Responses to Pre Bid Queries Received against RFP for Rate Contract of Procurement of Endpoint Detection and Response (EDR) Solution, floated vide NIB no. F3.3(513)/RISL/Pur/2024/6063 Dated: 27.01.2026

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
1	1. INVITATION FOR BID (IFB)& NOTICE INVITING BID (NIB)	10	Invitation for Bid (IFB) & NIB	Estimated Procurement Cost Rs.3.55 Cr (Rupees Three Crore and Fifty Five lac Only) (Incl. all Taxes and levies)	**Estimated Procurement Cost** **Rs. 4.55 Cr (Rupees Four Crore and Fifty Five lac Only) (Incl. all Taxes and levies)** Justification We have reviewed several previous tenders for EDR solutions issued by various government departments across India and observed that the presently considered estimated procurement cost does not adequately reflect prevailing global market prices. Additionally, continuous fluctuations in international pricing indices, foreign exchange rates (USD to INR), and global inflationary trends have led to an upward revision in procurement costs for IT hardware and allied components. Considering the above factors and to ensure realistic cost estimation, wider bidder participation it is proposed to revise the Estimated Procurement Cost to Rs. 4.55 Crore (Rupees Four Crore and Fifty Five lac Only), inclusive of all applicable taxes and levies. This revision is essential to align the estimated cost with current market realities and to avoid the risk of procurement failure due to non-responsive bids or unviable pricing.	As per RFP
2	1. INVITATION FOR BID (IFB)& NOTICE INVITING BID (NIB)	10	Procurement Cost	Estimated Procurement Cost: 3.55 Cr. With Taxes	Its too less taking care BOQ of the RFP, is should be **minimum 5 Cr + Taxes.** Same can be validated from other reference order for the same product.	As per RFP
3	3. Qualification / Eligibility	13	Technical Capability - I	The bidder must have successfully completed or partially completed one work order / contract of System Software/ Licenses (OS, Antivirus/EDR, Web/DB Servers, etc.) of value not less than the amount Rs. 2.80 Crore in any Public Sector Bank / BFSI / PSU / Government Organization / Telecom organization in India during the period from 01/04/2020 onwards. OR The bidder must have successfully completed or partially completed Two work order/ contract of System Software/ Licenses (OS, Antivirus/EDR, Web/DB Servers, etc.) of value not less than the amount Rs. 1.75 Crore each in any Public Sector Bank / BFSI / PSU / Government Organization / Telecom organization in India during the period from 01/04/2020 onwards.	The bidder must have successfully completed or partially completed one work order / contract of System Software/ Licenses (OS, Antivirus/EDR, Web/DB Servers, etc.) of value not less than the amount Rs. **2.45 Crore** in any Public Sector Bank / BFSI / PSU / Government Organization / Telecom organization in India during the period from 01/04/2020 onwards. OR The bidder must have successfully completed or partially completed Two work order/ contract of System Software/ Licenses (OS, Antivirus/EDR, Web/DB Servers, etc.) of value not less than the amount Rs. **1.60 Crore** each in any Public Sector Bank / BFSI / PSU / Government Organization / Telecom organization in India during the period from 01/04/2020 onwards.	Refer Amended RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
4	3. Qualification / Eligibility	14	Technical Capability - II	The bidder must have successfully completed or partially completed one work order/ contract for implementing EDR solution in any Public Sector Bank / BFSI / PSU / Government Organization / Telecom organization in India during the period from 01/04/2020 onwards, for a minimum of 3000 EDR Licences.	Technical Capability – II The bidder must have successfully completed or partially completed one work order/ contract for implementing EDR solution in any Public Sector Bank / BFSI / PSU / Government Organization / Telecom organization in India during the period from 01/04/2020 onwards, for a minimum of 3000 EDR Licences**/ Antivirus Software/ Endpoint Protection**	As per RFP
5	3. Qualification / Eligibility	14	Technical Capability - II	The bidder must have successfully completed or partially completed one work order/ contract for implementing EDR solution in any Public Sector Bank /BFSI / PSU / Government Organization / Telecom organization in India during the period from 01/04/2020 onwards, for a minimum of 3000 EDR Licences.	The bidder must have successfully completed or partially completed one work order/ contract for implementing EDR solution in any Public Sector Bank /BFSI / PSU / Government Organization /Telecom organization in India during the period from 01/04/2020 onwards, for a **minimum of 6000 EDR Licences.** This will help only capabale System Integrator having better exeprience to participate.	As per RFP
6	4. SCOPE OF WORK, DELIVERABLES AND TIMELINES	18	2.1. Installation, Configuration, and Integration	Installation & Configuration	Is High Availability (HA) and Disaster Recovery (DR) required for EDR management servers?	As per RFP
7	4. SCOPE OF WORK, DELIVERABLES AND TIMELINES	18	2.1. Installation, Configuration, and Integration	Scope of Work - integration	Please confirm the SIEM and SOAR platforms currently deployed at RSDC (OEM name and version) and whether bi-directional integration is required.	As per RFP - The detail would be shared with Successful bidder.

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
8	4. SCOPE OF WORK, DELIVERABLES AND TIMELINES	17	Advanced Capabilities	Generic	For platforms such as Oracle Exadata, IBM PureApp, Oracle Exalogic, and OpenShift, is agent-based EDR mandatory on all components or are non-intrusive options acceptable?	As per RFP - Agent-based EDR may be deployed on supported server components wherever feasible. For engineered or appliance-based platforms such as Oracle Exadata, IBM PureApplication, Oracle Exalogic, and Red Hat OpenShift, where third-party agent installation is restricted or not recommended by OEM guidelines, non-intrusive or OEM-supported monitoring mechanisms shall be acceptable, provided adequate security visibility is ensured.
9	4. SCOPE OF WORK, DELIVERABLES AND TIMELINES	17	Scope of Work	Generic	Is there an endpoint agent deployment tool available to install the agent and remove any pre-existing agents?	As per RFP - Steps and scripts would be provided by successful bidder. Execution would be performed by DC team.
10	4. SCOPE OF WORK, DELIVERABLES AND TIMELINES	17	Scope of Work	Generic	Who will be responsible for removing/decommission any pre-existing agents?	As per RFP - Steps and scripts would be provided by successful bidder. Execution would be performed by DC team.

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
11	4. SCOPE OF WORK, DELIVERABLES AND TIMELINES	17		Scope of Work	Will RISL provide dedicated servers/VMs for EDR management, database, and analytics components	As per RFP - Infrastructure shall be provisioned as per the RFP. Detailed allocation will be shared with the successful bidder; however, the SI shall provision and include licenses for all required software components, including OS, database, analytics, and related applications.
12	5.INSTRUCTION TO BIDDERS (ITB)	27	Bid Security	The bid security may be given in the form of cash, a banker's cheque or demand draft or bank guarantee or electronic bank guarantee (e-BG), in specified format, of a scheduled bank or Insurance Surety Bonds	Pls. Provide the indicative format for Insurance Surety Bonds, same is not mentioned in RFP	As per RFP
13	5.INSTRUCTION TO BIDDERS (ITB)	37	Performance Security:	f. In case of procurement of works, the successful bidder at the time of signing of the contract agreement, may submit option for deduction of performance security from his each running and final bill @ 10% of the amount of the bill.	Request for Changes: In case of procurement of works, the successful bidder at the time of signing of the contract agreement, may submit option for deduction of performance security from his each running and final bill @ 5% of the amount of the bill. as per Government of Rajasthan prevailing rules and regulations, of the amount of supply order in case of procurement of goods and services. In case of Small Scale Industries (SSI) of Rajasthan, it shall be 1% of the amount of quantity ordered for supply of goods and in case of sick industries, other than SSI, whose cases are pending before the Board of Industrial and Financial Reconstruction (BIFR), it shall be 2% of the amount of supply order	As per RFP
14	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	66	7. Special T&C of Tender & Contract 1) Payment Terms and Schedule	Completion of Activities applicable and as mentioned in Chapter 4. Payable Amount 85% value of supplied items.	Completion of Activities applicable and as mentioned in Chapter 4. Payable Amount **91% value of supplied items.** Justification It is submitted that the Performance Security, as stipulated in the tender conditions, shall be furnished separately in accordance with the applicable procurement rules. In view of the same, retention of a higher portion of the payment is not considered necessary. Revision of the payable amount to 91% of the value of supplied items shall reduce working capital constraints on the bidder and facilitate smoother project execution, while also enabling more competitive pricing, thereby resulting in overall financial benefit to the Department.	As per RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
15	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	66	7. Special T&C of Tender & Contract 1) Payment Terms and Schedule	Completion of Activities applicable and as mentioned in Chapter 4. Timelines (T= Date of WO) T1=T+90 days	Completion of Activities applicable and as mentioned in Chapter 4. Timelines (T= Date of WO) **T1=T+120 days** Justification Since the proposed EDR solution is required to be integrated with the Department’s existing SIEM, APT, SOAR and other deployed security systems, additional time is necessary for order processing, delivery of licenses / appliances, solution integration, configuration and comprehensive interoperability and scenario-based testing prior to production rollout. Accordingly, to ensure successful implementation in line with the scope defined in SoW and to avoid operational risks, it is requested to revise the milestone T1 from T + 90 days to T + 120 days.	As per RFP
16	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	66	7. Special T&C of Tender & Contract 1) Payment Terms and Schedule	Completion of every support year for three years from the date of installation. Payable Amount 5% value of supplied items end of each year for three years from the date of installation (after deducting penalties, if any and as applicable).	Completion of every support year for three years from the date of installation. Payable Amount **3% value** of supplied items end of each year for three years from the date of installation (after deducting penalties, if any and as applicable). Justification It is submitted that the Performance Security, as stipulated in the tender conditions, shall be furnished separately in accordance with the applicable procurement rules. In view of the same, retention of a higher portion of the payment is not considered necessary. Revision of the payable amount to 3% of the value of supplied items end of each year for 3 years from date of installation shall reduce working capital constraints on the bidder and facilitate smoother project execution, while also enabling more competitive pricing, thereby resulting in overall financial benefit to the Department.	As per RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
17	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	67	7. Special T&C of Tender & Contract 2) Service Level Standards / Requirements / Agreement	Clause No. b Maximum applicable penalty shall be 50% of agreed value of item.	Clause No. b Maximum applicable penalty shall be **10%** of agreed value of item. Justification With reference to Clause (b) under Service Level Standards, it is respectfully submitted that the presently stipulated maximum penalty of 50% of the agreed value of the item is commercially onerous and disproportionate to the nature of support services envisaged under the SLA. It is therefore requested to consider rationalising the maximum applicable penalty and revising the same to 10% of the agreed value of the item, so as to ensure fair and balanced contractual obligations and to encourage wider bidder participation. Further, it is requested to kindly clarify the interpretation of the term “agreed value of the item”, i.e. whether the same refers to the unit price or the total item value, and whether such value is to be considered inclusive or exclusive of GST, for uniform understanding and accurate commercial evaluation.	Refer Amended RFP
18	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	67	7. Special T&C of Tender & Contract 2) Service Level Standards / Requirements / Agreement	Clause No. b Service Level --> Within 12 hours of lodging the complaint --> No penalty Service Level --> After 12 hours of lodging the complaint --> 1% of item cost, per item per next 12 hours	Clarification Sought With reference to Clause (b) under Service Level Standards, it is observed that the penalty provisions are applicable irrespective of actual service impact. It is submitted that certain support activities such as technical assistance, configuration support, advisory services and OEM consultations are routine in nature and may not result in any service outage, performance degradation or operational disruption. It is respectfully requested that the penalty mechanism under Clause (b) may be reviewed and made applicable only in cases involving defined and measurable service impact, such as service downtime, performance degradation or non-achievement of agreed availability parameters. This will ensure equitable and balanced contractual conditions, in line with the objective of SLA enforcement and will encourage wider bidder participation. Further, it is requested to kindly clarify the interpretation of the term “1% of item cost”, i.e. whether the same refers to the unit price of the item or the total item value, and whether the calculation is inclusive or exclusive of GST, for uniform understanding and accurate commercial evaluation.	As per RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
19	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	66	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT 1) Payment Terms and Schedule	(b) Maximum applicable penalty shall be 50% of agreed value of item.	Request for Changes: Maximum applicable penalty shall be **10%** of agreed value of item.	Refer Amended RFP
20	7. SPECIAL TERMS AND CONDITIONS OF TENDER & CONTRACT	66	Balalnce Payment of 15%	5% value of supplied items end of each year for three years from the date of installation (after deducting penalties, if any and as applicable).	Request to release **100% against submision of additional PBG of 15%.**	As per RFP
21	ANNEXURE-2: TECHNICAL SPECIFICATION	70	Annexure-2 – Technical Specifications	Annexure-2 – Technical Specifications	Will RISL share the detailed list of operating systems, kernel versions, and hardening standards currently used at RSDC and DR sites?	As per RFP - Detailed environment information will be shared with successful bidder.
22	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 13	Should provide automatic recommendations/ remediation's against existing vulnerabilities, dynamic or customized tuning EDR/ HIPS engine and provide automatic recommendation/ remediation's.	We would like to highlight that allowing either recommendation or remediation as an option may weaken the overall security posture and does not align with the proactive security approach advocated in CERT-In advisories and best practices. In a data center environment, recommendations without remediation rely on manual intervention and may lead to delays in risk mitigation. Therefore, it is requested that both recommendation and remediation capabilities be mandatorily incorporated to ensure timely, effective, and compliant security controls. Clause should read as : Should provide automatic r**ecommendations and remediation's** against existing vulnerabilities, dynamic or customized tuning EDR/ HIPS engine and provide automatic recommendation and remediation's.	As per RFP
23	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 13	Should provide automatic recommendations/ remediation's against existing vulnerabilities, dynamic or customized tuning EDR/ HIPS engine and provide automatic recommendation/ remediation's.	We would like to highlight that allowing either recommendation or remediation as an option may weaken the overall security posture and does not align with the proactive security approach advocated in CERT-In advisories and best practices. In a data center environment, recommendations without remediation rely on manual intervention and may lead to delays in risk mitigation. Therefore, it is requested that both recommendation and remediation capabilities be mandatorily incorporated to ensure timely, effective, and compliant security controls. Clause should read as : Should provide automatic **recommendations and remediation's** against existing vulnerabilities, dynamic or customized tuning EDR/ HIPS engine and provide automatic recommendation and remediation's.	As per RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
24	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 17 - Gartner Clause	Proposed OEM should be positioned in any quadrant from latest published Gartner Magic quadrant report for Endpoint Protection.	Gartner Clause has mentioned in Item No. 1 at Sr. No. 17 whereas it has been not mentioned in Item No. 2, which is most critical componenet, pls. mentioned same clause in item no. 2 also.	As per RFP
25	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 17 - Gartner Clause	Proposed OEM should be positioned in any quadrant from latest published Gartner Magic quadrant report for Endpoint Protection.	In accordance with the guidelines outlined in the Request for Proposal (RFP), the clauses recommend a proposal from an Original Equipment Manufacturer (OEM) currently positioned in the latest Gartner Magic Quadrant. We kindly request your consideration to include either Gartner Leaders and Challengers to ensure the selection of best-of-breed products for securing crown jewels. Clause should read as: Proposed OEM must be positioned in **either the Leaders or Challengers quadrant** according to the latest published Gartner Magic Quadrant report for Endpoint Protection.	As per RFP
26	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 17 - Gartner Clause	Proposed OEM should be positioned in any quadrant from latest published Gartner Magic quadrant report for Endpoint Protection.	In accordance with the guidelines outlined in the Request for Proposal (RFP), the clauses recommend a proposal from an Original Equipment Manufacturer (OEM) currently positioned in the latest Gartner Magic Quadrant. We kindly request your consideration to include either Gartner Leaders and Challengers to ensure the selection of best-of-breed products for securing crown jewels. Clause should read as: Proposed OEM must be positioned in **either the Leaders or Challengers quadrant** according to the latest published Gartner Magic Quadrant report for Endpoint Protection.	As per RFP
27	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 18	Management of proposed solution should support Windows/ Linux platform.	As per the RFP specifications, it's noted that the proposed management server should be compatible with either Windows or Linux operating systems. Additionally, we kindly request clarification regarding the requirement for database licensing for management server. Furthermore, we would appreciate the inclusion of MS-SQL, Oracle and PostgreSQL for logging events to non-proprietary, industry-standard databases. Clause should read as: Management of proposed solution should support Windows and Linux platform and Solution should support the logging of events to a non- proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL also management platform should support Windows & Linux operating systems.	Refer Amended RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
28	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 18	Management of proposed solution should support Windows/ Linux platform	As per the RFP specifications, it's noted that the proposed management server should be compatible with either Windows or Linux operating systems. Additionally, we kindly request clarification regarding the requirement for database licensing for management server. Furthermore, we would appreciate the inclusion of MS-SQL, Oracle and PostgreSQL for logging events to non-proprietary, industry-standard databases. Clause should read as: Management of proposed solution should support Windows and Linux platform and Solution should support the logging of events to a non- proprietary, industry-class database such as MS-SQL, Oracle, PostgreSQL also management platform should support Windows & Linux operating systems.	Refer Amended RFP
29	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 19	It should be capable of recommending rules /remediation's based on vulnerabilities with the help of virtual patching or prevent exploit attempt etc. and should have capabilities to schedule recommendation scan.	We would like to highlight that allowing either recommendation or remediation as an option may weaken the overall security posture and does not align with the proactive security approach advocated in CERT-In advisories and best practices. In a data center environment, recommendations without remediation rely on manual intervention and may lead to delays in risk mitigation. Therefore, it is requested that both recommendation and remediation capabilities be mandatorily incorporated to ensure timely, effective, and compliant security controls. Clause should read as : It should be capable of **recommending rules and remediation's** based on vulnerabilities with the help of virtual patching and prevent exploit attempt etc. and should have capabilities to schedule recommendation scan.	As per RFP
30	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 19	It should be capable of recommending rules /remediation's based on vulnerabilities with the help of virtual patching or prevent exploit attempt etc. and should have capabilities to schedule recommendation scan.	We would like to highlight that allowing either recommendation or remediation as an option may weaken the overall security posture and does not align with the proactive security approach advocated in CERT-In advisories and best practices. In a data center environment, recommendations without remediation rely on manual intervention and may lead to delays in risk mitigation. Therefore, it is requested that both recommendation and remediation capabilities be mandatorily incorporated to ensure timely, effective, and compliant security controls. Clause should read as : It should be capable of **recommending rules and remediation's** based on vulnerabilities with the help of virtual patching and prevent exploit attempt etc. and should have capabilities to schedule recommendation scan.	As per RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
31	ANNEXURE-2: TECHNICAL SPECIFICATION	70	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 2	Solution should support stateful Inspection Firewall, Anti-Malware, Integrity Monitoring/Threat Prevention, Application Control, log inspection and recommended scan/ device control, MITRE ATTACK framework, sandbox capability, machine learning in single module and agent capabilities	As per the RFP specifications, this requirement appears to seek the inclusion of either Integrity Monitoring or Threat Prevention, along with Recommended Scan or Device Control. However, these are distinct technologies with different objectives, and each plays a critical role in data center security. Therefore, we respectfully request the inclusion of all the specified components— Integrity Monitoring, Threat Prevention, Recommended Scan, and Device Control—to ensure comprehensive and effective security coverage for the data center. Clause should read as : Solution should support stateful Inspection Firewall, Anti- Malware, **Integrity Monitoring, Threat Prevention**, Application Control, log inspection, r**ecommended scan, device control**, MITRE ATTACK framework, sandbox capability, machine learning in single module and agent capabilities	As per RFP
32	ANNEXURE-2: TECHNICAL SPECIFICATION	70	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 2	Solution should support stateful Inspection Firewall, Anti-Malware, Integrity Monitoring/Threat Prevention, Application Control, log inspection and recommended scan/ device control, MITRE ATTACK framework, sandbox capability, machine learning in single module and agent capabilities	As per the RFP specifications, this requirement appears to seek the inclusion of either Integrity Monitoring or Threat Prevention, along with Recommended Scan or Device Control. However, these are distinct technologies with different objectives, and each plays a critical role in data center security. Therefore, we respectfully request the inclusion of all the specified components— Integrity Monitoring, Threat Prevention, Recommended Scan, and Device Control—to ensure comprehensive and effective security coverage for the data center. Clause should read as : Solution should support stateful Inspection Firewall, Anti- Malware, **Integrity Monitoring, Threat Prevention**, Application Control, log inspection, r**ecommended scan, device control**, MITRE ATTACK framework, sandbox capability, machine learning in single module and agent capabilities	As per RFP
33	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 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 / Linux Servers. It should not leverage existing network security layer of RSDC and must be a dedicated HIPS/EDR engine.	We would like to highlight that allowing either Windows or Linux as an option for sandboxing may weaken the overall security posture and result in limited threat detection, as sandbox analysis would be restricted to a single operating system. Given that agent compatibility has been specified for both Windows and Linux environments, it is critical that sandboxing supports both operating systems. Therefore, it is requested that Windows and Linux sandboxing be mandatorily included to ensure effective detection and analysis of ransomware and advanced malware variants targeting both platforms. Clause should read as : 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 and Linux Servers.** It should not leverage existing network security layer of RSDC and must be a dedicated HIPS/EDR engine.	Refer Amended RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
34	ANNEXURE-2: TECHNICAL SPECIFICATION	71	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 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 / Linux Servers. It should not leverage existing network security layer of RSDC and must be a dedicated HIPS/EDR engine.	We would like to highlight that allowing either Windows or Linux as an option for sandboxing may weaken the overall security posture and result in limited threat detection, as sandbox analysis would be restricted to a single operating system. Given that agent compatibility has been specified for both Windows and Linux environments, it is critical that sandboxing supports both operating systems. Therefore, it is requested that Windows and Linux sandboxing be mandatorily included to ensure effective detection and analysis of ransomware and advanced malware variants targeting both platforms. Clause should read as : 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 and Linux Servers.** It should not leverage existing network security layer of RSDC and must be a dedicated HIPS/EDR engine.	Refer Amended RFP
35	ANNEXURE-2: TECHNICAL SPECIFICATION	70	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 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.	As per RFP specification mentioned, this particular point is requesting the inclusion of predefined lists of critical system files, either for operating systems or applications (such as web servers, DNS, etc.). However, it is observed that excluding the operating system/application may potentially compromise data center security. Therefore, we kindly request the inclusion of both components—operating systems and applications—for enhanced efficacy in ensuring data center security. Clause should read as : Solution should support any pre- defined lists of critical system files for various **operating systems and applications** (web servers, DNS, etc.) and support custom rules as well.	Refer Amended RFP
36	ANNEXURE-2: TECHNICAL SPECIFICATION	70	Item -1: Endpoint Detection and Response (EDR) for Blade / Rack Servers / VM - Point No. 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.	As per RFP specification mentioned, this particular point is requesting the inclusion of predefined lists of critical system files, either for operating systems or applications (such as web servers, DNS, etc.). However, it is observed that excluding the operating system/application may potentially compromise data center security. Therefore, we kindly request the inclusion of both components—operating systems and applications—for enhanced efficacy in ensuring data center security. Clause should read as : Solution should support any pre- defined lists of critical system files for various **operating systems and applications** (web servers, DNS, etc.) and support custom rules as well.	Refer Amended RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
37	ANNEXURE-2: TECHNICAL SPECIFICATION	77	Item -2: Endpoint Detection and Response (EDR) for Servers with advanced capabilities - Point No. 5.5	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.	As per RFP specification mentioned, this particular point is requesting the inclusion of predefined lists of critical system files, either for operating systems or applications (such as web servers, DNS, etc.). However, it is observed that excluding the operating system/application may potentially compromise data center security. Therefore, we kindly request the inclusion of both components—operating systems and applications—for enhanced efficacy in ensuring data center security. Clause should read as : Solution should support any pre- defined lists of critical system files for various **operating systems and applications** (web servers, DNS, etc.) and support custom rules as well.	Refer Amended RFP
38	ANNEXURE-2: TECHNICAL SPECIFICATION	77	Item -2: Endpoint Detection and Response (EDR) for Servers with advanced capabilities - Point No. 5.5	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.	As per RFP specification mentioned, this particular point is requesting the inclusion of predefined lists of critical system files, either for operating systems or applications (such as web servers, DNS, etc.). However, it is observed that excluding the operating system/application may potentially compromise data center security. Therefore, we kindly request the inclusion of both components—operating systems and applications—for enhanced efficacy in ensuring data center security. Clause should read as : Solution should support any pre- defined lists of critical system files for various **operating systems and applications** (web servers, DNS, etc.) and support custom rules as well.	Refer Amended RFP
39	ANNEXURE-2: TECHNICAL SPECIFICATION	78	Item -2: Endpoint Detection and Response (EDR) with Advanced Capabilities - Device Control - Point No. 7.1	7.1 Solution should have ability to whitelist and blacklist the external devices like USB. Solution should allow admin to create policies for group of servers to ensure secure access to external devices.	Request for Changes: **We recommend removing the USB security requirement from this proposal.** While USB controls are essential for user endpoints, server security is better achieved by hardening the physical and virtual layers. Deleting this clause will allow us to focus exclusively on the critical components of the server protection suite.	Refer Amended RFP
40	ANNEXURE-2: TECHNICAL SPECIFICATION	78	Item -2: Endpoint Detection and Response (EDR) with Advanced Capabilities - Device Control - Point No. 7.1	7.1 Solution should have ability to whitelist and blacklist the external devices like USB. Solution should allow admin to create policies for group of servers to ensure secure access to external devices.	Request for Changes: **We recommend removing the USB security requirement from this proposal.** While USB controls are essential for user endpoints, server security is better achieved by hardening the physical and virtual layers. Deleting this clause will allow us to focus exclusively on the critical components of the server protection suite.	Refer Amended RFP

SN.	RFP Chapter/Field	RFP Page No.	RFP Rule No.	Rule Details	Query/ Suggestion/ Clarification	Final Response
41	ANNEXURE-2: TECHNICAL SPECIFICATION	74	Item -2: Endpoint Detection and Response (EDR) with Advanced Capabilities - Point No. 1.4	1.4) 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 along with customized operating environments (Oracle Exadata), Appliance-based platforms (IBM pure app / Cloud pack system & Oracle exalogic / Private Cloud Appliance), and On premises micro-services servers (Red Hat Open Shift) and should support latest kernel variant of respective OS and should support auto updated agents in client server environment	Request for Changes: Assuming the platforms/environments mentioned will be considered compatible provided that the solution supports the underlying guest operating systems running on the VMs of these platforms, as explicitly listed in the requirement (MS Windows Server 2016/2019/2022 and above, RHEL 7.x/8.x/9.x and above, CentOS, Oracle Linux, SUSE Linux, Ubuntu Linux), including support for latest kernel variants and auto-updated agents. Hope the understanding is aligned as per the required usecase.	As per RFP - Support required for listed OS including latest kernels.
42	ANNEXURE-2: TECHNICAL SPECIFICATION	74	Item -2: Endpoint Detection and Response (EDR) with Advanced Capabilities - Point No. 1.4	1.4) 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 along with customized operating environments (Oracle Exadata), Appliance-based platforms (IBM pure app / Cloud pack system & Oracle exalogic / Private Cloud Appliance), and On premises micro-services servers (Red Hat Open Shift) and should support latest kernel variant of respective OS and should support auto updated agents in client server environment	Assuming the platforms /environments mentioned will be considered compatible provided that the solution supports the underlying guest operating systems running on the VMs of these platforms, as explicitly listed in the requirement (MS Windows Server 2016/2019/2022 and above, RHEL 7.x/8.x/9.x and above, CentOS, Oracle Linux, SUSE Linux, Ubuntu Linux), including support for latest kernel variants and auto-updated agents. Hope the understanding is aligned as per the required usecase.	As per RFP - Support required for listed OS including latest kernels.
43			Suggestion/Recommendation		As per MoUD, NCIIPC, DSCI, NIST and Cert-In guidelines which recommend to adhere defence in depth layered security approach by incorporating different dedicated security layers from different OEM to avoid any single point of failure. We would request you to not allow existing network security and routing switching vendor to participate for current RFP for endpoint security requirement to avoid single point of failure inline to guidelines laid down by our governing agencies.	As per RFP
44			Suggestion/Recommendation		As per MoUD, NCIIPC, DSCI, NIST and Cert-In guidelines which recommend to adhere defence in depth layered security approach by incorporating different dedicated security layers from different OEM to avoid any single point of failure. We would request you to not allow existing network security and routing switching vendor to participate for current RFP for endpoint security requirement to avoid single point of failure inline to guidelines laid down by our governing agencies.	As per RFP