Government eProcurement System

Government eProcurement System

Published Corrigendum Details

Date : 19-Dec-2025 04:14 PM

Print

Organisation Chain :	Council of Scientific and Industrial Research||IGIB-Delhi - CSIR||Purchase-IGIB - CSIR
Tender ID :	2025_CSIR_258127_1
Tender Ref No :	IGIB/7-2NC/299/25-26(1302)
Tender Title :	Supply, Installation and Commissioning and Testing of Next Generation Firewall NGFW ,etc
Corrigendum Type :	Technical Bid

Corrigendum Document Details

Corr.No.	Corrigendum Title	Corrigendum Description	Published Date	Document Name	Doc Size(in KB)
1	Corrigendum	Modified specification of Supply, Installation and Commissioning and Testing of Next Generation Firewall NGFW ,etc	19-Dec-2025 04:14 PM	corr.pdf	552.59

सीएसआईआर
CSIR
भारत के नवाचार स्रोत
The Innovation Engine of India

IGIB
INSTITUTE OF GENOMICS
& INTEGRATIVE BIOLOGY
Genomics Knowledge Partner

सी.एस.आई.आर.–जीनोमिकी और समवेत जीवविज्ञान संस्थान
(वैज्ञानिक तथा औद्योगिक अनुसंधान परिषद्, भारत सरकार)
CSIR-Institute of Genomics & Integrative Biology
(Council of Scientific & Industrial Research, Govt. of India)

CORRIGENDUM

IGIB/7-2NC/299/25-26(1302) 19.12.2025

A Open tender in Two bid system for Supply, Installation & Commissioning and Testing of Next Generation Firewall NGFW, etc. Against Tender ID No. 2025_CSIR_258127_1 on 05.12.2025.

Based upon the pre bid meeting held on 15.12.2025 at 03:00 PM at IGIB, Mall Road the specification of the NIT are modified and are attached herewith for information (Annexure-A).

All the other T&C & specification of the NIT remain the same & continue to be part of NIT.

Store Purchase Officer

• मुख्य कार्यालयः–उत्तर परिसर, माल रोड, दिल्ली–110007
HEAD OFFICE:- NORTH CAMPUS, MALL ROAD, DELHI-110007 • Tel. : 91-11-27002200-201 • Fax : 91-11-27667471
Telefax : 91-11-27662407-08, 27662099 • E-mail : info@igib.res.in • Website : www.igib.res.in
• दक्षिण परिसर, मथुरा रोड, नई दिल्ली-110025
SOUTH CAMPUS, MATHURA ROAD, NEW DELHI-110025 • Tel : 26932421-23, 29879487-88

Annexure-A

Corrigendum - Tender No. IGIB/7-2NC/299/2025-26(1302)

Page No.	Existing Specification	Should be read as following
53 (Scope of Work)	3. Implementation & Migration should be done by OEM Engineer.	3. Implementation & Migration shall be performed by OEM-authorized engineers, or by engineers certified by the OEM and employed by the bidder, with OEM approval for critical configuration steps.
56 (Other Features & Compliance)	7. The Firewall solution offered must be Common Criteria EAL4+ certified and IPv6 ready logo certified. Proof of same to be submitted.	7. The Firewall solution offered must be Common Criteria EAL4+ certified and IPv6/USGv6 ready logo certified. Proof of same to be submitted.
57	Real-time threat intelligence updates from OEM; automatic sample submission	Real-time threat intelligence updates from OEM; automatic sample submission to sandboxing
57	Available on Windows/Windows Server/MacOS/Linux	Agent Installer Available on Windows/Windows Server/MacOS/Linux
57	Hybrid XDR: integrate third-party security telemetry natively (no paid add-ons), give detail, meaning, can be troublemaking	For OEM-native XDR, integration with the OEM's own security stack is sufficient. For non-OEM-native XDR, the solution must provide hybrid XDR capability to ingest and correlate third-party security telemetry natively, without requiring any paid add-ons. Documentary proof required.
57	Seamless integration with the FIREWALL procured as part of current RFP; health check before connecting via VPN	The XDR solution shall ensure that device posture and endpoint health assessment is enforced either (a) prior to permitting users to connect via VPN to the firewall, or (b) via a Zero Trust Network Access (ZTNA) mechanism that validates device posture before granting access to protected resources. Bidder shall submit OEM-published documentary evidence (datasheet / whitepaper / product manual / interoperability matrix) demonstrating compliance; self-certification alone shall not be considered sufficient

Note: OEM-native XDR solutions tightly integrated with the bidder's proposed firewall and endpoint ecosystem are acceptable, provided all specified functional requirements are met and supported by OEM-published documentation.