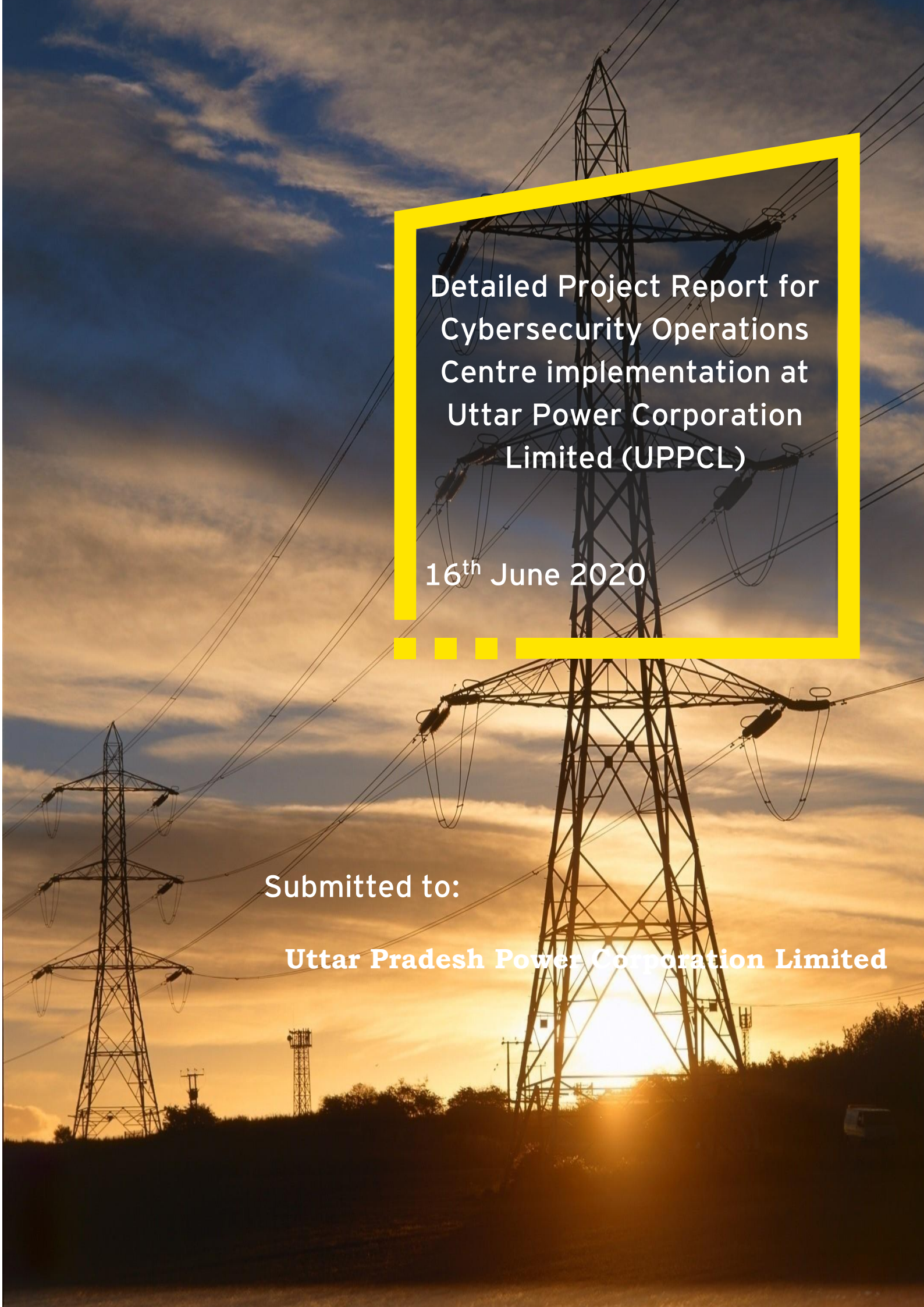

Detailed Project Report for Cybersecurity Operations Centre implementation at Uttar Power Corporation Limited (UPPCL)

16th June 2020

Submitted to:

Uttar Pradesh Power Corporation Limited

Disclaimer:

This report has been prepared by Ernst & Young LLP (hereinafter referred to as "Ernst & Young" or "EY") for Uttar Pradesh Power Corporation Limited (hereinafter referred to as "UPPCL") to provide Consultancy Services for Preparation of Detailed Project Report (DPR) for Cyber Security Operation Centre at Uttar Pradesh Power Corporation Limited.

The inferences/analyses made by Ernst & Young in this report are based on information collated through primary research, secondary research and our knowledge about the project and its objectives. Ernst & Young has taken due care to validate the authenticity and correctness of the information from various sources, however, no representations or warranty, expressed or implied, is given by Ernst & Young or any of its respective partners, officers, employees or agents as to the accuracy or completeness of the information, data or opinions provided to Ernst & Young by third parties or secondary sources. There is no independent verification has been done by EY.

Nothing contained herein, to the contrary and in no event shall Ernst & Young be liable for any loss of profit or revenues and any direct, incidental or consequential damages incurred by UPPCL or any other user of this report.

In case, the report is to be made available or disclosed to any third party, this disclaimer along with all the limiting factors must be issued to the concerned party. The fact that Ernst & Young assumes no liability whatsoever, if for the reason any third party is led to incur any loss for acting upon this report, must be brought to the notice of the concerned party.

Errors and Omissions:

When reading this document if you identify any errors or omissions please advise the author in writing, in 15 calendar days, giving a brief description of the problem, its location within the document and your contact details.

Confidentiality:

This report is intended solely for the information and use of the management of UPPCL and is not intended to be and should not be used by anyone other than these specified parties.

Ernst & Young therefore assumes no responsibility to any user of the report other than UPPCL. Any other persons who choose to rely on our report do so entirely at their own risk.

Table of Contents

List of Tables

1 Background

1.1 Introduction

Uttar Pradesh being the one of the largest State in India is also one of the most populous state of the country with its administrative capital Lucknow. With the levels of literacy rate of around at 70 % the state has abundant availability of quality human resource. It has the abundance of potential as destination for investments in manufacturing, tourism and Infrastructure services.

Power sector is the critical infrastructure element required for the smooth functioning of the economy. Efficient, reliant and sustainable power is essential to stimulate growth and prosperity in the state. The availability of the reliable, quality and affordable power can ensure growth of all sectors of the economy being it agricultural, industrial and others. Towns of Kanpur, Varanasi, Allahabad, Gorakhpur, Meerut, Aligarh, Moradabad, Muzaffarnagar, Saharanpur and Jhansi are known for their industrial importance in the state as well as at the national level.
Uttar Pradesh was one of the first state to embark upon economic and structural reforms in power sector. GoUP had taken key structural reforms and created entities , Uttar Pradesh Power Corporation Limited (2000) , Kanpur Electricity supply Company , KESCO (2000) , Purvanchal Vidyut Vitran Nigam Limited , PuVVNL – Varanasi (2003) , Madhyanchal Vidyut Vitran Nigam Limited , MVVNL- Lucknow (2003) , Paschimanchal Vidyut Vitran Nigam Limited , PaVVNL - Meerut (2003) and Dakshinanchal Vidyut Vitran Nigam Limited , DVVNL- Agra (2003).

UPPCL has the following major online systems in place-

- **Urban Online Billing:** To bring efficiency and transparency in operations, an online system for billing and collection consisting 17 modules is deployed in 168 towns across UP for a consumer base of 7.5 Million. The web applications have been hosted at on-premise Data Centre (DC) with replicated data in the Disaster Recovery Centre (DRC), and are accessed by various divisions, circle, sub-division and other offices situated at different locations in 168 towns across the state over WAN environment.
- **Mobile Applications:** Various mobile applications (e-Nivaran, e-Sanyojan, FAME) for urban and rural consumers have been developed for improving efficiency, revenue and easy functioning. These apps are integrated with urban and rural online billing systems and various payment service providers.
- **Customer Care Centre for urban Consumers:** Customer Care Centres for consumers are established in 4 Discoms to take care of the grievances and faster redressal. Consumer complaints are registered/tracked/resolved through 1912 (Toll Free Number). This system is integrated with urban online system and rural online billing system.
- **Web Self Service**: To facilitate its consumers UPPCL provides online payment, trust billing and load enhancement features to its users.
- **Prepaid Meter Online Recharge-** Integration is in place to do online recharge prepaid meter installed.

- **GIS and Network Analysis Solution** – GIS system is in place which includes asset mapping and consumer indexing. UPPCL also keeps updating the GIS database through incremental surveys of consumers and assets to accurately carry out energy accounting. To complement the GIS, GIS based network analysis system is implemented to be able to accurately carry out network studies and optimise deployment of network elements.
- **Integrations with Other Government Portals/Apps** – Billing system has been integrated with Centre for E-Governance and (Customer service centers)CSCs for bill payment, Udyog Bandhu, CM Dashboard, Energy Audit Module etc
- **Other Integrations with UPPCL** – Official website of www.uppcl.org has various integrations such as Energy Accounting Directory, Commercial Statements, Personal Information System, Jansunwai, Disciplinary Proceedings, Feeder wise Supply Hours, Daily Supply Hours, Court Case Monitoring etc.

1.2 About UPPCL

Uttar Pradesh Power Corporation Limited (UPPCL), is a company registered under the provisions of Companies Act 1956 / 2013 and is a fully owned entity of Government of Uttar Pradesh.

Besides being the holding company for Power Generation and Transmission entities, UPPCL is also the holding company for five DISCOMS namely Paschimanchal Vidyut Vitaran Nigam Limited (PVVNL), Purvanchal Vidyut Vitaran Nigam Limited (PuVVNL), Madhyanchal Vidyut Vitaran Nigam Limited (MVVNL), Dakshinanchal Vidyut Vitaran Limited (DVVNL) and Kanpur Electricity Supply Company (KESCO).These DISCOMs are responsible for supplying of electricity to the consumers and to maintain the 33/11, 11/0.433 KV, substations, 33/11 kV/LT network of the area, receiving electricity supply from higher voltage system, distribute it to its consumers, record their consumption, issue electricity bills according to applicable tariff and realize the revenue. Various divisions of the DISCOMs are also responsible to release new connections and from time to time extend and improve its distribution network and control the line losses of electricity, technical as well as commercial and various other related activities.

The Company is engaged primarily in the business of distribution of Electricity. It has been vested with the distribution assets, interest in property, rights and liabilities of the erstwhile UPSEB necessary for the business of distribution in its area of distribution comprising of all districts of Uttar Pradesh.

The above 5 Companies have been given the status of a Distribution licensee as per Section14 of the Electricity Act 2003. In order to fulfil the obligations of the Distribution licensee as mandated under the provision of Uttar Pradesh State Electricity Reforms Transfer Scheme 2012 and Electricity Act 2003, the main objects to be pursued by the company are:

- To undertake the activities of distribution to all consumers irrespective of the voltage, provision, supply, wheeling, purchase, sale, import, export and trading of electricity,

introduce open access in distribution as per the Electricity Act 2003 and/or the directions of the regulator.

- To plan, develop, acquire, establish, construct, erect, lay, hire, lease, buy, sell, operate, run, manage, maintain, enlarge, alter, renovate, modernize, work and use a power distribution system network in all its aspects including amongst others various voltage lines and associated sub -stations, including distribution centers, cables, wires, accumulators, plants, motors, meters, apparatus, computers and materials connected with sub-transmission, distribution, supply of electrical energy, ancillary services, telecommunication and telemetering equipment.
- To tender, finalize and execute Power Purchase Agreements and other agreements for sale or purchase of electricity with generating companies, trading companies, other distribution companies, Central and State generating authorities, departments or companies, societies, other States, utilities, Independent Power Producers and other Persons.
- To undertake Rural Electrification schemes in the licensed area.
- Any other work incidental to the objectives & functions of the company.

The details of 5 DISCOMS are as follows;

DISCOMS	RAPDRP PART A		Non-RAPDRP	
	No. of Consumer Served *	District Served	No. of Consumer Served*	District Served
Dakshinanchal Vidyut Vitran Nigam Ltd (DVVNL)	1093589	19	3286962	21
Madhyanchal Vidyut Vitran Nigam Ltd (MVVNL)	1815243	17	4126303	19
Purvanchal Vidyut Vitran Nigam Ltd (PuVVNL)	1229043	19	5573860	20
Paschimanchal Vidyut Vitran Nigam Ltd (PVVNL)	2421582	13	3321032	12
Kanpur Electric Supply Company (KESCO)	601819	1	Not in scope	
Total	**7161276**	**69**	**16308157**	**72**

Table 1 : Details of Consumers and Districts

***As per 2018 data**

Discoms	Zone	Circle	Distribution Division	SDO	Test Division
Dakshinanchal Vidyut Vitran Nigam Ltd (DVVNL)	6	28	77	190	23
Madhyanchal Vidyut Vitran Nigam Ltd (MVVNL)	6	29	105	205	27
Purvanchal Vidyut Vitran Nigam Ltd (PuVVNL)	6	30	96	194	22
Paschimanchal Vidyut Vitran Nigam Ltd (PVVNL)	6	29	96	195	28
Total	**24**	**116**	**374**	**784**	**100**

Table 2 – Details of RAPDRP PART-A and Non-RAPDRP Offices

1.3 Mission of UPPCL

Uttar Pradesh Power Corporation Ltd. (UPPCL), with a vision to provide, uninterrupted power supply to every consumer of the state is now looking forward to increasing the consumer base as well as increasing the revenue by incorporating new technology, process and procedure. The mission of Uttar Pradesh Power Corporation Limited (UPPCL) is to ensure reliable quality of power to its customers at competitive prices. The UPPCL is committed to achieving this mission through:

- Provide cost efficient good quality electricity to all categories of consumers for economic development/social uplift of the State.
- Make the energy sector commercially viable so that it ceases to be burden on the state budget; and
- Protect the investment of the consumers.

2 Objective

Cyber security is the body of technologies, processes and practices designed to protect networks, computers, programs and data from attack, damage or unauthorized access. In a computing context, security includes both cyber security and physical security. Ensuring cyber security requires coordinated efforts throughout an information system. It includes collection of policies, security concepts, security safeguards, guidelines, risk management approaches, tools, training, best practices, assurance and technologies that can be used to protect the cyber environment, organization and user's assets. Organization and user's assets include connected computing devices, personnel, infrastructure, applications, services, telecommunications systems, and the totality of transmitted and/or stored information in the cyber environment.

The mission of any Security Operations Centre is to detect and respond to cyber-attacks that place a client's high value assets at risk. CSOC approach, which will be mirrored at UPPCL, accomplishes this by maintaining focusing on high value assets and being use case and intelligence led. Some vendors adopt a top down approach (Risk focused), whilst others adopt a bottom up approach (Threat Focused).

2.1 Purpose

In order to streamline comprehensive information security monitoring and compliance, UPPCL on behalf of its DISCOMs proposes to implement and maintain Cyber Security Operations Center (CSOC) for its Information Technology setup, comprising critical infrastructure at DC, DR and other IT locations including third party Data centre hosting site comprising of existing as well as other site which may come up in the future. UPPCL intends to implement Cyber-Security Operation Centre (CSOC) for information assets at Primary Data Center and DR site. UPPCL expect Service provider to provide full-fledged Services including but not limited to design, supply, implementation, configuration, customization, integration, monitor, manage, backup, documentation, training, warranty support, post warranty maintenance support, back to back arrangement with OEM and any other activities

related to or connected to the Information Technology / Cyber security solutions, devices & technologies. UPPCL also has co-located Data Center/DR Site/Web servers from third party Datacenters and the System Integrator (SI) is expected to provide security services for co-located Datacenter setup as well.

UPPCL has its Primary Data Center at Lucknow with DR site at Noida. UPPCL has implemented various applications at DC and DR in a centralized environment and few applications are hosted on third party Data-centre and public cloud.

The proposed CSOC facility is to be equipped with set of tools such as Security Information and Event Management Tool (SIEM), Incident Management tool, Anti-APT, PIM, etc. and Security Intelligence services for better security monitoring and response capabilities.

UPPCL will be required following list of activities to establish CSOC:

a. Must have Security Monitoring of attacks into/on/against UPPCL's IT assets
b. Ability to manage security, configuration, availability, performance and fault management, advisory for the security devices and its software stipulated in scope.
c. Ability to ensure Malware Scanning / Protection/ Presentation /Reporting as required by UPPCL including total Anti-APT solution.
d. Ability to Provide proactive threat intelligence and threat hunting.
e. Must have Vulnerability Assessment & Penetration Testing for critical devices/ servers /applications/solutions on quarterly basis / as and when required by UPPCL and its DISCOMs and provide solution for closure.
f. Must have risk assessment and mitigation, protection, execution support for the Security solutions, devices, software and tools under the scope of CSOC.
g. Ability to ensure adherences to UPPCL's Information Security Policy and Cyber Security Policy.
h. Ability to Ensure adequacy, appropriateness and concurrency of various policies as per the requirement of regulatory authorities and Government of India Security authorities, IT Act 2000 and subsequent amendments and guidelines in place.
i. Ability to provide forensics support as per the requirement in case of any incident or as and when required.

As proposed, the security solutions have to be implemented in the UPPCL premises and the procured security solutions to be integrated with already existing SIEM tool. The proposed CSOC service should cover security event correlation, monitoring, incident management and providing proactive security alert and remediation. The selected vendor will be playing the role of Managed Security Services Provider (MSSP) of UPPCL as well as System Integrator (SI) for all the security solutions/tools.

2.2 CSOC Coverage

The coverage of CSOC will be in following areas:

- DC Lucknow
- DR Noida
- Field Offices

3 Scope of Work

3.1 Functional Principles

The Intent for implementing a CSOC at UPPCL is covered in the below functional principles:

a. **Detection of Information Security Threat & Prevention of Impact/ Breach:** The CSOC should be able to identify information security threats/ vectors targeting UPPCL's environment and prevent impact or breach due to these through implementation of adequate security mechanisms.

b. **Incident Management:** Reporting and logging of information security incidents through the use of appropriate ticketing tools. Track and monitor the closure of these information security incidents and Escalation of these incidents to appropriate teams/ individuals in the UPPCL if required.

c. **Continuous Improvement:** Continuously improve CSOC operations.

3.2 Cyber Security Operations Centre

a. CSOC operation is for a period of 5 years. The Bidder shall supply, install, customize, integrate, migrate, test, and troubleshoot the in-scope solutions.

b. Solutions to be implemented:

i. Threat Intelligence Platform and Automated incident response solution
ii. Vulnerability Management and penetration Testing
iii. Situational Awareness/Network Forensics Security Analytics solution
iv. Governance and Risk and Compliance
v. UEBA (User and Entity Behaviour Analysis)
vi. DDoS (Distributed Denial of Service)
vii. Brand / Dark Web Monitoring Security Intelligence Services
viii. Web Application Firewall and Web Application Scanner
ix. Database Activity Monitoring (DAM)
x. Deception Solution.
xi. Service Desk – Ticketing tool.

c. Implementation Procedure:

The implementation is to be done in two phases:

Phase 1 – Security Threat intelligent Platform Operations Control Centre setup with integration of critical devices and applications with existing SIEM tool.

Phase 2 – Implementation and Integration of other tools/services mentioned above with the CSOC.

3.3 Volume and Log Retention

Efforts for the solution is based on the following:

- Volume of logs generated from the devices in scope per day. This will be referred as Events Per Second (EPS)
- Retention period of logs
- Estimated for the log volume listed for the devices in scope is 10000 EPS (approx.).
- Solution should be scalable upto 20000 EPS.

3.4 Representative Team Structure

S.No.	Position	Responsibility
1	Project Manager	• Project Co-ordination • Define Strategy for Security Operations Centre • Approve/Prioritize use cases
2	SIEM SME	• SIEM Architecture Design & Implementation
3	SOC Lead L3	• Incident Communications • Metrics Collection and Reporting
4	SOC Lead L3	• Major Breach Support • Advanced Malware Analysis • Root cause identification, Incident containment, eradication and remediation
5	Analyst L2	• Basic Malware Analysis • Second Level incident validation • Proactive Log analysis/threat hunting
6	Analyst L1	• First Level triage and response to alerts/notifications • Close routine low severity incidents

4 Benefits

The actions SOCs perform have significant effects on business outcomes for a few key reasons. As cybersecurity is increasingly crucial, brands that embrace more protective measures find themselves ahead of the game. Within their organizations themselves, SOCs can have a positive impact due to their focus and expertise. Here are some of the specific benefits of the security operations centre, in whatever form it may come:

- **Centralizing the display of assets** – A real-time, holistic view of the software and processes that help run an organization makes it easy to detect problems as they occur or sooner. Even with dispersed materials, the centralized, non-stop visualization SOC monitoring offers is highly advantageous in maintaining smooth operations.
- **Solidifying client and employee trust** – Consumers and employees alike want to know their information will be safe once they offer it to their company of choice. Taking strict measures to prevent data loss is one of the best ways to improve and maintain brand integrity in the long run.
- **Collaborating across departments and functions** – SOCs are unique in that they are a team of highly trained individuals working toward a common goal. As they proceed during cybersecurity incidents, they require other departments to work similarly to operate efficiently. Within these instances, SOCs help with coordinating and communicating the organization as it strives to resolve the problem collectively.
- **Maximizing awareness to minimize costs** – Overall, the most significant benefit of a SOC is the increasing your ability to control all systems and reduce the potential for losses of data, contributing to higher returns on investment to prevent breaches. SOCs help maintain the integrity of sensitive information, save money in the long run and assist in avoiding the cost of significant recoveries from theft or fraud.

5 Costing

Total costing of the project with details	
Name of the Project & Project No.	Cyber Security Operation Centre
Date of Start of Project	2020
Scheduled Date of Completion	2025
Estimated Cost (Rs. Crs) at start of project	55.5
Cost Escalation / variation with reasons, if any	NA
Proposed Funding (Equity, Loan, Grant details)	Equity
Scheduled Date of Completion	2025
Delay & reasons, if any	NA

6 Duration

The estimated time period to complete the activity is by 2025 i.e. the duration is for **60 Months.**