RISL

RajCOMP Info Services Ltd.

(A Government of Rajasthan undertaking)

email: info.risl@rajasthan.gov.in
website: www.risl.rajasthan.gov.in

Ref. No. F3.3(513)/RISL/Pur/2024/1404 Dated: 23-05-2024

Corrigendum

In reference to RFP for Rate Contract for Supply & Installation of EDR licenses and SSL certificates for various websites/ applications floated vide NIB no. F3.3(513)/RISL/Pur/2024/7781 Dated: 19.02.2024 and eproc tender id 2024_RISL_382224_1), following amendments have been made:

I. Technical specifications for Item-1: Endpoint Detection and Remediation/ Response (EDR) in Annexure -2: Technical Specifications have been revised. Revised technical specifications for item-1 : Endpoint Detection and Remediation/ Response (EDR) are attached herewith as Annexure-A.

II. A new clause 5.39 is being appended for 'Risk and Cost' in Chapter 5: Instruction to Bidders (ITB) as follows:
If the bidder, breaches the contract by failing to deliver goods, services, or works according to the terms of the agreement, the procuring authority may terminate the contract and procure the required goods, services, or works from another source which is known as substitution. In such cases, the defaulting contractor bears the risk associated with their failure to fulfil their contractual obligations. If the cost of procuring the goods, services, or works from another source is higher than the original contract, the defaulting contractor is liable for the additional cost incurred by the procuring authority.

III. A new clause 5.28.e is being appended for 'Non-Disclosure Agreement (NDA)' in clause 5.28: Confidentiality as follows:

Bidder has to sign Non-Disclosure Agreement with the tendering authority as per indicative format annexed as Annexure -15: Non-Disclosure Agreement (attached herewith as Annexure B).

This amendment will supersede all references made to this regard.

(Pradumna Dixit)
SA (Jt. Director)

Annexure A

Annexure -2: Technical Specifications

Item-1 Endpoint Detection and Remediation/ Response (EDR)

Make Model offered………………………….. (Need to be filled by the bidder)

S No	Functional Specifications	Compliance (Yes/ No)
1.	Proposed solution should be completely On-Premise	
2.	Solution should support stateful Inspection Firewall, Anti-Malware, Integrity Monitoring, Application Control, log inspection and recommended scan, MITRE ATTACK framework, sandbox capability, machine learning in single module and agent capabilities	
3.	Detect and block unauthorized software execution with multi-platform application control	
4.	Proposed solution should have the ability to lock down a computer (prevent all communication) in case of an attack, except with management server.	
5.	Firewall rules should filter traffic based on source and destination IP address, port/MAC address, etc. and should detect reconnaissance activities such as port scans and Solution should be capable of blocking and detecting IPv6 attacks.	
6.	It should provide automatic rectification for known and unknown vulnerabilities and dynamically tuning EDR/ HIPS engine.	
7.	Solution should support any pre-defined lists of critical system files for various operating systems and/or applications (web servers, DNS, etc.) and support custom rules as well.	
8.	Solution should have feature to take backup of infected files and restoring the same.	
9.	The Solution must detect and block access to suspicious, dangerous phishing sites by scanning all form fields.	
10.	Shield known and unknown vulnerabilities in web, enterprise applications, and operating systems through a HIPS / Threat Inspection.	
11.	Solution should have Security Profiles which allows Integrity Monitoring rules to be configured for groups of systems, or individual systems. For example, all Linux and Windows servers use the same base security profile allowing further fine tuning if required. Rules should be Auto-Provisioned based on Server Posture. Monitors files, libraries, services and more for changes. When changes from this desired state are detected, details are logged, and alerts can be issued to stakeholders.	
12.	Variant Protection should look for obscure, polymorphic, or variants of malware by using fragments of previously seen malware and detection algorithms.	
13.	Should provide automatic recommendations/remediations against existing vulnerabilities, dynamically tuning EDR/ HIPS engine and provide automatic recommendation/ remediations.	
14.	Should have pre and post execution machine Learning and should have Ransom ware Protection in Behaviour Monitoring	
15.	Should support agents for a broader range of Server Operating Systems i.e., MS Windows Server 2016,2019,2022 and higher, RHEL 7.x, 8.x, 9.x and higher, CentOS Linux, Oracle Linux, SUSE Linux, Ubuntu Linux and should support latest kernel variant of respective OS and should support auto updated agents in client	

S No	Functional Specifications	Compliance (Yes/ No)
	server environment	
16.	Machine Learning: Analyses unknown files and zero-day threats using machine learning algorithms to determine if the file is malicious	
17.	Proposed OEM should be positioned in any quadrant from latest published Gartner Magic quadrant report for Endpoint Protection.	
18.	Management of proposed solution should support Windows/Linux platform	
19.	It should be capable of recommending rules / remediations based on vulnerabilities with the help of virtual patching etc. and should have capabilities to schedule recommendation scan.	
20.	Should automatically submit unknown files and suspicious object samples on real time basis as per analysis and revert back to server security. Should support sandbox environment for Windows Server 2016, 2019, 2022 and higher. It should not leverage existing network security layer of RSDC and must be a dedicated HIPS/EDR engine.	
21.	OEM of proposed solution should have local 24x7 TAC support in India	
22.	Agent should be light-weight and tamper-proof and should not downgrade the performance of the system. It should not allow the end-user, any application to uninstall it or change the effective policy.	
23.	The solution should have a dedicated centralised management server/console for managing the endpoints. All the dependent S/w required for deploying the management server should be bundled with the proposed solution. Management server should be able to pull the definition and other application updates from the internet and distribute them in real-time to all deployed agents. It should log (automated/ scheduled) the operations, security and policy related events in the central database and should be displayed on a time axis. It should allow the deployment of multiple instances of mgmt server, each for a specific site/ location/ group of endpoints. Also, there should not be any license implications for the deployment of multiple instances of management server/ console. The management and analytic components of the solution shall scale (using multiple instances) to support an endpoint client load of at least 5,000 endpoints. It should have a web-based console supported on modern browsers including MS-Edge, Google Chrome and Mozilla Firefox	
24.	The EDR solution should provide remote installation and updation of agents on endpoints. Also, the EDR solution should provide integration with MS-Active Directory for mandating the deployment of agents using the organisation's Group Policy.	
25.	The EDR solution should allow grouping of endpoints as per requirement.	
26.	The EDR solution should offer the facility of searching events based on Source IP, Destination IP, Port, Hostname, Domain Name, Process name, File name, Folder name, Hash values.	
27.	Communication between the agents and management server(s) should be encrypted.	
28.	The EDR solution should provide configurable alerting.	
29.	The EDR solution should preferably not have any restrictions on data retention	

S No	Functional Specifications	Compliance (Yes/ No)
	and should be limited to the local available storage.	
30.	The EDR solution should have granular reporting (both on-demand and scheduled) on threats identified & blocked including potential unwanted programs and known/ unknown malware.	
31.	Reports should be supported in at least PDF and XLS/ CSV formats.	
32.	The solution should have integrated capability for event analysis.	
33.	Should integrate with leading OEM's SIEM and SOAR platforms.	
34.	The solution should provide capabilities including Exploit protection, Automated Detection, Containment (Automated/Manual Isolation/ Quarantine), Investigation/analysis and Elimination	
35.	The solution should be able to detect fileless attacks, parent-child process relationships, loading/ unloading of DLLs, files download from internet, modifications to the system files and system registry/ configuration, start-up programs and record/log their activities.	
36.	The solution should provide granular definition of prevention rules, instead of on/off switch for legitimate command interpreters like powershell, wmi, etc., advanced anti-ransomware protection based technology.	
37.	The EDR solution should have ability to approve & blacklist apps via SHA256 hash, certificate or path and deobfuscate encoded powershell payloads.	
38.	The EDR solution should have the ability to trace any malicious/ suspicious activity and record/log all user activity like files downloaded, programs executed etc. across all OS platforms. It should not be limited to record/log the malicious activities/ actions only.	
39.	The EDR solution should provide detailed information of inbound/ outbound network connections at endpoints associated with the process and able to identify malicious/ suspicious activities.	
40.	The EDR solution should provide visibility into lateral movement from endpoints.	
41.	The EDR solution should be able to detect and alert for any Data Exfiltration / breach activity.	
42.	The EDR solution should have guided Threat Hunting and IR/log Inspection capabilities.	
43.	The EDR solution should provide automated Root Cause Analysis (RCA) any malicious/ suspicious activity and visualization of an attack.	
44.	The EDR solution should have the ability to ingest and consume the Threat Intel from the respective OEM and other alliances (if any) in a non-proprietary format (CSV, STIX/ TAXII)	
45.	The EDR solution should allow blocking and restricting the access to USB Mass/ Removal Storage Media (without affecting USB Keyboard and Mouse) on endpoints.	
46.	The EDR solution should allow blocking the execution of admin-defined files and applications on endpoints including the RDP/ SSH access.	

S No	Functional Specifications	Compliance (Yes/ No)
47.	Should be able to protect the endpoint from virus, backdoors, adware, spyware, malware (known/ unknown), BoT, ransomware, CnC Servers, malicious websites, zero-day attacks, crypto lockers, and other malicious content, if any, on local endpoint and network.	
48.	The EDR solution should have the capability to add exclusions of local files, folder and installed applications.	

Note:

1. All the items of above mentioned should be supplied with OEM Warranty, Support, Subscription/ Software Assurance. (License and asset ownership is required on the date of installation for all OS & related software products)
2. All the supplied Hardware/ Software should be Interoperable, IPv6 ready and in compliance with the policies/ guidelines issued by DIT, GoI in this regard. Also, the bidder is to quote/ propose only one make/ model against item.
3. *All the specifications below are minimum specifications and higher specifications shall be used wherever necessary/ required. Deviation on higher side shall only be considered and no extra weightage shall be awarded for such deviations.* ***The bidder is required to submit the technical compliance statement for each item only on the respective OEM's letter-head.***

Annexure - B

ANNEXURE-15: INDICATIVE CONFIDENTIALITY AND NON DISCLOSURE AGREEMENT

CONFIDENTIALITY AND NON-DISCLOSURE AGREEMENT

This confidentiality and non-disclosure agreement ("Agreement") is made on this ___________day of ____, (Year)

BETWEEN

Managing Director, RajComp Info Services Ltd., B-Block, 1st Floor, Yojna Bhawan, Tilak Marg, C-Scheme, Jaipur-302005 (hereinafter referred to as "RISL", which expression shall, unless repugnant to the context hereof or excluded specifically, mean and include its successors, assigns and administrators) of the FIRST PART,

AND

Company Name, India (hereinafter referred to as 'Successful Bidder/ Supplier', which expression shall, unless repugnant to the context hereof or excluded specifically, mean and include its successors, assigns and administrators) of the SECOND PART.

WHEREAS

a. The RISL wishes to appoint an agency for_________________Yojana Bhawan, Jaipur for a period of __ years. For the purpose there will be a requirement to exchange certain information related to or hosted inRajasthan State Data Centre (RSDC) which is proprietary andconfidential information.
b. The RISL is willing to disclose such information to successful bidder only on the terms and conditions contained in this Agreement. The successful bidder agrees to hold the Covered Data and Information in strict confidence. Successful bidder shall not use or disclose Covered Data and Information received from or on behalf of Government of Rajasthan/RISL except as permitted or required by the Agreement, or as otherwise authorized in writing by RISL.

NOW, THEREFORE, THE PARTIES HERETO AGREE AS FOLLOWS:

1. **Definition: In this agreement unless the contest otherwise requires:**

1.1. "Confidential Information" shall mean

a) any and all information concerning Rajasthan State Data Centre (RSDC)or any other successor,
b) any and all trade secrets or other confidential or proprietary information related and hosted in State Data Centre (SDC)
c) Passwords of IT/Non IT equipments of SDC, user identifications, or other information that may be used to access information systems, networking diagrams, technical specifications of IT/Non IT equipments, policies of firewall/IDs/IPS /routers /switches and information hosted on IT equipments in Rajasthan State Data Centre (RSDC)

1.2. Proprietary Information shall mean as technical data and other information (including but not limited to digital data, products, substances, organisms, technology, research results or plans, system processes, workflows, know-how, reports, descriptions, drawings, design, compositions, strategies, trade secrets, business and financial information, and computer software) in whatever form, which is related or hosted with Rajasthan State Data Centre (RSDC)and is disclosed or delivered by the First Party to the Second Party, whether by means of written or oral disclosure or otherwise.

2. **Limitations on Use and Disclosure of Confidential and Proprietary Information**

2.1. Confidential and Proprietary Information disclosed by the RISL and/or other departments/PSU whose data are hosted in Rajasthan State Data Centre (RSDC)shall be used by the successful bidder solely for the purpose of fulfillment of the obligation and work assigned to it as per order no.______________and shall not otherwise be used for his benefit or otherwise. All information encountered in the performance of duties shall be treated as confidential unless and until advised otherwise by RISL or its representative.

Successful bidder shall not share, record, transmit, alter, or delete information residing/hosted in the information systems except as required in performance of the job duties.

2.2. Confidential and Proprietary Information shall not be copied or reproduced by the successful BIDDER without the express written permission of the RISL, except for such copies as may be reasonably required for accomplishment of the purpose stated in the tender no.______________________.

2.3. Confidential and Proprietary Information shall be disclosed only to the Director or employees of the successful bidder who have a 'need to know' in connection with the purpose stated above, and who additionally agree to the nondisclosure requirements of this Agreement. Any further disclosure of confidential and Proprietary Information by the successful bidder shall be treated as a breach of this Agreement by the successful bidder.

2.4. Confidential and Proprietary Information shall not be disclosed by the successful bidder to any third party without the prior written consent of the First Party.

2.5. This Agreement shall not restrict disclosure or use of Confidential and Proprietary Information which:

a. was in the public domain at the time of disclosure or thereafter enters the public domain through no breach of this Agreement by the successful bidder; or
b. was, at the time of receipt, otherwise known to the successful bidder without restriction as to use or disclosure; or
c. becomes known to the successful bidder from a source other than the RISL and/or other departments/PSU without a breach of this Agreement by the successful bidder; or
d. is developed independently by the successful bidder without the use of Proprietary Information disclosed to it hereunder; or
e. is otherwise required to be disclosed by law.

3. Business Obligation:

3.1. During the complete contract period and even after 3 years of the expiry of the agreement, the successful bidder shall not

a. Disclose Confidential Information in any manner or form to any person other than its own employees for the limited purpose stated herein, or
b. Use Confidential Information for its own benefit or for the benefit of any person or entity other than the RISL, without the prior written consent of the RISL .

3.2. Whereas, the RISL as a matter of policy and with a view to operate and maintain SDC has given order to the successful bidder Work Order Nofor __________________at Yojana Bhawan, Jaipur for a period of __ year as specified in the service level agreement (SLA).

3.3. Whereas, the RISL under the circumstances referred, herein before, wants to protect itself from any misuse of the confidential and proprietary information by the third party i.e. person or persons (employees of successful bidder), had entered into an agreement with the successful BIDDER that the second party shall not divulge such information either during the course of the life of this agreement or even after the expiry of the agreement.

3.4. Whereas, the successful bidder has agreed to fully abide by the terms of this non-disclosure agreement and it has also been agreed by the parties that if there will be any breach or violation of the terms of agreement vis-à-vis non-disclosure clause, the successful bidder shall not only be liable for consequential costs and damages but in addition to that will also be liable for criminal prosecution in accordance with the prevailing laws.

3.5. whereas, the successful bidder having in his possession or control any secret official code or password or digital data or any sketch, plan, model, article, note, document or information which falls within the purview of confidential or proprietary information, the successful bidder shall not part with any part of such information to anyone under any circumstances, whatsoever, without the prior approval of the risl and if this is violated, the risl shall have the legal right to initiate civil and criminal proceeding against it under the provisions of the relevant law.

3.6. Whereas, the RISL shall have the entire control over the functioning of the Successful bidder and the successful bidder shall work according to the instruction of the RISL and in case if this is violated by the successful bidder in any mode or manner, the RISL shall have the legal right to initiate civil and criminal proceeding against it under the provisions of the relevant law.

3.7. Whereas, if the successful bidder permits any person or persons without permission of the RISL to have –

a. Access or secures access to such computer, computer system or computer network which has the connectivity with the confidential and proprietary information or;

b. Downloads, copies or extracts any data, computer data base or information from such Database Server, Web Server, Computer System, networking equipments or Computer Network including information or data held or stored in any removable storage medium which has the connectivity with the confidential and proprietary information or;

c. Damages any Database Server or causes to damage any Database Server, Web Server, computer system, computer network, data, data base or any other programmes residing in such Server, computer system or computer network;

d. Denies or causes the denial of access to any authorized person of the RISL to have access to any computer system or computer network by any means;

Shall be liable to pay damages by way of compensation and would also be liable for criminal prosecution in accordance with the prevailing laws.

3.8 successful bidder shall report to RISL any use or disclosure of confidential and/or proprietary information/data not authorized by this Agreement in writing by RISL. Successful bidder shall make the report to RISL within not less than one (1) business day after successful bidder learns of such use or disclosure. Successful bidder's report shall identify:

a) The nature of the unauthorized use or disclosure,

b) The confidential and/or proprietary information/data used or disclosed,

c) Who made the unauthorized use or received the unauthorized disclosure,

d) What successful bidder has done or shall do to mitigate any deleterious effect of the unauthorized use or disclosure, and

e) What corrective action successful bidder has taken or shall take to prevent future similar unauthorized use or disclosure.

SUCCESSFUL BIDDER shall provide such other information, including a written report, as reasonably requested by RISL.

3.9 The successful bidder hereby agrees and consents that temporary or permanent injunctive relief and/or an order of specific performance may be granted in lieu of, or in addition to other available relief in any proceeding brought by RISL to enforce this Agreement, without the necessity of proof of actual damages and without posting bond for such relief.

4. **Dispute Resolution:**

4.1. Whereas, both the parties have agreed that in the event of any dispute or differences arising in between the parties, the courts at Jaipur shall only have jurisdiction to adjudicate the disputes/differences.

IN WITNESS WHERE OF the Parties here to have hereunto set their hands and seal the day and year first above written.

Signed By:	Signed By:
( ) Designation:, Company:	Managing Director, RISL

In the presence of:	*In the presence of:*
( ) Designation: Company:	() Designation: RISL
( ) Designation: Company:	() Designation: