Clarification-I dated 02.07.2024 for Hiring of Threat Intelligence services in I3SOC under Spec. No. CC/NT/S-IT/DOM/A06/24/07591

Sr.No.	Section	Clause Description	Query	POWERGRID Clarification
1	**12.0.0 CONTRACT PERFORMANCE GUARANTEE – CONDITIONS OF CONTRACT**	12.0.1 The Contractor shall, within twenty-eight (28) days of the notification of award, provide a performance security for the due performance of the Contract in the amount equivalent to Ten percent (10%) of the Contract Price, with a validity up to ninety (90) days beyond the Defect Liability Period.	Dear Sir, Performance Security of 10% of total contract value has been asked whereas we have participated in various government bids , where security deposit has been asked only 3% of total contract value. Even we have recently participated in a bid of PGCIL where Performance Security was asked for 5% of total contract value, a bid document is enclosed for your reference. **Hence we request you to please amend the clause as, performance security for the due performance of the Contract in the amount equivalent to three percent (3%) of the Contract Price.**	refer Amendment-II to the Bidding Document.
2	B. Threat Intel Web Portal Capabilities:	14. The threat intelligence solution shall provide a cloud-based sandbox for detonating and analysis of suspicious files with 200 files/analysis per day.	Manual Sandbox analysis requires a lot of compute and bandwidth consumption and based upon our experience customers need to have max of 250 files analysis per month. Therefore, request you to consider below updated statement: The threat intelligence solution shall provide a cloud-based sandbox for detonating and analysis of suspicious files with around 200 files analysis per month.	TS shall prevail
3	C. Dark Web Intelligence Requirements	4. The offered solution must have a capability to create a Threat Actor and Malware heat map or attributions specific to POWERGRID based on the POWERGRID defined watch lists.	We need telemetry from PowerGrid to have this attribution therefore request to have this changed to Powergrid related industry instead of power grid itself. Please find below updated statement: The offered solution must have a capability to create a Threat Actor and Malware heat map or attribution specific to POWERGRID or POWERGRID based industry based on the POWERGRID defined watch lists.	TS shall prevail
4	C.Dark Web Intelligence Requirements	10. The solution must be able to look for Exploit Proof of Concepts on selective technologies & sources like Dark Web and Underground forums to visualize and reduce Zero-day exploits.	As per our understanding, requirement is to have information around latest vulnerabilities and its exploit information (either existing (or validated) or unknown (zero Day)) irrespective of this information being displayed in Threat Intel dashboard or Deep Dark web sources. Ideally information on deep dark web is usually false information. Therefore, request to cater below updated statement: The solution must be able to look for Exploit Proof of Concepts covering both validated and unknown exploits along with details and severity assigned to it.	TS shall prevail