दि न्यू इन्डिया एश्योरन्स कंपनी लिमिटेड
(भारत सरकार का उपक्रम)
THE NEW INDIA ASSURANCE COMPANY LTD.
(Govt. of India Undertaking)
पंजीकृत एवं प्रधान कार्यालय : न्यु इन्डिया एश्योरन्स बिल्डिंग, 87, महात्मा गांधी मार्ग, फोर्ट, मुंबई - 400 001.
Regd. & Head Office : New India Assurance Bldg., 87, M.G. Road, Fort, Mumbai - 400 001.
CIN No. L66000MH1919GOI000526

Phone : 022 2270 8100
022 2270 8400
Website : www.newindia.co.in

CORRIGENDUM-1

Re: REQUEST FOR PROPOSAL (RFP) FOR SELECTION OF MANAGED SECURITY SERVICE PROVIDER (MSSP) FOR SECURITY OPERATIONS CENTRE.

Bid Number: GEM/2025/B/6454339 Dated: 16-07-2025

SN	Page No.	Clause	Description in RFP	Changed To
1	12	16.1) PROJECT IMPLEMENTATION	Provisioning of secure and reliable network connectivity between the organization's premises and the Security Operations Center (SOC) ensuring adequate bandwidth, redundancy, and low latency to support continuous log ingestion, monitoring, and incident response activities.	Provisioning of secure and reliable MPLS-based network connectivity between the organization's premises and the Security Operations Center (SOC), ensuring adequate bandwidth, redundancy, and low latency to support continuous log ingestion, real-time monitoring, and incident response activities. The organization currently uses MPLS services from providers such as BSNL and SIFY. VPN-based connectivity will not be considered due to performance, reliability, and security considerations.
2	14	Scope Of Work -> Security Operations Centre	The bidder shall host the Security Operations Centre (SOC) for the NIA exclusively within a MeitY empaneled Government Community Cloud (GCC) data center. The proposed SOC infrastructure, including all associated tools, platforms, and data, must reside within the GCC environment to ensure compliance with Government of India cloud hosting guidelines and data sovereignty requirements. No part of the SOC services shall be hosted on commercial or non-GCC cloud environments. All data– including system logs, access logs, activity logs, audit	The bidder shall host the Security Operations Centre (SOC) for the NIA. The SOC infrastructure and its associated tools and platforms must be deployed in an environment that ensures physical or logical isolation and control, adhering to robust security standards for data protection and operational integrity within India. All data including system logs, access logs, activity logs, audit logs, and related metadata must be stored exclusively on servers located within India.

SN	Page No.	Clause	Description in RFP	Changed To
			logs, and related metadata is stored exclusively on servers located within India	
3	24	Threat Intelligence	To ensure data retention and archival policies are configured in CTI as per NIA's compliance requirements.	Removed
4	29	Training	For each deliverable installed, the supplier should train the designated NIA's technical team members in all aspects of delivered products to enable them to effectively operate and perform administration of the total system.	For each deliverable installed, the bidder/OEM shall provide a high-level knowledge transfer and orientation to the designated NIA's technical team members, covering all aspects of implemented solutions.
5	46	Technical Evaluation	The Bidder must have successfully implemented or managed MSSP model or on premise Security operation center (*SOC) during last 5 years in organizations like PSU/Central Government/State Government/Regulatory Bodies/ BFSI* Sector Firms in India. The SOC must be currently operational and running 5 and above clients - Score of 15 marks More than 3 and below 5- Score of 10 marks More than 1 and below 3 - Score of 5 marks Note: Bidder must have provided any of the one solutions (SOAR, UEBA) along with the SIEM. * BFSI must be an organization having minimum of 500 branches or Rs. One Lakh Crores Business in India.	The Bidder must have successfully implemented and managed MSSP model or on premise Security operation center (*SOC) during last 5 years in organizations like PSU/Central Government/State Government/Regulatory Bodies/ BFSI* Sector Firms in India. The SOC must be currently operational and running 5 and above clients - Score of 15 marks More than 3 and below 5- Score of 10 marks More than 1 and below 3 - Score of 5 marks Note: Bidder must have provided any of the one solutions (SOAR, UEBA) along with the SIEM. * BFSI must be an organization having minimum of 500 branches or Rs. One Lakh Crores Business in India.

SN	Page No.	Clause	Description in RFP	Changed To
6	46	Technical Evaluation	The Bidder for SIEM must have supplied a SIEM solution in PSU/Central Government/State Government/Regulatory Bodies/ BFSI* Sector Firms in India. Supply Experience Each reference of 15000 EPS and above with minimum 500 branches/ offices - 5 marks Each reference of 7500 EPS and above with minimum 500 branches/ offices - 4 marks Each reference of 5000 EPS and above with minimum 500 branches/ offices - 3 marks Note: Max. 3 references will be considered. * BFSI must be an organization having minimum of 500 branches or Rs. One Lakh Crores Business in India.	The Bidder for SIEM must have implemented and managed a SIEM solution in PSU/Central Government/State Government/Regulatory Bodies/ BFSI* Sector Firms in India. Supply Experience Each reference of 15000 EPS and above with minimum 500 branches/ offices - 5 marks Each reference of 7500 EPS and above with minimum 500 branches/ offices - 4 marks Each reference of 5000 EPS and above with minimum 500 branches/ offices - 3 marks Note: Max. 3 references will be considered. * BFSI must be an organization having minimum of 500 branches or Rs. One Lakh Crores Business in India.
7	47	Technical Evaluation	The Bidder for SOAR must have supplied a SOAR solution with minimum 5 Analyst/ User licenses in PSU/Central Government/State Government/Regulatory Bodies/ BFSI* Sector Firms. Supply Experience 5 and above clients - Score of 10 marks More than 3 and below 5- Score of 5 marks More than 1 and below 3 - Score of 3 marks Note: *BFSI must be an organization having minimum of 500 branches or Rs. One Lakh Crores Business in India.	The Bidder for SOAR must have implemented and managed a SOAR solution with minimum 5 Analyst/ User licenses in PSU/Central Government/State Government/Regulatory Bodies/ BFSI* Sector Firms. Supply Experience 5 and above clients - Score of 10 marks More than 3 and below 5- Score of 5 marks More than 1 and below 3 - Score of 3 marks Note: *BFSI must be an organization having minimum of 500 branches or Rs. One Lakh Crores Business in India.

SN	Page No.	Clause	Description in RFP	Changed To
8	48	Technical Evaluation	The Bidder must have supplied a UEBA solution in PSU/Central Government/State Government/Regulatory Bodies/ BFSI* Sector. Supply Experience: Each reference of 15,000 endpoints and above - 5 marks Each reference of 10,000 endpoints and below 15,000 endpoints -3 marks Note: Max. 2 references will be considered. * BFSI must be an organization having minimum of 500 branches or Rs. One Lakh Crores Business in India.	The Bidder must have implemented and managed a UEBA solution in PSU/Central Government/State Government/Regulatory Bodies/ BFSI* Sector. Supply Experience: Each reference of 15,000 endpoints and above - 5 marks Each reference of 10,000 endpoints and below 15,000 endpoints -3 marks Note: Max. 2 references will be considered. * BFSI must be an organization having minimum of 500 branches or Rs. One Lakh Crores Business in India.
9	49	Technical Evaluation SL7 Evaluation Parameters	The bidder shall possess OEM-certified resources for the proposed SIEM, SOAR, and UEBA solutions. Marks will be awarded based on the number of such certified professionals, as detailed below: More than 15 certified resources - 15 marks Between 10 and 15 certified resources - 10 marks Between 7 and 10 certified resources - 5 marks Note: All certified professionals must be on the direct payroll of the bidder at the time of bid submission and during the course of the project.	The bidder shall possess OEM-certified resources for the proposed SIEM, SOAR solutions. Marks will be awarded based on the number of such certified professionals, as detailed below: More than 15 certified resources 15 marks Between 10 and 15 certified resources - 10 marks Between 7 and 10 certified resources - 5 marks Note: All certified professionals must be on the direct payroll of the bidder at the time of bid submission and during the course of the project.
10	49	Technical Evaluation SL7 Documents To Be Shared	An undertaking on the bidder's official letterhead must be submitted, clearly specifying the number of employees holding OEM certifications for the proposed SIEM, SOAR, and UEBA solutions. The undertaking should also	An undertaking on the bidder's official letterhead must be submitted, clearly specifying the number of employees holding OEM certifications for the proposed SIEM, SOAR solutions. The undertaking should also confirm that all such

SN	Page No.	Clause	Description in RFP	Changed To
			confirm that all such certified professionals are on the direct payroll of the bidder.	certified professionals are on the direct payroll of the bidder.
11	62	ANNEXURE - 2: TECHNICAL SPECIFICATION Security Information and Event Management SIEM Point 61	The solution must generate and alert when a new service appears on the network or when new assets appear where they shouldn't or are not planned.	The solution must integrate with external asset discovery tools or vulnerability scanners to generate alerts when new services or unplanned assets appear on the network.
12	68	ANNEXURE - 2: Security Orchestration and Automation (SOAR) Point 36	The solution should be capable to provide automated detailed post incident report about all the actions taken, root cause, collaborative actions/chats etc.	The solution should be capable to provide automated detailed post incident report about all the actions taken, root cause etc.
13	83	Security Information & Event Management (SIEM). 1.10	The Bidder has to document RCA for all incidents, ensuring accurate and detailed records are maintained. Document lessons learned and integrated them into SOC processes, training, and threat detection strategies.	The Bidder has to document RCA for all P1(Priority 1) incidents as well as for any other incidents upon request by NIA, ensuring accurate and detailed records are maintained. Document lessons learned and integrated them into SOC processes, training, and threat detection strategies.
14	118	ANNEXURE - 7: NON-DISCLOSURE AGREEMENT (FORMAT) -> Term	This Agreement shall remain in effect for the duration of the business relationship and for a period of ten (10) years after the expiration/ termination of this Agreement. The obligations of confidentiality shall survive the expiration/termination of this Agreement.	This Agreement shall remain in effect for the duration of the business relationship and for a period of three (3) years after the expiration/ termination of this Agreement. The obligations of confidentiality shall survive the expiration/termination of this Agreement.
15	143	ANNEXURE - 16: ABBREVIATIONS	Addition	P1 - Priority 1 P2 - Priority 2 P3 - Priority 3 P4 - Priority 4

CHIEF MANAGER