RailTel Corporation of India Limited

(A Government of India Enterprise)

Plate-A, 6th Floor, Office Block Tower-2,

Block-B, East Kidwai Nagar,

New Delhi -110023

Website: www.railtelindia.com

EOI No: RCIL/CO-EB /EOI/MKTG/IREPS/SIEM Solution/2023-24/1 DATED 06.10.2023

Corrigendum-2

Subject: Extension of Bid Submission Date, Time and Updation in Annexure-4A, Pre-Bid Queries and corrigendum of end Customer

Ref: This Office EOI No. RCIL/CO-EB /EOI/MKTG/IREPS/SIEM Solution/2023-24/1 DATED 06.10.2023

With reference to EOI No. "**RCIL/CO-EB /EOI/MKTG/IREPS/SIEM Solution/2023-24/1 DATED 06.10.2023**,

1. Following are changes in submission/opening date and time

Heading	Old	New
Submission date and time	18.10.2023 at 11:00 Hrs	19.10.2023 at 15:00 Hrs
Opening date and time	18.10.2023 at 12:00 Hrs	19.10.2023 at 16:00 Hrs

2. Updated Annexure- 4A
3. Attached pre bid queries and corrigendum issued by customer
4. Updated SOR at page-79 of EoI.

All terms and conditions of the EOI remain unchanged.

Sd/

Sr. Mgr/EB

For RailTel Corporation of India Ltd.

Annexure - 4A

Group A	MANDTORY ITEMS				All Incl. Rate (Group) (Rs.)				
1	**Item Code :** 001 ** **Group A** (Goods, GST-Y) **Description:** SIEM Solution (1:1 HA) with 100000 EPS at CRIS HQ New Delhi								
	Basic Rate (Rs./Unit)			Unconditional Discount, if any (%)			Packing Charges		
	Excise Duty Type			E.D Rate Including cess			Present E.D Rate		
	Forwarding Charges (Rs./Unit)								
	Other Charges-I Desc., If any			Other Charges (I)			Make/ Brand (Self or OEM Name)		
	Consignee	**Quantity (Numbers)**		**Freight (Rs./Unit)**	**Other Charges-II**		**GST**		**All Inclusive Rate (Rs./Unit)**
		Tendered	**Offered**		**Description**	**@**	**Types**	**Rate (%)**	
	CCODE-CN	**1**	**1**						
2	**Item Code :** 002 ** **Group A** (Goods, GST-Y) **Description:** SIEM Solution (1:1 HA) with 50000 EPS at CRIS DR DC at Secunderabad								
	Basic Rate (Rs./Unit)			Unconditional Discount, if any (%)			Packing Charges		
	Excise Duty Type			E.D Rate Including cess			Present E.D Rate		
	Forwarding Charges (Rs./Unit)								
	Other Charges-I Desc., If any			Other Charges (I)			Make/ Brand (Self or OEM Name)		
	Consignee	**Quantity (Numbers)**		**Freight (Rs./Unit)**	**Other Charges-II**		**GST**		**All Inclusive Rate (Rs./Unit)**
		Tendered	**Offered**		**Description**	**@**	**Types**	**Rate (%)**	
	CCODE-CN	**1**	**1**						
3	**Item Code :** 003 ** **Group A** (Service, GST-Y) **Description:** Implementation & Configuration Charges								
	Basic Rate (Rs./Unit)			Unconditional Discount, if any (%)			Packing Charges		
	Excise Duty Type			E.D Rate Including cess			Present E.D Rate		
	Forwarding Charges (Rs./Unit)								
	Other Charges-I Desc., If any			Other Charges (I)			Make/ Brand (Self or OEM Name)		
	Consignee	**Quantity (Numbers)**		**Freight (Rs./Unit)**	**Other Charges-II**		**GST**		**All Inclusive Rate (Rs./Unit)**
		Tendered	**Offered**		**Description**	**@**	**Types**	**Rate (%)**	
	CCODE-CN	**1**	**1**						
Group B	**OPTIONAL ITEM**				**All Incl. Rate (Group) (Rs.)**				
1	**Item Code :** 004 ** **Group** B (Service, GST-Y) **Description:** AMC/ATS charges for 4th year								
	Basic Rate (Rs./Unit)			Unconditional Discount, if any (%)			Packing Charges		
	Excise Duty Type			E.D Rate Including cess			Present E.D Rate		
	Forwarding Charges (Rs./Unit)								
	Other Charges-I Desc., If any			Other Charges (I)			Make/ Brand (Self or OEM Name)		
	Consignee	**Quantity (Numbers)**		**Freight (Rs./Unit)**	**Other Charges-II**		**GST**		**All Inclusive Rate (Rs./Unit)**
		Tendered	**Offered**		**Description**	**@**	**Types**	**Rate (%)**	
	CCODE-CN	**1**	**1**						
2	**Item Code :** 005 ** **Group** B (Service, GST-Y) **Description:** AMC/ATS charges for 5th year								
	Basic Rate (Rs./Unit)			Unconditional Discount, if any (%)			Packing Charges		
	Excise Duty Type			E.D Rate Including cess			Present E.D Rate		
	Forwarding Charges (Rs./Unit)								
	Other Charges-I Desc., If any			Other Charges (I)			Make/ Brand (Self or OEM Name)		
	Consignee	**Quantity (Numbers)**		**Freight (Rs./Unit)**	**Other Charges-II**		**GST**		**All Inclusive Rate (Rs./Unit)**
		Tendered	**Offered**		**Description**	**@**	**Types**	**Rate (%)**	
	CCODE-CN	**1**	**1**						

Corrigendum for old tender no 01235199 for Supply, Installation, Configuration & Commissioning and 03 years comprehensive Warranty & Support Services of Security Information and Event Management (SIEM) at CRIS HQ, New Delhi and at CRIS DR site at Secunderabad.			
S No.	**RFP Reference Para**	**Original Clause**	**Revised Clause**
1.	Clause 6.5 Qualification Criteria Parameters II point no – 2	2. The OEM of each of the offered solutions should have at least one such successful implementations with minimum 50,000 EPS in India for SIEM solution. **Document to be provided: -** ii) The bidder shall furnish an undertaking from OEMs for at least one such successful implementation in India for SIEM solution.	2. The OEM of offered SIEM solutions should have at least two successful implementations with minimum 50,000 EPS (sustained) in India during last 05 years upto closing date of the tender. Out of which atleast one successful implementation in Govt. Sector/PSUs/Nationalized/Scheduled Banks. **Document to be provided: -** ii) The bidder shall furnish an undertaking from OEMs for at least 02 successful implementations in India for SIEM solution along with details such as P.O. / W.O. copies & successful completion / commissioning certificates from customer. **The above modified clauses shall also be applicable in Annexure IV (A) in related column/row.**
2			

3.	Annexure-I(A) :- Technical specifications- Clause A. (2)	The SIEM solution at CRIS, New Delhi, will have collectors in high availability mode. Similarly, the SIEM solution at CRIS, Secunderabad will also have collectors in high availability mode	The SIEM solution at CRIS, New Delhi, shall have 03 log collectors with a capacity of 50000 EPS each (01 collector for RIDC, 01 collector for NGeT DC & 01 collector for CRIS private cloud). Each log collector shall be in high availability mode. Similarly, the SIEM solution at CRIS, Secunderabad will also have one log collector of 75000 EPS in high availability mode.
4.	Annexure-I(A) :- Technical specifications- Clause A. (15)	The SIEM solution shall be preferably on an appliance-based platform. In the case of a software platform, the bidder shall factor in hardware, OS, database, storage and any other licence to support the SIEM solution, including scalability, with no additional cost to be borne by the customer. At any time during the currency of contract, the hardware upgradation is required to meet the requirement, the bidder has to upgrade the hardware as required without any additional cost.	The SIEM solution shall be deployed preferably on an appliance-based platform. In the case of a software platform, the bidder shall factor in required hardware, OS, database, storage and any other licence to support the SIEM solution, including scalability, with no additional cost to CRIS. Hardware requirement sizing and other required parameters should be vetted by OEM of the offered SIEM solution. The complete solution should be in HA mode for appliance based as well as software based SIEM. Storage of the solution shall be configured in RAID to achieve high availability with dual controller. At any time during the currency of contract, if any hardware or software upgradation is required to meet the requirements, the bidder has to upgrade the same without any additional cost to CRIS. Data centre rack and network connection shall be provided by CRIS at both locations and internal network connectivity shall be done by bidder. Bidder should provide the details of power and Rack space requirement for both locations along with the bid.
5.	Annexure-I(A) :- Technical specifications- Clause C. (6)	The SIEM shall have storage capacity for log retention of at least 03 months for online data (raw + normalized) and 09 months for offline data (raw + normalized). Bidders shall perform storage calculations based on an average single event size of 550 bytes.	The SIEM shall have storage capacity for log retention of at least 03 months for online data (raw + normalized) on DAS/inbuilt storage and additional 09 months for offline data (raw + normalized) on DAS/SAN/NAS etc. Bidders shall perform storage calculations based on an average single event size of 550 bytes. Archive/offline data should be available for reporting as well as operational purpose through central management dashboard directly without any manual intervention.

6.	Annexure-I(A) :- Technical specifications- Clause G. (9)	The SIEM solution shall have integration with major commercially available tools "out of the box" for triggering actions without dependency on the SOAR solution.	The SIEM solution shall have integration capability with major commercially available SOAR tools "out of the box" for triggering actions.
7.	Annexure-I(A) :- Technical specifications- Clause A. (11)	The SIEM solution shall have a web-based GUI for management, analysis and reporting	The SIEM solution shall have a web-based / Thin -Client GUI for management, analysis and reporting.
8.	Annexure-I(A) :- Technical specifications- Clause B. (3)	The SIEM solution shall support a web-based GUI for management, analysis and reporting. The SIEM solution shall not require any plug-ins, Java, Flash, or thick-client software to function.	The SIEM solution shall support a web-based/ Thin-client GUI for management, analysis and reporting. The SIEM solution shall not require any plug-ins, Java, Flash, or thick-client software to function.
9.	Clause no. 8.10	New Clause is added	The bidder shall be responsible for providing all support services (such as fine tuning, optimization, new integration, changes in solution etc.) during the currency of contract, specified or otherwise, which are required to fulfil the intent of ensuring operability, maintainability and reliability of supplied SIEM solution covered under technical specifications (Annexure –I (A)) and defined Scope of work within the quoted/contract price.
10.	Annexure-I(A) :- Technical specifications- Clause A. (5)	At CRIS, New Delhi, the SIEM solution must provide a scalable, robust architecture that can support more than 150,000 EPS without performance degradation or additional cost. Similarly, the SIEM solution at CRIS, Secunderabad, shall provide a scalable, robust architecture capable of supporting more than 75,000 EPS without performance degradation or additional cost.	At CRIS, New Delhi, hardware of the offered SIEM solution must provide a scalable, robust architecture that can support upto 150,000 EPS without performance degradation or additional cost. Similarly, hardware of the offered SIEM solution at CRIS, Secunderabad, shall provide a scalable, robust architecture capable of supporting upto 75,000 EPS without performance degradation or additional cost.
11.	Annexure-IV(A) Item no. (i) (under column - “Credential to be provided”)	Authorization letter From OEM specific to this tender as per sample Performa given in Annexure-VI (A) of tender document.	Authorization letter From OEM specific to this tender as per sample Performa given in Annexure-6 of EGCC.

12.	Contents (Page no. 2)	As per existing serial numbers	Contents serial number from 12 onwards to be read as : 13. Termination of Contract 14. Delivery Schedule & Liquidated Damages (LD) 15. Inspection, Implementation and Acceptance procedure 16. Terms and Conditions for Payment 17. Documentation 18. Training 19. Other Terms and Conditions
13.	Annexure-II (Item no. 4 & 5)	New Items added	**Item no. 4 (Optional): -** **Item Description: -** AMC/ATS charges for 4th year. **Qty. (in Nos.)** :- 01 **Item no. 5(Optional): -** **Item Description: -**AMC/ATS charges for 5th year. **Qty. (in Nos.)** :- 01
14.	Clause no. 12.1	For the purpose of relative ranking of offers, all-inclusive prices for entire schedule of requirement (SOR) of the tender shall be taken into account. The evaluation criteria shall be total value wise.	For the purpose of relative ranking of offers, all-inclusive prices for entire schedule of requirement (SOR item no. 1 to 3) of the tender shall be taken into account. Post warranty charges for 4th and 5th years are optional items and shall not be taken into consideration for relative ranking of offers.
15.	Clause no. 12.4	New Clause is added	**Post Warranty Comprehensive Maintenance (AMC/ATS) : -** The bidder shall have to quote charges for post warranty comprehensive AMC/ATS separately for the 4th and 5th year. The scope of services to be provided during AMC/ATS and the associated SLA shall be the same as specified above for the 03 year warranty period. CRIS reserves the right to enter into AMC after satisfactory completion of 03 years warranty. The PWG Bond is liable to be forfeited if the vendor refuses to enter in to AMC/ATS on completion of warranty period at rates quoted in this offer.

Response to the Bidders/OEM queries against old tender no. 01235199

Sl.No.	RFP Clause	RFP Clause	Bidder's Query/Suggestion/Remarks	CRIS response/clarifications
1	Scope of Work & Page 3, 2.2	The bidder shall carry out proposed deployment with existing infrastructure as depicted below at clause no. 3. However, the bidder shall follow the implementation architecture in accordance to industry best practice in consultation with CRIS.	As per our understanding the bidder has to deploy proposed SIEM on newly supplied hardware via this RFP. Please confirm.	Yes, bidder has to provide the requisite hardware. Please refer corrigendum for more clarity.
2	Comprehensive warranty and support services Page 8, 8.5	The Bidder shall nominate an Account Manager / Senior functionary for day-to-day coordination with CRIS throughout the warranty support service period.	Kindly clarify, the Account Manager / Senior functionary shall extend support with day-to-day coordination remotely but should be physically available as and when required.	Clause is self explanatory. Bidder to ensure meeting the SLA and support service stipulated in the RFP
3	Page 12, 14.1	The complete solution components shall be delivered at respective sites as mentioned at Annexure- III of SCC part-II within 8 weeks of placement of Purchase Order.	8 weeks for supply of hardware, complete installation with integration with all data sources, parser development (if required) and fine tuning of SIEM solution will not be feasible. Hence requesting CRIS to amend implementation timelines to at least 24 weeks.	The clauses are stipulated based on project requirements and thus no change is proposed.
4	Technical Specification, Page 16	Technical Specifications: SIEM solution (1:1 HA mode) for 100000 EPS and SIEM solution (1:1 HA mode) for 50000 EPS	As per our understanding, the SIEM solution to be designed in 1:1 HA mode (active-passive mode) and the sizing of the hardware should be designed to cater 100,000 sustained EPS independently and not via HA cluster. Please confirm.	Please refer corrigendum.
5	Technical Specification, Page 16, Clause 2	The SIEM solution at CRIS, New Delhi, will have collectors in high availability mode. Similarly, the SIEM solution at CRIS, Secunderabad will also have collectors in high availability mode.	1. Kindly confirm if bidder has to propose collectors at central location or at multiple CRIS datacenter locations. 2. Please confirm, CRIS will be providing the power, cooling, network switch and Racks required for the proposed SIEM hardware.	Please refer corrigendum.
6	Technical Specification, Page 16, Clause 3	The SIEM solution at CRIS, New Delhi shall be sized for 100,000 sustained EPS (including 13000 Flows per second) at all layers, i.e. log collection, correlation and management respectively, and shall be scalable to handle 150,000 peak EPS (including 19500 Flows per second) at all layers without any hardware upgrade. In case of burst/spike SIEM solution should not drop or queue logs upto 1,50,000 EPS from day one. Moreover there should not be any limitation on the number of log sources integrated with the solution.	1. Please confirm the SIEM license to be proposed on day-1 will be, 100,000 sustained EPS and solution should be scalable to at least 150,000 sustained EPS, additional licenses with be procured as and when required. 2. The underlying hardware to be sized for 100,000 sustained EPS or 150,000 sustained EPS on day-1.	1. Clause is self explanatory. Hardware should be able to cater 150000 EPS from day one. 2. Clause is self explanatory. Hardware should be able to cater 75000 EPS from day one.
7	Scope of work, Page 4, 2.10	The Bidder shall ensure taking Backups by Bidder before HW/ SW upgrade/ Change and recovery in case of failure of upgrade/ change, in RFP/Tender.	Please share the details of backup solution,configuration tool at CRIS.	Manual backup is to be taken before such activities for recovery in case of failure of upgrade/update/ change.
8	SIEM solution, A-Architecture Requirements, Page 16, clause 3	The SIEM solution at CRIS, New Delhi shall be sized for 100,000 sustained EPS (including 13000 Flows per second) at all layers, i.e. log collection, correlation and management respectively, and shall be scalable to handle 150,000 peak EPS (including 19500 Flows per second) at all layers without any hardware upgrade. In case of burst/spike SIEM solution should not drop or queue logs upto 1,50,000 EPS from day one. Moreover there should not be any limitation on the number of log sources integrated with the solution.	As mentioned in the Specification that Solution "shall be scalable to handle 150,000 peak EPS (including 19500 Flows per second) at all layers without any hardware upgrade. We understand that solution need to be factored for 100,000 Sustained EPS license and Hardware should be capable to handle 150,000 Peak EPS. Please Clarify.	Clause is self explanatory. Hardware should be able to cater 150000 EPS from day one.
9	SIEM solution, A-Architecture Requirements, Page 16, clause 4	The SIEM solution at CRIS, Secunderabad shall be sized for 50,000 sustained EPS (including 6500 Flows per second) at all layers, i.e. log collection, correlation and management respectively, and shall be scalable to handle 75,000 peak EPS (including 9750 Flows per second) without any hardware upgrade. In case of burst/spike SIEM solution should not drop or queue logs upto 75,000 EPS from day one. Moreover there should not be any limitation on the number of log sources integrated with the solution.	As mentioned in the Specification that Solution "shall be scalable to handle 75,000 peak EPS (including 9750 Flows per second) without any hardware upgrade" We understand that solution need to be factored for 50,000 Sustained EPS license and Hardware should be capable to handle 75,000 Peak EPS. Please Clarify.	Clause is self explanatory. Hardware should be able to cater 75000 EPS from day one.
10	SIEM solution, A-Architecture Requirements, Page 16, Clause 8	The SIEM solution should be able to integrate with both on-premises and cloud-based devices.	Please clarify if CRIS is using any cloud based services for which we need to factor collector for cloud-based devices. Do we need to consider collectors for cloud based devices at CRIS, New Delhi and CRIS, Secunderabad both the location. Please specify the EPS capacity for Log collectors and count of Log Collectors at each locations i.e. New Delhi and Secundarabad.	Hardware sizing needs to be carried out in accordance with the RFP requirement.

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
11	SIEM solution, A-Architecture Requirements, Page 17, Clause 12	The SIEM solution shall be provided with complete failover mode.	As per our understanding High Availability is required at management Console and Collectors layer only as per Technical Specifications Point 1 & 2. High Availability at other layers/components, such as storage, is not required. Please Clarify	Please refer corrigendum.
12	SIEM solution, C-Log/Data Collection & Management, Page 19, Clause 6	The SIEM shall have storage capacity for log retention of at least 03 months for online data (raw + normalized) and 09 months for offline data (raw + normalized). Bidders shall perform storage calculations based on an average single event size of 550 bytes.	As per our understanding storage needs to be factored for 100% utilization considering 550 Bytes and with retention time period as below. For e.g. at Data Centre for calculations a.Retention required for RAW + Normalised data is 3 Months Online on SAN should be factored for min 1 PB. b.Archived Log Data retention will be for 12 Months out of which 3 Months of data should be factored for min 200 TB on SAN for fast reterivel of historical logs and 9 months of data should be factored for minimum 500TB on NAS/Tape library. Kindly clarify minimum storage required at DC and DR respectively, Retention period and type of storage for Online Data and Offline Data respectively. Also , kindly specify any RAID level for storage required.	Please refer corrigendum.
13	SIEM solution,G-Incident handling, Page 23, Clause 9	The SIEM solution shall have integration with major commercially available tools "out of the box" for triggering actions without dependency on the SOAR solution.	Technically the Workflow of SIEM is to consume alerts and feed the alerts to SOAR solution for response and trigger action. The Specification mentioned is restrictive and technically the feature asked is restrictive we request to change the Clause as "The SIEM solution shall have integration with major commercially available SOAR solution "out of the box" for triggering actions"	Please refer corrigendum.
14		Additional Technical Clause	Its recommended that a Next GEN SIEM should have support for inbuilt multiple advance technologies. Hence we recommend CRIS to ask for the following feature proof and latest technologies which is supported by SIEM and can be used in Future if required. 1. Next generation platform shall encompass log data with added context and threat intelligence. It should have inbuilt NDR functionality with Packet/Deep Packet inspection and EDR solution to provide complete network and endpoint visibility through deep packet inspection, high speed packet capture and analysis. 2. The Analyst UI must be a common interface to investigate data collected and normalized for SIEM (Logs) and DPI (Packet data) to correlate Logs and Packets using a single rule. 3. Proposed SIEM should have hardened OS based architecture where Operating system, SIEM software should be managed by the SIEM OEM only. 4.SIEM should have the ability to natively collect logs from logstash 5.Solution should be able to alert the analyst of any threat intel match in real time by infusing the threat intel with raw logs during normalization phase.	The specification items are stipulated based on project requirement and thus no change is proposed.

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
15	Qualification Criteria Parameters, Page 7	The OEM of each of the offered solutions should have at least one such successful implementations with minimum 50,000 EPS in India for SIEM solution.	OEM should have experience of similar scale , complexity and environment. Accordingly, we would kindly request CRIS to amend clause as below " The OEM of each of the offered solutions should have at least two (2) such successful implementations with Sign Off with minimum 50,000 EPS in India for SIEM solution deployed in Government Departments in India. OEM to provide complete customer documentary evidence to prove that their solutuon is sucessfully deployed. "	Please refer corrigendum.
16	Qualification Criteria Parameters, Page 7	The bidder should be a Private/Public Company registered under Companies Act 2013 or a registered cooperative society or Proprietorship/ Partnership firm and should be registered for more than 5 years as on date of closing of tender.	We would kindly request CRIS to ensure bidder and OEM both are in Business for more than 10 years from date of closing of tender. Accordingly,we would request CRIS to amend the clause as per below "The bidder and OEM both respectively should be a Private/Public Company registered under Companies Act 2013 or a registered cooperative society or Proprietorship/ Partnership firm and should be registered for more than 10 years as on date of closing of tender. "	The clauses are stipulated based on project requirements and thus no change is proposed.
17				
18	Delivery Schedule & Liquidated Damages (LD), Page number 12, clause 14	14.1 The complete solution components shall be delivered at respective sites as mentioned at Annexure- III of SCC part-II within 8 weeks of placement of Purchase Order.	Would request you to please confirm if this timeline can be relaxed 16 Weeks, also details on the key deliverables/Milestone	The clauses are stipulated based on project requirement and thus no change is proposed.
19	Inspection, Implementation and Acceptance procedure, Page number 13, Clause 15.8	15.8 Final Acceptance Testing shall be done for the supplied equipment as per the ATP (Acceptance Test Procedure) given in Annexure-I(B). a) Installation of equipment and its integration with existing infrastructure.	Please confirm if OLD SIEM log integration is required with new SIEM tool or if this can be relaxed.	Integration with existing SIEM is not required.
20	Page number 9, Clause 9.2	Total Service failure or Degradation in system performance	Please confirm how performance degration criteria will be defined, Basis on which penalties will be charged.	Clause is self-explanatory.
21	Annexure-II, Page 30	SIEM Solution (1:1 HA Mode) with 50000 EPS at CRIS DR DC at Secunderabad	Log retention expectation & Log availability expecation whenever DR drill is conducted or DR Site is invoked what is is expectation for being in HA	SIEM solution at CRIS secunderabad is independent solution for ICT infrastructure deployed at CRIS, Secunderabad.
22	Scope of work, Page number 4, clause 2.12	The bidder shall ensure that all BYODs shall be kept free of Malware and under V-M-C (visibility, monitoring and control) of CRIS.	Please confirm if this can relaxed & as Monitoring & Management is not in Bidder's scope.	The clauses are stipulated based on project requirement and thus no change is proposed.
23	C. Log/Data Collection & Management, Page number 19, clause 6	The SIEM shall have storage capacity for log retention of at least 03 months for online data (raw + normalized) and 09 months for offline data (raw + normalized). Bidders shall perform storage calculations based on an average single event size of 550 bytes.	Please confirm Log retention required for DR site.	Please refer corrigendum.
24	Annexure-II, Page number 30 , Clause	SIEM Solution (1:1 HA Mode) with 50000 EPS at CRIS DR DC at Secunderabad	Please confirm which mode DR site will function (Active-Passive) or (Active-Active) mode.	SIEM solution at CRIS secunderabad is independent solution for ICT infrastructure deployed at CRIS, Secunderabad.
25	SCC Part-II, Page 12, Clause 6 to 9	SCOPE OF WORK; SYSTEM DEPLOYMENT ARCHITECTURE; DETAILED SCOPE OF WORK; Comprehensive Warranty Support & ATS Services including SLA/penalties	Both parties agree to mutually discuss LDs applicable to current scope under RFP.	Clauses are self explanatory

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
26	SCC Part-II, Page 12, Clause 6 to 9	Does the SOW cover Managed services as well? Below asks in the RFP are considered managed services by Tata Communications The Bidder shall ensure half yearly visit of expert for health checkup, update/ upgrades in case of no failure calls, in RFP/Tender In case of any performance or failure issue in accessing the services of offered solutions, the bidder shall arrange support engineer on site for timely resolution of the issue The Bidder shall ensure taking Backups by Bidder before HW/ SW upgrade/ Change and recovery in case of failure of upgrade/ change, in RFP/Tender The bidder shall ensure that all BYODs shall be kept free of Malware and under V-M-C (visibility, monitoring and control) of CRIS. Internal audit shall be undertaken by CRIS, any non-compliances will need to be resolved by the bidder in coordination with CRIS. The bidder should have a centralized helpdesk for logging of complaints. After the call is logged, the complainant shall receive a call back within 1 hour to brief the status of the call logged and the details of the engineer to whom the call is assigned, for efficient and quick resolution of the problem. The Bidder shall nominate an Account Manager / Senior functionary for day-to-day coordination with CRIS throughout the warranty support service period The Bidder shall provide Upgrades and Updates for all offered solutions as and when released by respective OEMs and shall be made available free of cost. Patch installation and software upgrades of offered solutions shall be carried out by the bidder as per the OEM recommendations. The solution provided by the bidder should not be declared end of sale within 2 years from the date of placement of PO. If any of the solution is declared end of sale within 2 years of placement of PO, the bidder has to provide the equivalent/upgraded solution without any financial implication to CRIS All the equipment shall have on-site warranty support i.e. the repair / replacement of faulty units during the warranty period has to be ensured at CRIS, New Delhi and DR DC, Secunderabad after the complaint is lodged at the nearest customer support office	CRIS SIEM RFP is for on premises SIEM, complete SIEM solution will be hosted in CRIS HQ DC and SC DR DC. Managed service is not in scope of this tender.	Clauses are self explanatory. Bidder to ensure requsite support services as per RFP terms and conditions.
27	Page 12, Clause 14	Liquidated damages in Delay in Delivery and Commissioning	Bidders requests that clause be amended to include additional 30 days' time period to be provided prior to levy of LD; LD must be sole and exclusive remedy wrt Supplier's failure to provide services in question by the due date. Further, both parties agree to mutually discuss LDs applicable to this deal.	The clauses are stipulated based on project requirement and thus no change is proposed.
28	Annexure - I (B), Page number 33,	Acceptance Test Procedure (ATP)	Bidder proposes to add time frame to 2 business days within which Customer must accept/reject our services, else services shall be deemed accepted	The clauses are stipulated based on project requirement and thus no change is proposed.
29	Page number 14, clause 16	Payment Terms	Bidder proposes to add payment term of 30 days i.e., Customer shall pay all amounts due within thirty (30) days from the date of invoice, to the bank account designated by Bidder, from time to time.	The clauses are stipulated based on project requirement and thus no change is proposed.
30	Page number 14, clause 19	Other Terms & Conditions: As per CRIS EGCC (Including modifications)	Please provide document being referred herein?	Please refer CRIS website i.e. www.cris.org.in and IREPS portal i.e. www.ireps.gov.in for EGCC.
31	Page 7, 1. (ii) 2.	OEM Undertaking : The OEM of each of the offered solutions should have at least one such successful implementations with minimum 50,000 EPS in India for SIEM solution.	Please modify the clause as : The OEM of each of the offered solutions should have at least one such successful implementations with minimum 30,000 EPS in India for SIEM solution.	The clauses are stipulated based on project requirement and thus no change is proposed.
32		Integration with existing infrastructure (Application, DB, Servers, Network & security devices and other ICT components) at CRIS, New Delhi, and DR DC, Secunderabad shall be done by bidder's engineer deputed at site.	Please provide the Volumetric for the current infrastructure which includes Network Deices, VM's including the Current EPS count in DR and DC	Please refer technical specifications for type of ICT infrastructure. However, the total no. of server (OS instances) are about 4000 servers for CRIS Chanakyapuri, New Delhi and about 2000 servers for CRIS, Secunderabad can be taken into consideration. The network and security devices are not included in this sizing.
33	Page 14, clause 16.2	Confirmation of the validity of PBG Bond of 10% of the value of the Purchase Order for a period up to 3 months beyond contract period.	When will the PBG amount provided back to the Bidder.	As per tender conditions PBG will be returned three months after all contractual obligations are completed by the Vendor
34	Page 3, clause 2.4	In case of any performance or failure issue in accessing the services of offered solutions, the bidder shall arrange support engineer on site for timely resolution of the issue.	What will be the Scope of expertise, Issue type and Skill that will be required to be Provided by Support engineer at Site	Bidder shall ensure adequate support to CRIS for meeting the SLA and support service stipulated in the RFP.
35	SLA & Damage charges for service unavailability, Page 9, clause 9.2	Damage charges shall be calculated on the basis of total service failure, no. of failure instances, duration of single failure instance as well as individual device/part failure. In case multiple clauses are applicable, the higher one shall be charged. Damage charges shall be calculated as per table given below:	Relaxation required for the Damage charges and Penalty	The clauses are stipulated based on project requirement and thus no change is proposed.

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
36				
37				
38	Page 9	9 SLA & Damage charges for service unavailability (complete clause)	We request CRIS to reduce the SLA penalty as these penalty are at very higher sides	The clauses are stipulated based on project requirement and thus no change is proposed.
39	Page 12	14.1 The complete solution components shall be delivered at respective sites as mentioned at Annexure- III of SCC part-II within 8 weeks of placement of Purchase Order	We request CRIS to please increase the delivery timelines from 8 weeks to 12 weeks and provide 4 weeks for the installation	The clauses are stipulated based on project requirement and thus no change is proposed.
40				
41	Page 7	The OEM of each of the offered solutions should have at least one such successful implementations with minimum 50,000 EPS in India for SIEM solution.	We request CRIS to provide relaxation and kinldy consider allow 20K EPS or Device based licensing model with minimum 500 GB per day /Device based as a proof	The clauses are stipulated based on project requirement and thus no change is proposed.
42		**9. SLA & Damage charges for service unavailabilit**y: All penalties shall be recovered from the invoices/PBG/deposit/any other payment to the bidder. The overall penalties will be capped at 10% of the contract value including taxes, duties, etc. which is in addition to any applicable LD. In case the total damages exceed the maximum limit, CRIS reserves the right to cancel the contract and forfeit the PBG	We request CRIS to reduce the Penalty clause Less than 5%	The clauses are stipulated based on project requirement and thus no change is proposed.
43	SIEM solution, A-Architecture RequirementsPage 16, Point 3	The SIEM solution at CRIS, New Delhi shall be sized for 100,000 sustained EPS (including 13000 Flows per second) at all layers, i.e. log collection, correlation and management respectively, and shall be scalable to handle 150,000 peak EPS (including 19500 Flows per second) at all layers without any hardware upgrade. In case of burst/spike SIEM solution should not drop or queue logs upto 1,50,000 EPS from day one. Moreover there should not be any limitation on the number of log sources integrated with the solution.	As mentioned in the Specification that Solution "shall be scalable to handle 150,000 peak EPS (including 19500 Flows per second) at all layers without any hardware upgrade. We understand that solution need to be factored for 100,000 Sustained EPS license and Hardware should be capable to handle 150,000 Peak EPS. Please Clarify.	1. Clause is self explanatory. Hardware should be able to cater 150000 EPS from day one. 2. Clause is self explanatory. Hardware should be able to cater 75000 EPS from day one.
44	SIEM solution, A-Architecture RequirementsPage 16, Point 4	The SIEM solution at CRIS, Secunderabad shall be sized for 50,000 sustained EPS (including 6500 Flows per second) at all layers, i.e. log collection, correlation and management respectively, and shall be scalable to handle 75,000 peak EPS (including 9750 Flows per second) without any hardware upgrade. In case of burst/spike SIEM solution should not drop or queue logs upto 75,000 EPS from day one. Moreover there should not be any limitation on the number of log sources integrated with the solution.	As mentioned in the Specification that Solution "shall be scalable to handle 75,000 peak EPS (including 9750 Flows per second) without any hardware upgrade" We understand that solution need to be factored for 50,000 Sustained EPS license and Hardware should be capable to handle 75,000 Peak EPS. Please Clarify.	Please refer corrigendum
45	SIEM solution, A-Architecture RequirementsPage 16, Point 8	The SIEM solution should be able to integrate with both on-premises and cloud-based devices.	Please clarify if CRIS is using any cloud based services for which we need to factor collector for cloud-based devices. Do we need to consider collectors for cloud based devices at CRIS, New Delhi and CRIS, Secunderabad both the location. Please specify the EPS capacity for Log collectors and count of Log Collectors at each locations i.e. New Delhi and Secundarabad.	Hardware sizing needs to be carried out in accordance with the RFP requirement.
46	SIEM solution, A-Architecture RequirementsPage 17, Point 12	The SIEM solution shall be provided with complete failover mode.	As per our understanding High Availability is required at management Console and Collectors layer only as per Technical Specifications Point 1 & 2. High Availability at other layers/components, such as storage, is not required. Please Clarify	Please refer corrigendum

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
47	SIEM solution, C-Log/Data Collection & Management, Page 19, Point 6	The SIEM shall have storage capacity for log retention of at least 03 months for online data (raw + normalized) and 09 months for offline data (raw + normalized). Bidders shall perform storage calculations based on an average single event size of 550 bytes.	As per our understanding storage needs to be factored for 100% utilization considering 550 Bytes and with retention time period as below. For e.g. at Data Centre for calculations a.Retention required for RAW + Normalised data is 3 Months Online on SAN should be factored for min 1 PB. b.Archived Log Data retention will be for 12 Months out of which 3 Months of data should be factored for min 200 TB on SAN for fast reterivel of historical logs and 9 months of data should be factored for minimum 500TB on NAS/Tape library. Kindly clarify minimum storage required at DC and DR respectively, Retention period and type of storage for Online Data and Offline Data respectively. Also , kindly specify any RAID level for storage required.	Please refer corrigendum
48	SIEM solution,G-Incident handling, Page 23,Point 9	The SIEM solution shall have integration with major commercially available tools "out of the box" for triggering actions without dependency on the SOAR solution.	Technically the Workflow of SIEM is to consume alerts and feed the alerts to SOAR solution for response and trigger action. The Specification mentioned is restrictive and technically the feature asked is restrictive we request to change the Clause as "The SIEM solution shall have integration with major commercially available SOAR solution "out of the box" for triggering actions"	Please refer corrigendum
49		Additional Technical Clause	Its recommended that a Next GEN SIEM should have support for inbuilt multiple advance technologies. Hence we recommend CRIS to ask for the following feature proof and latest technologies which is supported by SIEM and can be used in Future if required. 1. Next generation platform shall encompass log data with added context and threat intelligence. It should have inbuilt NDR functionality with Packet/Deep Packet inspection and EDR solution to provide complete network and endpoint visibility through deep packet inspection, high speed packet capture and analysis. 2. The Analyst UI must be a common interface to investigate data collected and normalized for SIEM (Logs) and DPI (Packet data) to correlate Logs and Packets using a single rule. 3. Proposed SIEM should have hardened OS based architecture where Operating system, SIEM software should be managed by the SIEM OEM only. 4.SIEM should have the ability to natively collect logs from logstash 5.Solution should be able to alert the analyst of any threat intel match in real time by infusing the threat intel with raw logs during normalization phase.	The clauses are stipulated based on project requirement and thus no change is proposed.
50	Qualification Criteria Parameters, Page 7	The OEM of each of the offered solutions should have at least one such successful implementations with minimum 50,000 EPS in India for SIEM solution.	OEM should have experience of similar scale , complexity and environment. Accordingly, we would kindly request CRIS to amend clause as below " The OEM of each of the offered solutions should have at least two (2) such successful implementations with Sign Off with minimum 50,000 EPS in India for SIEM solution deployed in Government Departments in India. OEM to provide complete customer documentary evidence to prove that their solutuon is sucessfully deployed. "	Please refer corrigendum

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
51				
52				
53	Qualification Criteria Parameters, Pg 6	Additional Clause Suggestion	OEM to have ability to provide support from India and should have at significant team based in India for Support/R&D activities. Accordingly, we would kindly request CRIS to add the following clause. "OEM should have India based support for offered products & related issues with first level support point in India which should be available on 24x7x365 basis. The Technical Assistance Centers (TAC) / Support Centre/Product Engineering based in India should offer post-sales support including Tele-Support for the offered products & related issues having atleast 100 Seats based in India. "	The clauses are stipulated based on project requirement and thus no change is proposed.
54				
55	Annexure – IV (A) OEM Undertaking	2. The OEM of each of the offered solutions should have at least one such successful implementations with minimum 50,000 EPS in India for SIEM solution.	Quoted Solution must have its presence in India for more than 10 years and must have at least 2 deployments along with customer signoff for more than 50000 EPS in Government of India organization and 1 deployment along with customer signoff for more than 100000 EPS in Government of India organization	Please refer corrigendum
56	Annexure-I(A) Technical Specifications:	Additional Point	The proposed SIEM OEM must be an industry standard, enterprise grade solution and shall be present in Magic Quadrant of Forrester / Gartner / IDC report for SIEM in last three years	The clauses are stipulated based on project requirement and thus no change is proposed.
57	Annexure-I(A) Technical Specifications:	11. The SIEM solution shall have a web-based GUI for management, analysis and reporting.	The SIEM solution shall have a web-based / **Thin -Client** GUI for management, analysis and reporting.	Please refer corrigendum
58	Annexure-I(A) Technical Specifications: B Administration	2. The SIEM solution shall provide central management of all components and administrative functions from a single management console. All components of the SIEM solution shall be managed centrally via a single graphical user interface.	The SIEM solution shall provide central management of all components ~~**and administrative functions**~~ from a single management console. All components of the SIEM solution shall be managed centrally via a single graphical user interface.	The clauses are stipulated based on project requirement and thus no change is proposed.
59	Annexure-I(A) Technical Specifications: B Administration	3. The SIEM solution shall support a web-based GUI for management, analysis and reporting. The SIEM solution shall not require any plug-ins, Java, Flash, or thick-client software to function.	3. The SIEM solution shall support a web-based / **Thin - Client** GUI for management, analysis and reporting. The SIEM solution shall not require any plug-ins, Java, Flash, or thick-client software to function.	Please refer corrigendum
60	Annexure-I(A) Technical Specifications: D Correlation and Analytics	1. The SIEM solution shall provide analytics on the data that is being collected and enriched.	The SIEM solution shall provide analytics and **realtime correlation** on the data that is being collected and enriched.	The clauses are stipulated based on project requirement and thus no change is proposed.
61	Annexure-I(A) Technical Specifications: G Incident handling	9. The SIEM solution shall have integration with major commercially available tools "out of the box" for triggering actions without dependency on the SOAR solution.	The SIEM solution shall have integration with major commercially available tools Out of the Box for triggering actions ~~**without dependency on the SOAR solution.**~~	Please refer corrigendum
62	Annexure-I(A) Technical Specifications:	Additional Point	**Changes Required:** SIEM solution must support in- memory correlations or near real-time correlations. Correlations rules must trigger before writing logs in database	The clauses are stipulated based on project requirement and thus no change is proposed.

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
63	Annexure-I(A) Technical Specifications:	Additional Point	**Changes Required:** SIEM solution must use data security by encrypting sensitive data with correlation capabilities on those encrypted fields	
64	Annexure-I(A) Technical Specifications:	Additional Point	**Changes Required:** Solution should have integration with threat intelligence feed (i.e. Virus Total, MISP etc) as well its own threat intelligence platform to have collaborative IOCs to enrich information for security analyst decision	
65	Annexure-I(A) Technical Specifications:	Additional Point	**Changes Required:** This ensures no surplus license cost to bidder/customer for SOAR while avail full loaded SOAR functionality throughout project tenure or active entitlement of the contract. If SOAR is not a primary requirement then native SOAR can be installed in future with just adding additional hardware.	
66	Pg no. 3	Integration with existing infrastructure (Application, DB, Servers, Network & security devices and other ICT components) at CRIS, New Delhi, and DR DC, Secunderabad shall be done by bidder's engineer deputed at site.	As per our understanding, Bidder will provide commands / scripts to CRIS team for enabling syslog, flow etc. However, enabling command on end devices will be carried out by respective solution owners. Kindly confirm.	Clause is self-explanatory. The bidder is required to provide requisite support for integration with existing infrastructure.
67	Pg no. 3	Supply, Installation, Configuration & Commissioning and 03 years comprehensive Warranty &Support Services of Security Information and Event Management (SIEM) at CRIS HQ, New Delhi and at CRIS DR site at Secunderabad as per the technical specifications given in Annexure-I (A) of SCC part-II.	As per our understanding, CRIS will provide rack, space, power, cooling, network switch connectivity etc. However, bidder will bring patch cords, power cables etc. to connect existing power rack supply and network switches. Kindly confirm.	Please refer corrigendum
68			Please furnish details of the total server count in CRIS environment which will be directly or indirectly integrated into the SIEM platform. This should include all categories such as production, non-production, testing & UAT setup (physical and virtual both).	Please refer technical specifications for type of ICT infrastructure. However, the total no. of server (OS instances) are about 4000 servers for CRIS Chanakyapuri, New Delhi and about 2000 servers for CRIS, Secunderabad can be taken into consideration. The network and security devices are not included in this
69			Please clarify , if only hardware is required for 1,50,000 EPS & 75,000 EPS with storage for the same or the license also need to be factored for the same for this additional value.	Please refer corrigendum.
70	Page no. 17	The SIEM solution should be able to integrate with two-factor authentication.	We support multi factor authentication in most of our cloud offerings. For on premise offerings, we do not support 2FA. AD authentiation and Role based access controls are possible. Would request to rephrase the clause as - The SIEM solution should support integartions with Active Directory or Radius server for Autehntication. It should also support role based access controls.	The clauses are stipulated based on project requirement and thus no change is proposed.
71	Page no. 19	The SIEM solution shall be able to consume logs from any log source without writing parser before hand or while integration. Parsers shall be built once the log is ingested.	Kindly rephrase the clause to make it more generic - The solution must supply own API and graphical tools for creating new connectors or similar parsing solution. The solution provide ease of use regular expression based ability to create custom parsers.	Clause is self explanatory.
72	Page no. 20	The SIEM solution shall supports protocols like syslog, JDBC, API, WMI, SFTP, FTP, SCP, SNMP, MQ etc. on single software/hardware appliance.	MQ is a vendor specific protocol typiclly required on distributed systems.Would request you to remove the protocol and rephrase the clause as - The SIEM solution shall supports protocols like syslog, JDBC, API, WMI, SFTP, FTP, SCP, SNMP, Netflow etc. on single software/hardware appliance.	The clauses are stipulated based on project requirement and thus no change is proposed.
73	Page no. 23	The SIEM solution shall include at the very least the following out-of-the-box use cases for Cloud Security Monitoring: -shall have out of the box rules, dashboards, and reports for MITRE ATTACK Cloud Matrix tactics, techniques, and sub-techniques. - Monitor cloud compute instances for activities related to cryptojacking/crypto mining. -Monitor potentially malicious behaviour, for example, new instances that originate from previously unseen regions, users who launch abnormally high numbers of instances, or compute instances started by previously unseen users, etc. -SIEM solution shall also provide several dashboards out of the box to give views on performance, health, configuration, and security of the cloud environment. It shall also have a topology view, which shall provide a dynamic map of cloud resources and their relationships etc.	We understand this is an on-premise requirement. The asked specifications are for cloud based security analytics platforms. We therefore request to remove the requirement.	The clauses are stipulated based on project requirement for CRIS Private Clolud and thus no change is proposed.
74	Page no. 23	The SIEM solution shall have Incident review framework to facilitate incident tracking, investigation, pivoting and closure.	Kindly clarify the ask for pivoting. Our SIEM solution provides a Incident management framework that can help in incident tracking, investigation and closure.	The clauses are stipulated based on project requirement and thus no change is proposed.

Response to the Bidders/OEM queries against old tender no. 01235199

Sl.No.	RFP Clause	RFP Clause	Bidder's Query/Suggestion/Remarks	CRIS response/clarifications
75	Page no. 23	The SIEM solution should be able to provide the capability to build a chronological timeline for the incident before and after a triggered event.	Kindly rephrase the clause as - The SIEM solution should be able to provide the capability to build a chronological timeline for the incident before and after a triggered event or it should integrate with a third party Incident management tool to provide the same capability.	The clauses are stipulated based on project requirement and thus no change is proposed.
76	Page no. 23	The SIEM solution shall boost productivity by highlighting only incidents with a high risk impact and a high level of confidence.	Kindly remove the clause as this is specific to a vendor.	The clauses are stipulated based on project requirement and thus no change is proposed.
77	Page no. 23	The SIEM solution shall be able to search and review responses and their outcomes, as well as manage domain-specific workflow actions.	Kindly remove the clause as this is specific to a vendor.	The clauses are stipulated based on project requirement and thus no change is proposed.
78	Page no. 23	The SIEM solution shall have integration with major commercially available tools "out of the box" for triggering actions without dependency on the SOAR solution.	Kindly rephrase the clause to make it more generic - Solution should be able support following actions based on configurable the condition defined; Log Event, Create a Case, Execute a Script, Send Message, Generate Reports, modify a watch list, Trigger an automatic IPS block, etc.	Please refer corrigendum
79	SIEM solution, A-Architecture RequirementsPage 16, Point 3	The SIEM solution at CRIS, New Delhi shall be sized for 100,000 sustained EPS (including 13000 Flows per second) at all layers, i.e. log collection, correlation and management respectively, and shall be scalable to handle 150,000 peak EPS (including 19500 Flows per second) at all layers without any hardware upgrade. In case of burst/spike SIEM solution should not drop or queue logs upto 1,50,000 EPS from day one. Moreover there should not be any limitation on the number of log sources integrated with the solution.	As mentioned in the Specification that Solution "shall be scalable to handle 150,000 peak EPS (including 19500 Flows per second) at all layers without any hardware upgrade. We understand that solution need to be factored for 100,000 Sustained EPS license and Hardware should be capable to handle 150,000 Peak EPS. Please Clarify.	Clause is self explanatory. Hardware should be able to cater 150000 EPS from day one.
80	SIEM solution, A-Architecture RequirementsPage 16, Point 4	The SIEM solution at CRIS, Secunderabad shall be sized for 50,000 sustained EPS (including 6500 Flows per second) at all layers, i.e. log collection, correlation and management respectively, and shall be scalable to handle 75,000 peak EPS (including 9750 Flows per second) without any hardware upgrade. In case of burst/spike SIEM solution should not drop or queue logs upto 75,000 EPS from day one. Moreover there should not be any limitation on the number of log sources integrated with the solution.	As mentioned in the Specification that Solution "shall be scalable to handle 75,000 peak EPS (including 9750 Flows per second) without any hardware upgrade" We understand that solution need to be factored for 50,000 Sustained EPS license and Hardware should be capable to handle 75,000 Peak EPS. Please Clarify.	Clause is self explanatory. Hardware should be able to cater 150000 EPS from day one.
81	SIEM solution, A-Architecture RequirementsPage 16, Point 8	The SIEM solution should be able to integrate with both on-premises and cloud-based devices.	Please clarify if CRIS is using any cloud based services for which we need to factor collector for cloud-based devices. Do we need to consider collectors for cloud based devices at CRIS, New Delhi and CRIS, Secunderabad both the location. Please specify the EPS capacity for Log collectors and count of Log Collectors at each locations i.e. New Delhi and Secundarabad.	Hardware sizing needs to be carried out in accordance with the RFP requirement.
82	SIEM solution, A-Architecture RequirementsPage 17, Point 12	The SIEM solution shall be provided with complete failover mode.	As per our understanding High Availability is required at management Console and Collectors layer only as per Technical Specifications Point 1 & 2. High Availability at other layers/components, such as storage, is not required. Please Clarify	Please refer corrigendum
83	SIEM solution, C-Log/Data Collection & Management, Page 19, Point 6	The SIEM shall have storage capacity for log retention of at least 03 months for online data (raw + normalized) and 09 months for offline data (raw + normalized). Bidders shall perform storage calculations based on an average single event size of 550 bytes.	As per our understanding storage needs to be factored for 100% utilization considering 550 Bytes and with retention time period as below. For e.g. at Data Centre for calculations a.Retention required for RAW + Normalised data is 3 Months Online on SAN should be factored for min 1 PB. b.Archived Log Data retention will be for 12 Months out of which 3 Months of data should be factored for min 200 TB on SAN for fast reterivel of historical logs and 9 months of data should be factored for minimum 500TB on NAS/Tape library. Kindly clarify minimum storage required at DC and DR respectively, Retention period and type of storage for Online Data and Offline Data respectively. Also , kindly specify any RAID level for storage required.	Please refer corrigendum

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
84	SIEM solution,G-Incident handling, Page 23,Point 9	The SIEM solution shall have integration with major commercially available tools "out of the box" for triggering actions without dependency on the SOAR solution.	Technically the Workflow of SIEM is to consume alerts and feed the alerts to SOAR solution for response and trigger action. The Specification mentioned is restrictive and technically the feature asked is restrictive we request to change the Clause as "The SIEM solution shall have integration with major commercially available SOAR solution "out of the box" for triggering actions"	Please refer corrigendum
85		Additional Technical Clause	Its recommended that a Next GEN SIEM should have support for inbuilt multiple advance technologies. Hence we recommend CRIS to ask for the following feature proof and latest technologies which is supported by SIEM and can be used in Future if required. 1. Next generation platform shall encompass log data with added context and threat intelligence. It should have inbuilt NDR functionality with Packet/Deep Packet inspection and EDR solution to provide complete network and endpoint visibility through deep packet inspection, high speed packet capture and analysis. 2. The Analyst UI must be a common interface to investigate data collected and normalized for SIEM (Logs) and DPI (Packet data) to correlate Logs and Packets using a single rule. 3. Proposed SIEM should have hardened OS based architecture where Operating system, SIEM software should be managed by the SIEM OEM only. 4.SIEM should have the ability to natively collect logs from logstash 5.Solution should be able to alert the analyst of any threat intel match in real time by infusing the threat intel with raw logs during normalization phase.	The specification items are stipulated based on project requirement and thus no change is proposed.
86	Qualification Criteria Parameters, Page 7	The OEM of each of the offered solutions should have at least one such successful implementations with minimum 50,000 EPS in India for SIEM solution.	OEM should have experience of similar scale , complexity and environment. Accordingly, we would kindly request CRIS to amend clause as below " The OEM of each of the offered solutions should have at least two (2) such successful implementations with Sign Off with minimum 50,000 EPS in India for SIEM solution deployed in Government Departments in India. OEM to provide complete customer documentary evidence to prove that their solutuon is sucessfully deployed. "	Please refer corrigendum
87				
88				

Response to the Bidders/OEM queries against old tender no. 01235199				
Sl.No.	**RFP Clause**	**RFP Clause**	**Bidder's Query/Suggestion/Remarks**	**CRIS response/clarifications**
89	Qualification Criteria Parameters, Pg 6	Additional Clause Suggestion	OEM to have ability to provide support from India and should have at significant team based in India for Support/R&D activities. Accordingly, we would kindly request CRIS to add the following clause. "OEM should have India based support for offered products & related issues with first level support point in India which should be available on 24x7x365 basis. The Technical Assistance Centers (TAC) / Support Centre/Product Engineering based in India should offer post-sales support including Tele-Support for the offered products & related issues having atleast 100 Seats based in India. "	The clauses are stipulated based on project requirements and thus no change is proposed.
90				
91				
92				

Updated SOR @ Page-79 of EoI

Schedule of Requirement (SoR)		
S.No.	Item Description	Qty. (in Nos.)
1	SIEM Solution (1:1 HA Mode) with 100000 EPS at COR HQ New Delhi	1
2	SIEM Solution (1:1 HA Mode) with 50000 EPS at COR Secunderabad	1
3	Implementation & Configuration charges	1