SUBMISSION OF RESEARCH OBJECTIVE

1. Research Objective (Topic): **Establishing a Cyber Range tailored for LDC (Power Grid Operation) usage.**

2. **Lead of project-GM and above**: Sh. Gurmit Singh, GM (Logistics-IT) & CISO

3. **Co-Ordinator of Project**: Sh. Tapobrata Paul, Manager (Logistics-IT)

4. **Key Problem Areas**:
    i. As per CEA guideline Cyber mock drill must be conducted on regular periods. But non availability of proper simulation platforms, materials and grid operator centric guideline becomes a challenge.
    ii. RLDCs have integrated IT/OT technologies such as SCADA, URTDSM, REMCs, IT Data Centers and office computer network to ensure efficient and reliable management of Grid. However, this interconnectedness across also exposes them to cyber threats, including ransomware, phishing attacks, and insider threats. This huge infra needs to be simulated and tested against various threats and attack scenarios. No simulation software/application at present is there for testing the infrastructures and related changes.
    iii. Establishing and maintaining a Cyber Range comes with its own set of challenges, including the need for substantial initial investment in infrastructure and content development, ensuring the relevance and currency of training materials, and adapting to rapidly evolving cyber threats. Development of simulation attacks requires continuous research in this field.
5. **Objectives:**
    i. Create a Training Platform: Provide hands-on training to LDC personnel, including operators, IT/OT engineers, and cybersecurity professionals, to enhance their ability to detect, respond to, and recover from cyber-attacks.

ii. **Create a Testing/Simulation Platform:** Conduct realistic cyber-attack simulations to assess the resilience of LDC infrastructure, processes, and personnel against various threats.

iii. To assess the cyber security skill gap of IT/OT/Cybersecurity Engineers and the cyber security awareness gap of employees.

iv. Facilitate R&D activities aimed at developing innovative cybersecurity solutions and best practices tailored to the unique challenges of grid operation centers.

6. METHODOLOGY OF RESEARCH:

- Infrastructure Setup: Procure necessary hardware, software, and networking equipment or cloud based infrastructure to establish the Cyber Range infrastructure.
- Develop Simulation Environment: A realistic small replica of LDC infrastructure, including IT/OT devices and network architecture to simulate various cyber-attack scenarios and analyze results through developed software Environment.
- Content Development: Collaborate with subject matter experts to develop customized training content and simulation scenarios tailored to LDC cybersecurity challenges. Necessary software suite to be developed for cyber-attack simulation, detection tools, analysis tools, predictive tools for training/testing/R&D activities. The simulation scenarios should also include incident scenarios as per CCMP.
- Develop Training Modules: Customized software training modules covering cybersecurity fundamentals, threat intelligence analysis, incident response procedures, cyber forensics and best practices for securing critical infrastructure. Development of training content for baseline configuration of desktops, servers, and network devices, along with corresponding exercises.

- Develop Red Team/Blue Team Exercises: Develop simulated cyber-attack scenarios where Red Teams can attempt to breach the LDC defenses while Blue Teams defend against these attacks, fostering collaboration and enhancing response capabilities.
- Develop Training Metrics and Evaluation: Detailed documentation for training procedure, establish metrics to measure the effectiveness of training exercises and identify areas for improvement in cybersecurity posture as per latest research and development in the industry.
- Deployment of necessary tools for malware analysis, network analysis, and digital forensics, as well as the establishment of an environment for sandbox malware analysis.
- Developing self-paced basic cybersecurity awareness training content, advanced, and expert-level training, along with assessments. These will serve as training requirements for newly joined employees and annual compliance.
- Additional Development of an evaluation platform to assess cybersecurity awareness among employees through quizzes, tabletop exercises and phishing demonstrations, aiming to identify and address knowledge gaps effectively.

7. IMPLEMENTATION PLAN OF THE CYBER RANGE DEVLOPMENT:

- ERLDC, GRID-INDIA may engage any industry/institution as consultant for the project.
- The engaged consultant /institution shall prepare a detailed scope, roadmap and deliverables for the research project.
- As per consultant recommendations, necessary hardware/ infrastructure and software tools/licenses shall be procured for GRID-INDIA.
- As per consultant recommendation, System Integrator and Software developers may be engaged for setting up Cyber range and development of necessary customized software as per the detailed scope.

- Testing and acceptance can be done jointly by the engaged institution/ consultant and GRID-INDIA.
- The project can have many stages and Stage wise payment can be made to engaged consultant/institution as per target achieved.

8. Citation/References (Relevant Literature/Technical Papers):

- Advanced Research on Integrated Energy Systems Cyber Range: https://www.nrel.gov/security-resilience/cyber-range.html
- Yamin, Muhammad Mudassar, Basel Katt, and Vasileios Gkioulos. "Cyber ranges and security testbeds: Scenarios, functions, tools and architecture." Computers & Security 88 (2020): 101636.
- D. Mashima, M. M. Roomi, B. Ng, Z. Kalberczyk, S. M. Suhail Hussain and E. -C. Chang, "Towards Automated Generation of Smart Grid Cyber Range for Cybersecurity Experiments and Training," 2023 53rd Annual IEEE/IFIP International Conference on Dependable Systems and Networks - Supplemental Volume (DSN-S), Porto, Portugal, 2023, pp. 49-55, doi: 10.1109/DSN-S58398.2023.00024.