



# RajCOMP Info Services Ltd.

(A Government of Rajasthan undertaking)

email: [info.risl@rajasthan.gov.in](mailto:info.risl@rajasthan.gov.in)  
website: [www.risl.rajasthan.gov.in](http://www.risl.rajasthan.gov.in)

Ref. No. F3.3 (449)/RISL/Tech/Misc/2022/1171

Dated: 17.05.2023

## Corrigendum

In reference to RFP for Supply, Installation, Configuration, Integration, Testing, Training, Commissioning, Operations & Maintenance (Three Years) of CYBER RANGE Platform for Rajasthan Cyber Security CoE floated vide NIB no. F3.3 (449)/RISL/Tech/Misc/2022/8280 Date: 02.03.2023 (eProc id 2023\_RISL\_322612\_1), following amendments have been made in Final RFP:-

### 1. Amendments in clause

#### Annexure-2 Technical Specifications

Old Clause		New Clause	
<b>Item-1: - Cyber Range Platform including associated Hardware and Software</b>	(5) (m) Based on the current threat landscape, the pre-packaged scenarios to be included in the solution from day one are: - Advanced Network Forensics, Anomaly Detection and Forensics, Application DDoS, APT-1 , APT-18, APT-29, APT-30, APT-37, Automating and Response with SOAR, BlackEnergy, Blue Team Introduction Scenario, Botnet Attack, Bruteforce Attacks, <b>Centralized Defense (Splunk and IBM QRadar)</b> , Cloud Security, Compromised Hosts: Control Access and Monitoring for Malicious Threats, Credential Sharing, Cross-site Scripting, Custom Detection, Cyber Defense Response Challenge: Incident Response, Data Exfiltration in a vDC environment, Database Vulnerabilities (Top 10), Defend Identities and Password Compromise, Dictionary Attacks, DMZ Penetration, DNS Vulnerabilities, Email Exploitation, Encryption, End to End Exploitation Lab, End-to-End Exploitation - Advanced Attack Lab, Hack the Endpoint, Insider Threats: Move Within to Obtain and Export Your Data, Inter vDC attacks, Intra vDC attacks, Know Your	<b>Item-1: - Cyber Range Platform including associated Hardware and Software</b>	(5) (m) Based on the current threat landscape, the pre-packaged scenarios to be included in the solution from day one are: - Advanced Network Forensics, Anomaly Detection and Forensics, Application DDoS, APT-1 , APT-18, APT-29, APT-30, APT-37, Automating and Response with SOAR, BlackEnergy, Blue Team Introduction Scenario, Botnet Attack, Bruteforce Attacks, Cloud Security, Compromised Hosts: Control Access and Monitoring for Malicious Threats, Credential Sharing, Cross-site Scripting, Custom Detection, Cyber Defense Response Challenge: Incident Response, Data Exfiltration in a vDC environment, Database Vulnerabilities (Top 10), Defend Identities and Password Compromise, Dictionary Attacks, DMZ Penetration, DNS Vulnerabilities, Email Exploitation, Encryption, End to End Exploitation Lab, End-to-End Exploitation - Advanced Attack Lab, Hack the Endpoint, Insider Threats: Move Within to Obtain and Export



# RajCOMP Info Services Ltd.

(A Government of Rajasthan undertaking)

email: [info.risl@rajasthan.gov.in](mailto:info.risl@rajasthan.gov.in)  
website: [www.risl.rajasthan.gov.in](http://www.risl.rajasthan.gov.in)

## Annexure-2 Technical Specifications

Old Clause		New Clause	
	Packets, Malware Detection, MFA Bypass, MITM in WiFi, Network Access Control, Network Forensics I, OSINT, Privilege Access Management, Ransomware - A, Ransomware - B, Red Team Introduction Scenario, Rogue AP Interference, Scripting Language Weakness, Security Orchestration, Signature based Detection, Silence Threat Hunting Scenario, Smash and Grab: Attacking Public Network Services Through the Front Door, Snooping, SQL Injection, state exhaustion attacks, StuxNet, Target Reconnaissance: Gathering Information about Vulnerabilities for a Future Attack, The Ransom Scenario, Threat Investigation, Trojan Backdoor, Volumetric attacks, Wall of Sheep, Web Defense and Resource Sustainability Part 1 and 2, Web Vulnerabilities (Top 10), Wi-Fi Security, Wireless Attack Detection.		Your Data, Inter vDC attacks, Intra vDC attacks, Know Your Packets, Malware Detection, MFA Bypass, MITM in WiFi, Network Access Control, Network Forensics I, OSINT, Privilege Access Management, Ransomware - A, Ransomware - B, Red Team Introduction Scenario, Rogue AP Interference, Scripting Language Weakness, Security Orchestration, Signature based Detection, Silence Threat Hunting Scenario, Smash and Grab: Attacking Public Network Services Through the Front Door, Snooping, SQL Injection, state exhaustion attacks, StuxNet, Target Reconnaissance: Gathering Information about Vulnerabilities for a Future Attack, The Ransom Scenario, Threat Investigation, Trojan Backdoor, Volumetric attacks, Wall of Sheep, Web Defense and Resource Sustainability Part 1 and 2, Web Vulnerabilities (Top 10), Wi-Fi Security, Wireless Attack Detection.
<b>Item-3: - Breach</b>	(1)(b) (i). A valid ISO 9001 and ISO 27001 certification	<b>Item-3: - Breach</b>	(1) (b) (i). A valid ISO 27001 certification
	(1) (b) (ii). A direct support centre in India		(1) (b) (ii). A <b>direct/partner's</b> support centre in India



# RajCOMP Info Services Ltd.

(A Government of Rajasthan undertaking)

email: [info.risl@rajasthan.gov.in](mailto:info.risl@rajasthan.gov.in)

website: [www.risl.rajasthan.gov.in](http://www.risl.rajasthan.gov.in)

## Annexure-2 Technical Specifications

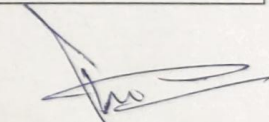
Old Clause		New Clause	
<b>Attack Simulation Appliance</b>	(4) (j) If the proposed solution is an agent-based solution then the agent(s) must be lightweight and infrastructure-agnostic so that the solution can operate on on-premise infrastructure, private or public clouds and on local or remote user laptops/ desktops/ work stations. <b>It must also provide a topology viewer which shows in real time how the agents are interconnected and the available paths that exist across all agents.</b> Minimum 10 Agent Licenses to be supplied.	<b>Attack Simulation Appliance</b>	(4) (j) If the proposed solution is an agent-based solution then the agent(s) must be lightweight and infrastructure-agnostic so that the solution can operate on on-premise infrastructure, private or public clouds and on local or remote user laptops/ desktops/ work stations. Minimum 10 Agent Licenses to be supplied.

Note :- All the provisions of RTPPA Act 2012 and Rules, 2013 thereto shall be applicable for this procurement. Furthermore, in case of any inconsistency in any of the provisions of this bidding document with the RTPPA Act 2012 and Rules, 2013 thereto, the later shall prevail.

### 2. Revised dates for submission of Bids, Bidding document fees, Bid Security and RISL processing fees and Date/Time/Place of technical bid opening

E-Proc Tender ID	2023_RISL_322612_1
Period of Sale of Bidding Documents	From 02.03.2023 (6:00 PM) to 26.05.2023 (up to 4:00 PM)
Start/End Date for the submission of Bids	From 11.04.2023 (6:00 PM) to 26.05.2023 (up to 4:00 PM)
Submission date of Banker's Cheque/ Demand Draft for Tender fees, Bid Security and Processing fee	Up to 04:00 PM on 26.05.2023
Date/ Time/ Place of Technical Bid Opening	<ul style="list-style-type: none"><li>• 26.05.2023 (04:30 PM)</li><li>• Place: RISL, eProcurement Hall, First Floor, Yojana Bhawan, C-Block, Tilak Marg, C-Scheme, Jaipur (Rajasthan)</li></ul>

This amendment will supersede all references made to this regard.

  
(Pradumna Dixit)  
System Analyst (Jt. Director)