further agrees that NPTI shall have the fullest liberty without our consent and without affecting in any manner our obligations hereunder to vary any of the terms and conditions of the said contract or to extend time for performance by the said Contractor(s) from time to time or to postpone for any time or from time to time exercise of any of the powers vested in NPTI against the said Contractor(s) and to forbear or enforce any of the terms and condition relating to the said agreement and we shall not be relieved from our liability by reason of anysuch variation, or extension being granted to the said Contractor(s) or for any forbearance, act or omission on the part of NPTI or any indulgence by NPTI to the said Contractor(s) or any such matter or thing whatsoever which under the law relating to sureties would, but for this provision, have effect of so relieving us.

5. The Bank further agrees that the Guarantee herein contained shall remain in full force during the period that is taken for the performance of the contract and all dues of NPTI under or by virtue of this contract have been fully paid and its claim satisfied or discharged or till NPTI discharges this guarantee in writing, whichever is earlier.

6. This Guarantee shall not be discharged by any change in our constitution, in the constitution of NPTI or that of the Contractor.

7. The bank confirms that this guarantee has been issued with observance of appropriate laws of the country of issue.

8. The Bank also agrees that this guarantee shall be governed and constructed in accordance with Indian Laws and subject to the exclusive jurisdiction of Indian Courts of the place from where the purchase order has been placed.

9. Notwithstanding anything contained hereinabove, our liability under this Guarantee is limited to Indian Rs.____/(in figures )_______(Indian Rupees/ in Words) __________I and our guarantee shall remain in force until __________(indicate the date of expiry or bank guarantee, any claim under this Guarantee must be received by us before the expiry of this Bank Guarantee. If no such claim has been received by us by the said date, the rights of NPTI under this Guarantee will cease. However, if such a claim has been received by us within the said date, all the rights of NPTI under this Guarantee shall be valid and shall not cease until we have satisfied that claim.

In witness whereof, the Bank through its authorized officer has set its hand and stamp on this ______day _____ of _____2024 at ______

**WITNESS NO1**

_________________ _______________

(Signature) (Signature)

Full Name, Designation
Official Address

**Witness No 2**

________________
(Signature)

Full Name and Official
Address (in legible Letters)

Full Name, Designation
Official Address

Attorney as Power of
Attorney No. ______
Dated____________

## Annexure-3 Contract Agreement Format

# CONTRACT FOR providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode)

This CONTRACT (hereinafter, together with all Appendices attached hereto and forming an integral part hereof, called the “Contract”) is made the _______day of the month _____ of ________2024, between, on the one hand National Power Training Institute (NPTI) (hereinafter called “Owner”) and, on the other hand, ______________ (hereinafter called the “Agency”).

WHEREAS

**A.** Owner intends to engage Agency towards providing experts/resource personnel for conducting Cyber Security Training and Certification Programs (Offline, Online and Hybrid Mode)

**B.** The Agencies, having represented to the Owner that they have required professional skills, personnel and technical resources agreed to provide the Services on the terms and conditions set forth in this Contract;

NOW THEREFORE the parties hereto hereby agree as follows:

## 1. GENERAL PROVISIONS

### 1.1. Definitions

Unless the context otherwise requires, the following terms whenever used in this Contract have the following meanings:

**a)** “Applicable Law” means the laws and any other instruments having the force of law in the Owner’s country, as they may be issued and in force from time to time;
**b)** “Contract” means this Contract together with all Appendices/ Attachments and including all modifications made in accordance with the provisions of Clause 2.5 hereof between the Owner and the agency;
**c)** “Effective Date” means the date on which this Contract comes into force and effect pursuant to Clause-2.l hereof;
**d)** “Personnel” means persons hired by the agency as employees and assigned to the performance of the Services or any part thereof’.
**e)** “Party” means the Owner or the Agency, as the case may be;
**f)** “Services” means the work to be performed by the Agency pursuant to this Contract
**g)** “Starting Date” means the date of issue of LOI.

### 1.2. Relation between the Parties

Nothing contained herein shall be construed as establishing a relation of master and servant or of agent and principal as between the Owner and the Agency. The Agency, subject to this Contract, have complete charge of personnel performing the Services and shall be fully responsible for the Services performed by them or on their behalf hereunder.

### 1.3. Law Governing Contract

This Contract, its meaning and interpretation, and the relation between the Parties shall be governed by the Applicable Law of India.

### 1.4. Language

This Contract has been executed in the English language, which shall be the binding and controlling language for all matters relating to the meaning or interpretation of this contract.

### 1.5. Headings

The headings shall not limit, alter or affect the meaning of this Contract.

### 1.6. Notices

**1.6.1.** Any notice, request or consent required or permitted to be given or made pursuant to this Contract shall be in writing. Any such notice, request or consent shall be deemed to have been given or made when delivered in person to an authorized representative of the Party to whom the communication is addressed, or when sent by registered mail, telex, telegram or facsimile to such Party at the following address:

**For the Owner:**

Attention:

Facsimile:

For the Agency:

Attention:

Facsimile

**1.6.2.** Notice will be deemed to be effective as follows

**a)** In the case of personal delivery or registered mail, on delivery;

**1.6.3.** A Party may change its address for notice hereunder by giving the other Party notice of such change pursuant to this Clause.

### 1.7. Location

The Services shall be performed Pan India basis or at such location required / approved by Owner.

### 1.8. Authorized Representatives

Any action required or permitted to be taken, and any document required or permitted to be executed under this Contract, may be taken or executed:

a) on behalf of the Owner by______ or his designated representative;

b) On behalf of the Agency by ______ or his designated representative.

## 2. COMMENCEMENT, COMPLETION, MODIFICATION AND TERMINATION OF CONTRACT

### 2.1. Effectiveness of Contract

This Agreement will become effective upon signing by both the parties.

### 2.2. Commencement of Services

The Agency shall begin carrying out the Services immediately viz. from the date of issue of LOI (the “Starting Date”), or on such date as the Parties may agree in writing.

### 2.3. Expiration of Contract

Unless terminated earlier pursuant to Clause-2.8 hereof, this Contract shall be effective for a period of three years from the date of effectiveness of the contract, which may be terminated at any time during the entire period of empanelment with one month notice from either parties.

2.4. Entire Agreement.

This Contract contains all covenants, stipulations and provisions agreed by the parties. No agent or representative of either Party has authority to make, and the parties shall not be bound by or be liable for, any statement, representation, promise or agreement not set forth herein.

2.5. Modification

Modification of the terms and conditions of this Contract, including any modification of the scope of the Services, may only be made by written agreement between the parties and shall not be effective until the consent of the parties has been obtained, however, each Party shall give due consideration to any proposals for modification made by the other Party.

2.6. Force Majeure

2.6.1. Definition

In the event of either party being rendered unable by Force Majeure to perform any obligation required to be performed by them under the CONTRACT, the relative obligation of the party affected by such Force Majeure shall be suspended for the period during which such cause lasts.

The term “Force Majeure” as employed herein shall mean acts of God, War, Civil Riots, Fire directly affecting the performance of the CONTRACT, Flood and Acts and Regulations of respective government of the two parties, namely Owner and the Agency.

Upon the occurrence of such cause and upon its termination, the party alleging that it has been rendered unable as aforesaid thereby, shall notify the other party in writing, the beginning of the cause amounting to Force Majeure as also the ending of the said clause by giving notice to the other party within 72 hours of the ending of the cause respectively. If the deliveries are suspended by Force Majeure conditions lasting for more than 2 (two) months, Owner shall have the option of canceling this CONTRACT in whole or part at his discretion without any liability at his part.

Time for performance of the relative obligation suspended by Force Majeure shall then stand extended by the period for which such cause lasts.

2.6.2. No Breach of Contract

The failure of a party to fulfill any of its obligations hereunder shall not be considered to be a breach of or default under, this Contract in so far as such inability arises from an event of Force Majeure, provided that the party affected by such an event has taken all reasonable precautions, due care and reasonable alternative measures, all with the objective of carrying out the terms and conditions of this Contract.

2.6.3. Measures to be taken

a) A Party affected by an event of Force Majeure shall take all reasonable measures to remove such Party’s inability to fulfill its obligations hereunder with a minimum of delay.

b) A Party affected by an event of Force Majeure shall notify theother Party such event as soon as possible, and in any event not later than fourteen (14) days following the occurrence of such event, providing evidence of the nature and cause of such event, and shall similarly give notice of the restoration of normal conditions as soon as possible.

c) The parties shall take all reasonable measures to minimize the consequences of any event of Force Majeure.

2.6.4. Extension of Time

Any period within which a Party shall, pursuant to this Contract, complete any action or task, shall be extended for a period equal to the time during which such Party was unable to perform such action as a result of Force Majeure.

2.6.5. Consultation

Not later than thirty (30) days after the Agency, as the result of an event of Force Majeure, have become unable to perform a material portion of the Services, the parties shall consult with each other with a view to agreeing on appropriate measures to be taken in the circumstances.

2.7. Suspension

The Owner may, by written notice of suspension to the Agency, suspend all payments to the Agency hereunder if the Agency fail to perform any of their obligations under this contract, including the carrying out of services, provided that such notice of suspension (i) shall specify the nature of the failure, and (ii) shall request the Agency to remedy such failure within a period not exceeding thirty (30) days after receipt by the Agency of such notice of suspension and if such failure is not rectified within the period, then shall invoke contract performance guarantee.

2.8. Termination

2.8.1. By the Owner

The Owner may by not less than thirty (30) days' written notice of termination to the Agency (except in the event listed in paragraph (f) below, for which there shall be a written notice of not less than sixty (60) days) such notice to be given after the occurrence of any of the events specified in paragraphs (a) to (g) of this Clause-2.8.l, terminate this Contract:

a) If the Agency fail to remedy a failure in the performance of their obligations hereunder, as specified in a notice of suspension pursuant to Clause-2.7 here-in-above, within thirty (30) days of receipt of such notice of suspension or within such further period as the Owner may have subsequently approved in writing;

b) If the Agency become insolvent or bankrupt or enter into an agreements with their creditors for relief of debt or take advance of any law for the benefit or debtors or go into liquidation receivership whether compulsory or voluntary;

c) If the Agency fail to comply with any final decision reached as a result of arbitration proceedings pursuant to Clause-7 hereof;

d) If the Agency submit to the Owner a statement which has a material effect on the rights, obligations or interests of the Owner and which the Agency know to be false;

e) If, as the result of Force Majeure, the Agency are unable to perform a material portion of the Services for a period of not less than sixty (60) days; or

f) If the Agency has engaged in corrupt or fraudulent practices or is found to have misrepresented the facts or has provided false information/documentation.

g) If the Owner, in its sole discretion and for any reason whatsoever, decides to terminate this Contract.

2.8.2. Cessation of Rights and Obligations

Upon termination of this Contract pursuant to Clauses- 2.8.1 hereof or upon expiration of this Contract pursuant to Clause-2.3 hereof, all rights and obligations of the parties hereunder shall cease, except:

a) Such rights and obligations as may have accrued on the date of termination or expiration,

b) The obligation of confidentiality set forth in Clause-3.2.4 hereof,

c) Any right which a Party may have under the Applicable Law.

2.8.3. Cessation of Services

Upon termination of this Contract by notice to pursuant to clauses-2.8.1 hereof, the Agency shall, immediately upon dispatch or receipt of such notice, take all- necessary steps to bring the Services to a close in a prompt and orderly manner and shall make every reasonable effort to keep expenditures for this purpose to a minimum.

2.8.4. Payment upon Termination

Upon termination of this Contract pursuant to Clause-2.8.1 hereof the Owner shall make the following payments to the Agency:

a) Remuneration for Services satisfactorily performed prior to the effective date of termination;

b) Reimbursable expenditures for expenditures actually incurred prior to the effective date of termination; and

c) Except in the case of termination pursuant to paragraphs (a) to (d) of Clause-2.8.1 hereof reimbursement of any reasonable cost incident to the prompt and orderly termination of the Contract including the cost of the return travel of the Agency' personnel and their eligible dependents.

3. OBLIGATIONS OF THE AGENCY

3.1. General

3.1.1. Standard of Performance

The Agency shall perform the Services and carry out their obligations hereunder with all due diligence, efficiency and economy, in accordance with generally accepted techniques and practices used with professional engineering and consulting standards recognized by professional bodies, and shall observe sound management, and technical and engineering practices, and employ appropriate advanced technology and safe and effective equipment, and methods. The Agency shall always act, in respect of any matter relating to this Contract or to the Services, as faithful advisers to the Owner, and shall at all times support and safeguard the Owner's legitimate interests in any dealings with Third parties.

3.1.2. Law Governing Services

The Agency shall perform the Services in accordance with the Applicable Law and shall take all practicable steps to ensure that the Personnel and agents of the Agency comply with the Applicable Law.

3.1.3. Conflict of Interest

The Agency shall hold the Owner's interest paramount, without any consideration for future work, and strictly avoid conflict with other assignments or their corporate interests.

3.2.1. Agency Not to Benefit from Commissions, Discounts etc.

The payment of the Agency shall constitute the Agency's only payment in connection with this Contract or the Services, and the Agency shall not accept for their own benefit any trade commission, discount, or similar payment in connection with activities pursuant to this Contract or to the Services or in the discharge of their obligations under the Contract, and the Agency shall use their best efforts to ensure that the Personnel, and agents of either of them similarly shall not receive any such additional payment.

3.2.2. Agency and Affiliates not to be otherwise interested in Project

The Agency agrees that, during the term of this Contract and after its termination, the Agency shall be disqualified from providing goods, works or services (other than consulting services) resulting from or directly related to the Agency's Services for the preparation or implementation of the project.

3.2.3. Prohibition of Conflicting Activities

The Agency shall not engage, either directly or indirectly, in any business or professional activities which would conflict with the activities assigned to them under this Contract.

The Agency hired to provide services for the proposed assignment will be disqualified from services related to the initial assignment for the same project subsequently.

In case of rating of the proposed project, for which this consultancy services are being provided, then the Agency will not rate this project nor in any way be associated in rating of this project.

3.2.4. Confidentiality

The Agency and the Personnel of either of them shall not, either during the term or within 6 months after the expiration of this Contract, disclose any proprietary or confidential information relating to the Project, the Services, this Contract or the Owner's business or operations without the prior written consent of the Owner.

3.3. Insurance to be taken out by the Agency

The Agency shall take out and maintain at their own cost, appropriate insurance against all the risks, and for all the coverage, like staff compensation, employment liability insurance for all the staff on the assignment comprehensive general liability insurance, including contractual liability coverage adequate to cover the indemnity of obligation against all damages, costs, and charges and expenses for injury to any person or damage to any property arising out of, or in connection with, the services which result from the fault of the Agency or their staff on the assignment.

3.4. Liability of the Agency

The Agency shall be liable to the Owner for the performance of the Services in accordance with the provisions of this Contract and for any loss suffered by the Owner as a result of a default of the Agency in such performance, subject to the following limitations:

a) The Agency shall not be liable for any damage or injury caused by or arising out of the act, neglect, default or omission of any persons other than the Agency or the Personnel of either of them; and

b) The Agency shall not be liable for any loss or damage caused by or arising out of circumstances over which the Agency had no control, provided that there is no negligence or wrongful actions.

c) The liability of the Agency will be limited to the extent of contract value of the project.

3.5. Indemnification of the Owner by the Agency

The Agency shall keep the Owner, both during and after the term of this Contract, fully and effectively indemnified against all losses, damage, injuries, deaths, expenses, actions, proceedings, demands, costs and claims, including, but not limited to, legal fees and expenses, suffered by the Owner or any Third Party, where such loss, damage, injury or death is the result of a wrongful action, negligence or breach of Contract of the Agency, or the Personnel or agents of either of them including the use or violation of any copyright work or literary property or patented invention, article or appliance.

3.6. Documents prepared by the Agency to be the Property of the Owner:

All plans, drawings, specifications. designs, reports and other documents prepared by the Agency in performing the Services shall become and remain the property of the Owner, and the Agency shall, not later than upon termination or expiration of this Contract, deliver all such documents to the Owner, together with a detailed inventory thereof. The Agency may retain a copy of such documents shall not use them for purposes unrelated to this Contract without the prior written approval of the Owner.

4. AGENCY' PERSONNEL

4.1. General

The Agency shall deploy qualified and experienced personnel/Faculty/Experts as are required to carry out the Services.

4.2. Description of Personnel

The titles, agreed job descriptions and minimum qualifications of each of the Agency' Personnel shall be specified to the Owner at the time of award of the assignment.

4.3. Removal and/or Replacement of Personnel

a) Except as the Owner may otherwise agree, no changes shall be made in the Personnel. If, for any reason beyond the reasonable control of the Agency, it becomes necessary to replace any of the Personnel, the Agency shall forthwith provide as a replacement a person of equivalent or better qualifications, which shall be approved by the Owner.

b) If the Owner:

1) Finds that any of the Personnel has committed serious misconduct or has 0n charged with having committed a criminal action, or

2) Has reasonable cause to be dissatisfied with the performance of any of the Personnel, then the Agency shall at the Owner's written request specifying the grounds therefore, forthwith provide as a replacement a person with qualifications and experience acceptable to the Owner.

c) Any of the Personnel provided as a replacement under Clauses (a) and (b) above, the rate of remuneration applicable to such person as well as any reimbursable expenditures (including expenditures due to the number of eligible dependents) the Agency may wish to claim as a result of such replacement, shall be subject to the prior written approval by the Owner. Except as the Owner may otherwise agree,

1) The Agency shall bear all additional travel and other costs arising out of or incidental to any removal and/or replacement, and

5. OBLIGATIONS OF THE OWNER/AGENCY

5.1 Payment

In consideration of the Services performed by the Agency under this Contract the owner shall make payment to the Agency in such manner as is provided by this Contract as per terms and conditions mentioned in scope of works

5.2 Roles and Responsibilities

The Owner and the Agency agree to assume responsibilities and tasks as elaborated in the scope of work along.

5.3 The owner shall cause the payment of the Agency as per the above given in schedule of payment, within thirty (30) days after the receipt of bills with supporting document by the Owner. But if the progress is not satisfactory and according to agreed work program / schedule, the payment may be withheld.

5.4 Final Payment shall be made only after satisfactory completion of all the activities as per TOR of the project.

6. FAIRNESS AND GOOD FAITH

6.1. Good Faith:

The parties undertake to act in good faith respect to each other's rights under this Contract and to adopt all reasonable measures to ensure the realization of the objectives of this Contract.

6.2. Operation of the contract:

The parties recognize that it is impractical in this Contract to provide for every contingency which may arise during the life of this contract, and the parties hereby agree that it is their intention that this Contract shall operate fairly as between them and without detriment to the interest of either of them and that, if during the tenure of this Contract either Party believes that this Contract is operating unfairly, the parties will use their best efforts to agree on such action as may be necessary to remove the cause or causes of such unfairness, but no-failure to agree on any action pursuant to this Clause shall give rise to a dispute subject to arbitration in accordance with Clause-8 hereof.

7. JURISDICTION AND APPLICABLE LAW:

This agreement including all matter connected with this Agreement, shall be governed by the laws of India (both substantive and procedural) for the time being in force and shall be subject to exclusive jurisdiction of the Indian Courts at Faridabad.

8. SETTLEMENT OF DISPUTES:

8.1. Amicable Settlement

Except as otherwise provided elsewhere in the contract, if any dispute, difference, question or disagreement arises between the parties hereto or their respective representatives or assignees, in connection with construction, meaning, operation, effect, interpretation of the contract or breach thereof which parties are unable to settle mutually, the same shall be referred to Arbitration as provided hereunder:

1) A party wishing to commence arbitration proceeding shall invoke Arbitration Clause by giving 60 days notice to the other party.

2) The party invoking arbitration shall specify all the points of disputes with details of the amount claimed to be referred to arbitration at the time of invocation of arbitration and not thereafter.

3) NPTI shall appoint a Sole Arbitrator with the approval of Director General, NPTI.

4) It is agreed that there will be no objection that the Arbitrator appointed holds equity shares of NPTI or is a retired employee of NPTI.

5) If any of the Arbitrators so appointed dies, resigns, becomes incapacitated or withdraws for any reason from the proceedings, it shall be lawful for the concerned party to appoint another person in his place in the same manner as aforesaid. Such person shall proceed with the reference from the stage where his predecessor has left if both parties consent for the same; otherwise, he shall proceed de novo.

6) It is a term of the Contract that neither party shall be entitled for any pre- reference or pendent- lite interest on its claims. Parties agree that any claim for such interest made by ay party shall be void.

7) The arbitrator(s) shall give reasoned and speaking award and it shall be final and binding on the parties.

8) The parties to the arbitration will bear the fees and expenses in equal proportion to be determined by the arbitrators.

9) The venue of arbitration will be Faridabad.

10) Subject to aforesaid, provisions of the Arbitration and Conciliation Act, 1996 and any statutory modifications or re-enactment thereof shall apply to the arbitration proceeding under this clause.

8.2. The courts of Faridabad alone shall have exclusive jurisdiction on any dispute arising out of this contract.

IN WITNESS WHEREOF, the Parties hereto have caused this Contract to be signed in their respective names as of the day and year first above written.

FOR AND ON BEHALF (OWNER)

BY ……………………………………

Authorized Signatory

Date:

Place:

FOR AND ON BEHALF OF [AGENCY]

BY ……………………………………………

Authorized Signatory

Date:

Place:

## Appendix 1

| **Program Schedule II** | | | |
|---|---|---|---|
| **Program Title** | | **Basic Level Cyber Security Training & Certification** | |
| **Duration** | | **01 Week** | |
| **Participants** | | **Power Professionals** | |
| **Mode of Training** | | **Offline** | |
| **Day** | **Session in Hrs** | **Topics** | **Contents** |
| **Day 1**<br>**Monday** | **FN/AN (9:30 to 13:00)**<br>**15min Tea Break** | **Introduction to Cyber Security and Cyber Risk Management** | **Inauguration (09:15 - 09:30 Hrs)**<br>• **1. Introduction to Cyber Security: - Details (30 Min)**<br>• 1.1. What is Cyber Security?<br>• 1.2. What are the Cyber Risks?<br>• 1.3. Basic Cyber hygiene<br>• 1.4. Cyber Security of IT vs. OT<br>• **2. Role of CSIRT-Power, CERT-In, Power Sector** CERTs, NCIIPC, IT Act 2000 with amendments, Govt. Initiatives and Guidelines, **GIGW 3.0** (**90 Min**)<br>• 2.1 Cyber Security Guidelines issued by CEA<br>• **3 Risk Assessment (60 Min)**<br>• 3.1 Models: - List of models to be identified<br>• **Assessment (Quiz of 15 MCQ) (15Min)**<br>****Tentative list of faculties to be identified for this session. |
| | **A N (14:00 to 18:00)**<br>**15 min Tea Break** | | **1.Cyber Security Threat Landscape (60 Min)**<br>• Man in the middle Attack<br>• DoS /DDoS<br>• Ransom ware Attack etc.<br>**2.Modes of Attack (90 Min)**<br>• Phishing Awareness<br>• Remote Session Security<br>• Device/End Point Security<br>• Server Security<br>• Network Security<br>• Application Security, ICS and SCADA Security<br>3.**Examples of Attack (30 Min)**<br>**4.Assessment (Quiz of 15 MCQ) (15 Min)** |
| **Day 2**<br>**Tuesday** | **FN (09:30 to 13:00)**<br>**15 min Tea Break** | **Network Security** | **1.Network Elements (30 Min)**<br>• Firewall<br>• Router<br>• Storage Devices<br>• Switch |

|  |  |  |  |
|---|---|---|---|
|  |  |  | • Servers<br>• Intrusion Detection and Intrusion Prevention<br>**2. Network Security Fundamentals (30 Min)**<br>• Network Protocols and their security Issues<br>○ DNS, TCP/IP, LAN, Physical Layer Security<br>○ Wifi Security<br>○ Intranet Security<br>○ Port Analysis<br>• Network Cyber Threats<br>**3. Mitigation Measures (30 Min)**<br>• Network Zoning and Segregation<br>• Detecting Network based Attacks<br>• Encryption, Hashing, Digital Signature<br>• Router Security<br>**4. Reference architecture of Power Sector (45 Min)**<br>**5. Examples of Vulnerability in devices and examples of security gaps in network architecture (45 Min)**<br>**6.Assessment (Quiz of 15 MCQ) (15 Min)** |
|  | **A N (14:00 to 18:00)**<br>**15 min Tea Break** |  | **LAB 1: Hands on Malware Analysis (90 Min)**<br>• Manual Tools to check malware<br>• Use URL, IP address, Domains & File Hashes and Use of Virus Total to check against malware<br>• Malware Analysis Tool Usage (Signature, Yara Rules)<br>**LAB 2: Operating System Hardening (120 Min)**<br>• Understanding the concept of O/S Hardening against Vulnerabilities<br>• Lynis Tool for Linux<br>• Windows Group Policy Edit Tool<br>• Openscap and Scap Workbench for Configuration Audit<br>**Assessment (Quiz of 15 MCQ) (15 Min)** |
| **Day 3**<br>**Wednesday** | **FN (09:30 to 13:00)**<br>**15 min Tea Break** | **Application Security** | **1.Security Threats to Applications – Stand alone, Network based applications, Web applications (90 Min)**<br>• Application Security Threats and Problems<br>• Application Security Threat Detection and Mitigation<br>• Web Application Security Threats and Attacks<br>• Web Application Attack Detection<br>• SSL/TLS and Digital Certificates<br>**2.Vulnerability Assessment and Penetration Testing (VAPT) (90 Min)**<br>• OWASP Top 10 Vulnerabilities |

| | | | |
|---|---|---|---|
| | | | • Capturing Web traffic<br>• Web Application VAPT<br>**3. Assessment (Quiz of 15 MCQ) (15 Min)** |
| | **AN (14:00 to 18:00)**<br>**15 min Tea Break** | | **Application Security (60 Min)**<br>• Buffer Overflow Lab<br>• Integer Overflow Lab<br>• Privilege Escalation Labs<br>• Open VAS Lab<br>**Web Security (60 Min)**<br>• Command Injection Lab<br>• SQL Injection Lab<br>• Cross-site Scripting Lab<br>• Cross-site Request Forgery Lab<br>• Session Hijacking Lab<br>• OWASP vulnerabilities Lab<br>**Network Labs (90 Min)**<br>• Arp Spoofing Lab<br>• Packet Sniffing and Packet Analysis Lab<br>• Man-in-the-Middle Attack<br>• Network reconnaissance, Wireshark overview & Hands on<br>**Assessment (Quiz of 15 MCQ) (15 Min)** |
| **Day 4**<br>**Thursday** | **FN (09:30 to 13:00)**<br>**15 min Tea Break** | **Best Practices and Awareness** | **1. Cyber Security Standards (90 Min)**<br>• Introduction to various standards such as NIST Cyber Security Framework/NERC-CIP/ISO27001/ISO27002/ISO 27019 etc.<br>• NESCOR guide to vulnerability assessment<br>**2. Security assessment strategy (30 Min)**<br>• Risk Assessment<br>**3. Cyber Security Hardening Techniques: - (30 Min)**<br>• Authentication and Authorization<br>• Network Traffic Analysis<br>• Patch Management and Up gradation<br>**4.Case Studies:-(15 Min)**<br>• SolarWind, Colonial Pipeline, Black Energy 3 &Stuxnet, malware infection on Kudankulam Nuclear Power Plant (KKNPP) - Lessons Learnt<br>**5. Assessment (Quiz of 15 MCQ) (15 Min)** |
| | **A N (14:00 to 18:00)**<br>**15 min Tea Break** | | **Wifi Network Lab (90 Min)**<br>• Password sniffing in wifi network<br>• Reconnaissance on wifi network using aircrack-ng<br>• Wifi password cracking lab |

| | | | |
|---|---|---|---|
| | | | **IDS Lab (120 Min)**<br>• Using Snort NIDS<br>• Using Zeek/Bro NIDS<br>• Visualization of network traffic data<br>• Visualization of security events using ELK<br>• Host/Endpoint Intrusion Detection Lab using Wazuh<br>• OSSEC HIDS Lab<br>**Assessment (Quiz of 15 MCQ) (15 Min)** |
| **Day 5**<br>**Friday** | **FN (09:30 to 13:00)**<br>**15 min Tea Break** | **Emerging Technologies** | **1. Cyber Security Tools and Technologies:-(90 Min)**<br>• Intrusion Detection System (IDS) & Intrusion Prevention System (IPS)<br>• Deception technology<br>• Data diode<br>• SIEM (Security Information and Event<br>• Management) & EDR (Endpoint Detection & Response)<br>• SOC (Security Operation Center)<br>**2. Cyber Security integration with other technologies:(90 Min)**<br>• Technologies for anomaly detection in power system<br>• Malware Detection<br>• Artificial Intelligence and Machine Learning<br>• Industrial IoT<br>• Big Data<br>• Blockchain etc.<br>3. **Assessment (Quiz of 15 MCQ) (15 Min)** |
| | **A N (14:00 to 17:30)**<br>**30 min Tea Break** | | **Lab:-(90 Min)**<br>• Honeypots for Threat Intelligence Collection Lab<br>• Use of Honey Tokens<br>**Assessment (Quiz of 15 MCQ) (45 Min)**<br>**Open Discussion and Queries (60 Min)** |
| | **17:30 to 18:00** | Overall feedback of the training program & Interaction with participants | |

| Program Schedule -I | | | |
|---|---|---|---|
| **Program Title** | | **Basic level theory on Cyber Security for Power Professionals** | |
| **Duration** | | **01 Week** | |
| **Participants** | | **Power Sector Professionals** | |
| **Mode of Training** | | **Online Two weeks** | |
| **Day** | **Session in Hrs** | **Topics** | **Contents** |
| **Day 1**<br>**Monday** | **FN**<br>**(10:00 to 13:00)** | **Introduction to Cyber Security and Cyber Risk Management** | **Inauguration (09:15 - 10:00 Hrs)**<br>• Introduction to Cyber Security<br>• What is Cyber Security?<br>• What are the Cyber Risks?<br>• Risk Assessment Models<br>• Basic Cyber hygiene<br>• Cyber Security of IT vs. OT<br>• Role of CERT-In, Power Sector Sectorial CERTs, NCIIPC, IT Act 2000 with amendments, Govt. Initiatives and Guidelines |
| | **A N (14:00 to 17:00)** | | **Cyber Security Awareness**<br>• Phishing Awareness<br>• Remote Session Security<br>• Device/End Point Security<br>• Server Security<br>• Network Security<br>• Application Security |
| **Day 2**<br>**Tuesday** | **FN (10:00 to 13:00)** | **Network Security** | Network Security Fundamentals<br>• Network Zoning and Segregation<br>• Network Cyber Threats<br>• Network Protocols and their security Issues<br>o DNS, TCP/IP, LAN, Physical Layer Security<br>o Wifi Security<br>o Intranet Security<br>o Port Analysis<br>• Mitigation Techniques<br>• ICS and SCADA Security<br>Assessment of Day 1 (Quiz of 30 MCQ – 40 min) |

| | | | |
|---|---|---|---|
| | **A N (14:00 to 17:00)** | | • Firewall<br>• Intrusion Detection and Intrusion Prevention<br>• Deception Technology<br>• Detecting Network based Attacks<br>• Encryption, Hashing, Digital Signature<br>• Router Security |
| **Day 3**<br>**Wednesday** | **FN (10:00 to 13:00)** | **Application Security** | Security Threats to Applications – Stand alone, Network based applications, Web applications<br>• Application Security Threats and Problems<br>• Application Security Threat Detection and Mitigation<br>• Vulnerability Assessment and Penetration Testing (VAPT)<br>• OWASP Top 10 Vulnerabilities<br>**Assessment of Day 2(Quiz of 30 MCQ– 40 min)** |
| | **A N (14:00 to 17:00)** | | Web Application Security Threats and Attacks<br>Web Application Attack Detection<br>SSL/TLS and Digital Certificates<br>Capturing Web traffic<br>Authentication and Authorization<br>Network traffic AnalysisWeb Application VAPT |
| **Day 4**<br>**Thursday** | **FN (10:00 to 13:00)** | **Best Practices and Awareness** | • Security assessment strategy<br>o Risk Assessment<br>• SIEM (Security Information and Event Management) & EDR (Endpoint Detection & Response)<br>• Patch Management and Upgradation<br>• SOC (Security Operation Center)<br>• Technologies for anomaly detection in power system<br>• Solar, Wind, Colonial Pipeline, Black Energy 3 &Stuxnet, malware infection on Kudankulam Nuclear Power Plant (KKNPP) - Lessons Learnt<br>o<br>**Assessment of Day 3 (Quiz of 30 MCQ– 40 min)** |
| | **A N**<br>**(14:00 to 17:00)** | | Introduction to various standards such as NIST Cyber Security Framework/NERC-CIP/ISO27001/ISO27002/ISO 27019 etc.<br>NESCOR guide to vulnerability assessment |

|  |  |  |  |
|---|---|---|---|
| **Day 5**<br>**Friday** | **FN**<br>**(10:00 to 13:00)** | **Emerging Technologies** | - Data diode<br>- Artificial Intelligence and Machine Learning<br>- Malware Detection<br>- Industrial IoT<br>- Big Data<br>- Blockchain etc.<br>**Assessment of Day 4 (Quiz of 30 MCQ– 40 min)** |
|  | **A N**<br>**(14:00 to 16:30)** |  | - Address and interaction by esteemed guest 14:00 to 15:30 PM<br>**Final Assessment 15:45 – 16:30 PM (Quiz of 30 MCQs– 45 min)** |
|  | **16:30**<br>**to**<br>**17:00** | Overall feedback of the training program, Interaction with participants and Queries |  |

| **Program Schedule-I**<br>**Hands on** |  |  |  |
|---|---|---|---|
| **Program Title** |  | **Basic Level Hands-OnPracticeonCyberSecurityforPowerProfessionals** |  |
| **Duration** |  | **01Week** |  |
| **Participants** |  | **Power Sector Professionals** |  |
| **Mode of Training** |  | **Online** |  |
| **Day** | **Session in Hrs** | **Topics** | **Contents** |
| **Day1Monday** | **FN**<br>**(10:00to 12:00)** | Hardening Your System | **Inauguration (09:15-10:00Hrs)** |
|  |  |  | LAB: Hands on Malware Analysis<br>- Manual Tools to check malware<br>- Using File Hashes and Use of Virus Total to check against<br>- Existing malware |
|  | **AN**<br>**(14:30to 16:30)** |  | LAB: Operating System Hardening<br>- Understanding the concept of O/S Hardening against Vulnerabilities<br>- Lyn is Tool for Linux<br>- Windows Group Policy Edit Tool<br>- Openscap and Scap Work bench for Configuration Audit |
| **Day2Tuesday** | **FN(10:00 to 12:00)** | Finding Security Flows | Application Security<br>- Buffer Overflow Lab<br>- Integer Overflow Lab<br>- Privilege Escalation Labs |

|  |  |  |  |
|---|---|---|---|
|  | **AN(14:30to 16:30)** |  | Web Security<br>• Command Injection Lab<br>• SQL Injection Lab<br>• Cross-site Scripting Lab<br>• Cross-site Request Forgery Lab<br>• Session Hijacking Lab |
| **Day3Wednesday** | **FN(10:00 to 12:00)** | Network Security Lab | Network Labs<br>• Arp Spoofing Lab<br>• Packet Sniffing and Packet Analysis Lab<br>• Man-in-the-Middle Attack<br>• Network reconnaissance Lab |
|  | **AN (14:30 to 16:30)** |  | Wifi Network Lab<br>• Password sniffing in wifi network<br>• Reconnaissance on wifi network using air crack-ng<br>• Wifi password cracking lab |
| **Day4Thursday** | **FN (10:00 to 12:00)** | Intrusion Detection Lab | • Using Snort NIDS<br>• Using Zeek/Bro NIDS<br>• Visualization of network traffic data |
|  | **AN (14:30 to 16:30)** |  | • Host/End point Intrusion Detection Lab using Wazuh |
| **Day5Friday** | **FN (10:00 to 12:00)** | Deception Technology Labs and Organizational Security Policy Lab | • Honey pots for Threat Intelligence Collection Lab<br>• Use of Honey Tokens |
|  | **AN (14:30 to 16:30)** |  | Organization Level Security Policy – Requirements, Discussions and Formulation (Discussion Oriented Lab) |
|  | **16:30 To 17:00** | Overall feedback of the training program & Interaction with participants |  |

|  |  |  |  |
|---|---|---|---|
| **Program Schedule –(Intermediate-Level)** |  |  |  |
| **Program Title** |  | **Intermediate Level Cyber Security Training Program for Power Professionals** |  |
| **Duration** |  | **02 Weeks** |  |
| **Participants** |  | **Engineers from Power Utilities** |  |
| **Mode of Training** |  | **Hybrid** |  |
| **Day** | **Session in Hrs** | **Topics** | **Contents** |
| **Day 1 Monday** | **FN (10:00 to 12:00)** | Risk Driven Cyber Security and Cyber Security Maturity Model | Inauguration (09:15 - 10:00 Hrs)<br>Introduction to Risk Driven Cyber Security<br>• Risk Assessment Methodology<br>• Risk Driven Cyber Security Levels<br>• NIST CSF and 5 core functions |

| | | | |
|---|---|---|---|
| | **A N (14:30 to 16:30)** | | • NIST CSF Tiers and Maturity Models<br>• Cyber Security Maturity Model<br>• Assessment (Quiz of 15 MCQ) |
| **Day 2**<br>**Tuesday** | **FN (10:00 to 12:00)** | | Implementing IDENTIFY Function<br>• Asset Enumeration, Asset Management System<br>• Asset Vulnerability Assessment<br>• User Life Cycle<br>• Authentication and Authorization Technologies<br>• Threat Models based on Asset Vulnerabilities<br>• Assessment (Quiz of 15 MCQ) |
| | **A N (14:30 to 16:30)** | | |
| **Day 3**<br>**Wednesday** | **FN (10:00 to 12:00)** | Risk Driven Protection and Detection Techniques | Protection Function<br>• Configuration Management<br>• Malware Analysis<br>• Vulnerability Assessment and Pen-Testing<br>• Perimeter Security |
| | **A N (14:30 to 16:30)** | | • Risk Analysis and Appropriate Protection Functions<br>• Encryption, Hashing, Digital Signature<br>• Digital Certificates<br>• Web Application Protection<br>• Assessment (15 MCQ Questions) |
| **Day 4**<br>**Thursday** | **FN (10:00 to 12:00)** | | Detection Function<br>• Intrusion Detection and Intrusion Prevention<br>• Detecting Network based Attacks<br>• End Point Intrusion Detection and Protection |
| | **A N (14:30 to 16:30)** | | • Tools for Continuous Monitoring (SIEM, SOC)<br>• Escalation of Cyber Events<br>• Assessment (Quiz of 15 MCQ) |
| **Day 5**<br>**Friday** | **FN (10:00 to 12:00)** | Risk Driven Response | Response Function<br>• Response Planning<br>• Analysis and Forensics<br>• Mitigation Planning |
| | **A N (17:00 to 19:00)** | | • Ransomware Attack Response<br>• Supply Chain Attack Response<br>• Risk Assessment Update<br>• Communication and Escalation<br>• Assessment (Quiz of 15 MCQ) |
| **Day 6**<br>**Monday** | **FN (10:00 to 12:00)** | Recovery | • Ransomware Attacks<br>• Backup Process<br>• Recovery from Backups |
| | **A N (17:00 to 19:00)** | | • Drills for Recovery<br>• Communication<br>• Assessment (Quiz of 15 MCQ) |

|  |  |  |  |
|---|---|---|---|
| **Day 7**<br>**Tuesday** | **FN (10:00 to 12:00)** | Detailed Risk Assessment Methodology | • ISO27001 Risk Methodology<br>• System Architecture diagram<br>• Network Architecture Diagram |
|  | **A N (17:00 to 19:00)** |  | • Dependence Analysis (OEMs and other Service Providers)<br>• Other Risk Factors<br>• Assessment (Quiz of 15 MCQ) |
| **Day 8**<br>**Wednesday** | **FN (10:00 to 12:00)** |  | • Risk Matrix<br>• Threat Intelligence<br>• Likelihood Computation |
|  | **A N (17:00 to 19:00)** |  | • Risk Measurements<br>• Risk Based Security Profile<br>• Assessment (Quiz of 15 MCQ) |
| **Day 9**<br>**Thursday** | **FN (10:00 to 12:00)** | Need for Organizational Security Policy, Policy Adoption and Policy Implementation | Working Together in formulating Cyber Security Policy for your organization (Interactive) |
|  | **A N (14:30 to 16:30)** |  |  |
| **Day 10**<br>**Friday** | **FN (10:00 to 12:00)** |  | Discussing policy formulated, Discuss Implementability, Fitment to Risk Profile (Interactive) |
|  | **A N (14:30 to 16:30)** |  |  |
|  | **16:30 to** | Overall feedback of the training program & Interaction with participants |  |

|  |  |  |  |
|---|---|---|---|
| **Program Schedule-III**<br>**Hands on** |  |  |  |
| **Program Title** |  | **Intermediate Level Hands-On Practice on Cyber Security for Power Professionals** |  |
| **Duration** |  | **01 Week** |  |
| **Participants** |  | **Engineers from Power Utilities** |  |
| **Mode of Training** |  | **Hybrid** |  |
| **Day** | **Session in Hrs** | **Topics** | **Contents** |
| **Day 1**<br>**Monday** | **FN (10:00 to 12:00)** | Hardening Your System | Inauguration (09:15 - 10:00 Hrs) |
|  |  |  | LAB: Hands on Malware Analysis<br>• Manual Tools to check malware<br>• Using File Hashes and Use of Virus Total to check against<br>• existing malware<br>• Malware Analysis Tool Usage (Signature, Yara rules) |
|  | **A N (14:30 to 16:30)** |  | LAB: Operating System Hardening<br>• Understanding the concept of O/S Hardening against Vulnerabilities<br>• Lynis Tool for Linux<br>• Windows Group Policy Edit Tool |

| | | | |
|---|---|---|---|
| | | | • Openscap and Scap Workbench for Configuration Audit |
| **Day 2**<br>**Tuesday** | **FN (10:00 to 12:00)** | Finding Security Flows | Application Security<br>• Buffer Overflow Lab<br>• Integer Overflow Lab<br>• Privilege Escalation Labs |
| | **A N (14:30 to 16:30)** | | Web Security<br>• Command Injection Lab<br>• SQL Injection Lab<br>• Cross-site Scripting Lab<br>• Cross-site Request Forgery Lab<br>• Session Hijacking Lab |
| **Day 3**<br>**Wednesday** | **FN (10:00 to 12:00)** | Network Security Lab | Network Labs<br>• Arp Spoofing Lab<br>• Packet Sniffing and Packet Analysis Lab<br>• Man-in-the-Middle Attack<br>• Network reconnaissance Lab |
| | **A N (17:00 to 19:00)** | | Wifi Network Lab<br>• Password sniffing in wifi network<br>• Reconnaissance on wifi network using aircrack-ng<br>• Wifi password cracking lab |
| **Day 4**<br>**Thursday** | **FN (10:00 to 12:00)** | Intrusion Detection Lab | • Using Snort NIDS<br>• Using Zeek/Bro NIDS<br>• Visualization of network traffic data |
| | **A N (17:00 to 19:00)** | | • Host/Endpoint Intrusion Detection Lab using Wazuh |
| **Day 5**<br>**Friday** | **FN (10:00 to 12:00)** | Deception Technology Labs<br>and Organizational Security Policy Lab | • Honeypots for Threat Intelligence Collection Lab<br>• Use of Honey Tokens |
| | **A N (14:30 to 16:30)** | | Organization Level Security Policy – Requirements, Discussions and Formulation (Discussion Oriented Lab) |
| | **16:30 to 17:00** | Overall feedback of the training program & Interaction with participants | |

| **Program Schedule -IV** | | | |
|---|---|---|---|
| **Program Title** | **Advance Level Cyber Security Training Program for Power Professionals** | | |
| **Duration** | **02 Weeks** | | |
| **Participants** | **Engineers from Power Utilities** | | |
| **Mode of Training** | **Hybrid** | | |
| **Day** | **Session in Hrs** | **Topics** | **Contents** |
| **Day 1**<br>**Monday** | **FN (10:00 to 12:00)** | | Inauguration (09:15 - 10:00 Hrs)<br>Introduction to Cyber Security for Critical Infrastructure: |

|  |  |  |  |
|---|---|---|---|
|  |  | Cyber Security & Protocol Vulnerability | · ICS Security<br>· SCADA Security |
|  | **A N (14:30 to 16:30)** |  | · OSI Model<br>Assessment (Quiz of 15 MCQ) |
| **Day 2**<br>**Tuesday** | **FN (10:00 to 12:00)** |  | Understanding of Protocol Vulnerability:<br>· PCN Protocols<br>· Modbus |
|  | **A N (14:30 to 16:30)** |  | · IECTC 57 Protocol<br>Assessment (Quiz of 15 MCQ) |
| **Day 3**<br>**Wednesday** | **FN (10:00 to 12:00)** | Standards & Practices | Standards & Best Practices:<br>· NIST SP 80-161<br>· NERC - CIP (North American Electric Reliability Corporation Critical Infrastructure Protection) |
|  | **A N (14:30 to 16:30)** |  | · Incident response & incident reporting<br>Assessment (Quiz of 15 MCQ) |
| **Day 4**<br>**Thursday** | **FN (10:00 to 12:00)** |  | IEC 62443 Standards:<br>· Zones and Conduits<br>· Patch management |
|  | **A N (14:30 to 16:30)** |  | · Risk Assessment<br>· Security Requirement<br>Assessment (Quiz of 15 MCQ) |
| **Day 5**<br>**Friday** | **FN (10:00 to 12:00)** | Vulnerability & Malware | Device Level Vulnerability:<br>· Embedded Security<br>· Firmware Analysis<br>· Side Channel Attack |
|  | **A N (17:00 to 19:00)** |  | Malware Analysis:<br>· Static Analysis<br>· Dynamic Analysis<br>· Assessment (Quiz of 15 MCQ) |
| **Day 6**<br>**Monday** | **FN (10:00 to 12:00)** | VAPT | Vulnerability Assessment and Penetration Testing – I<br>· Vulnerability identification<br>· Common SCADA vulnerabilities<br>· Physical access<br>· Vulnerability scanning |
|  | **A N (17:00 to 19:00)** |  | · Server OS testing<br>· Patch levels<br>· Default and insecure configurations<br>Assessment (Quiz of 15 MCQ) |
| **Day 7**<br>**Tuesday** | **FN (10:00 to 12:00)** |  | Vulnerability Assessment and Penetration Testing – II<br>· Authentication and remote access<br>· Attacking ICS & Protocols<br>· Attacking standard services (HTTP, FTP) |

| | | | |
|---|---|---|---|
| | **A N (17:00 to 19:00)** | | · Attacking server OS<br>· Attacking ISC Protocols<br>· Attacking wireless communications<br>· Assessment (Quiz of 15 MCQ) |
| **Day 8**<br>**Wednesday** | **FN (10:00 to 12:00)** | Vulnerability Assessment & Forensic | Host, application and platform fingerprinting:<br>· Host and port scanning/Security considerations<br>· Scanning tools and techniques<br>· Scanning ICS/SCADA networks |
| | **A N (17:00 to 19:00)** | | · Vulnerability identification<br>· Common SCADA vulnerabilities<br>· Physical access<br>· Vulnerability scanning<br>Assessment (Quiz of 15 MCQ) |
| **Day 9**<br>**Thursday** | **FN (10:00 to 12:00)** | | · Server OS testing<br>· Patch levels<br>· Default and insecure configurations |
| | **A N (17:00 to 19:00)** | | SCADA Forensic:<br>· Network communications RF signal capture & analysis<br>· Sniffing network traffic |
| **Day 10**<br>**Friday** | **FN (10:00 to 12:00)** | | · Device functionality analysis<br>· Attacking ICS<br>· Attacking standard services (HTTP, FTP)<br>· Attacking server OS |
| | **A N (17:00 to 19:00)** | | · Attacking ISC Protocols<br>· Attacking wireless communications<br>· WEP/WPA2 password cracking<br>· Assessment (Quiz of 15 MCQ) |
| | **16:30 to 17:00** | Overall feedback of the training program & Interaction with participants | |

| **Program Schedule -IV**<br>**Hands on** | |
|---|---|
| **Program Title** | **Advance Level Hands-On Practice on Cyber Security for Power Professionals** |
| **Duration** | **01 Week** |
| **Participants** | **Engineers from Power Utilities** |
| **Mode of Training** | **Hybrid** |

| Day | Session in Hrs | Topics | Contents |
|---|---|---|---|
| **Day 1**<br>**Monday** | **FN (10:00 to 12:00)** | VAPT | Inauguration (09:15 - 10:00 Hrs)<br>LAB: Hands on Penetration Tests:<br>• Penetration Tests of Device and system (Pen Test)/ Physical test<br>• Facility for manually verifying the compliance against NERC CIP & IEEE 1686 Guidelines.<br>• Application layer protocol and its security extensions test |
| | **A N (14:30 to 16:30)** | | LAB: Hands on<br>• IP Scanning<br>• Port scanning tools |
| **Day 2**<br>**Tuesday** | **FN (10:00 to 12:00)** | Security Controls | Physical security & safety<br>• Categorization of system controls<br>• Identification/authentication/Authorization (IA&A)<br>• Remote access security and Encryption.<br>• Logical security |
| | **A N (14:30 to 16:30)** | | LAB: Hands on<br>• Concept of UTM box<br>• Firewall details<br>• Security Architecture<br>• Intrusion Detection system<br>• IDS/IPS (Introduction to Snort)<br>• Patch management |
| **Day 3**<br>**Wednesday** | **FN (10:00 to 12:00)** | Policy & practices | Strategic Planning and Building a Roadmap for Securing Critical Infrastructure<br>• Incident response<br>• Active Directory and group policy |
| | **A N (17:00 to 19:00)** | | ICS / SCADA Security Maturity Model<br>• Summary of good security practices, depth in defense<br>• Security solutions - Data Diodes, SIEM, SOC/NOC |
| **Day 4** | **FN (10:00 to 12:00)** | Securing Systems and Brainstorming Policies | An overview of the NIST Cyber security Framework for Critical Infrastructure (Part I) and (Part II) |
| | **A N (17:00 to 19:00)** | | Brain storming on relevance of NIST framework in Indian context specially for LDCs. |
| **Day 5**<br>**Friday** | **FN (10:00 to 12:00)** | Lessons Learned | Case study 2 - Ukrainian Power Grid (Black Energy 3)<br>Cyber attack &<br>Group discussions on lessons learned from Ukrainian Power Grid (BlackEnergy3) Cyber attack |
| | **A N (14:30 to 16:30)** | | Case study 1 - STUXNET &<br>Group discussions on lessons learned from<br>STUXNET WEP/WPA2 password cracking |
| | **16:30 to 17:00** | Overall feedback of the training program & Interaction with participants | |