			RFP	for procurement of Network APT Solution - RFP		.03.2022."	
C N	Document	Page	Clause No	Consolidated list of Replie	es to Pre-bid Queries	Additional Remarks (if any)	NPCI Response
0	Reference	No	Clause NO			Additional Remarks (if any)	INFCI Response
1	RFP	21	7.3	Customer BFSI reference in India (Bidder & OEM) Please provide at least 2 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct	Customer BFSI/ Govt. PSU reference in India (Bidder/ OEM) Please provide at least 2 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and		No change in RFP. Bidder should have experience of implementing network APT solution in at least 2 BFSI companies.
2	RFP	10	3.1 Scope of work:	telephone number Debider should ensure availability of on-site resource if required for troubleshooting and resolution of technical issues back-to-back support from OEM.	direct telephone number Request customer to please specify the requirement		Bidder should be available on NPCI site (Chennai/Hyderaba d) in case if technical issues cannot be resolved remotely.
3	RFP	25	8.10 Delivery schedule	 8.10 Delivery schedule Delivery, Installation & commissioning of the solution should be completed within 12 weeks from the date of receipt of purchase order. Delivery of hardware, software, and license should be within 6 weeks. Installation & commissioning should be completed in next 6 weeks. 	Request customer to please revise the timelines as below: • Delivery of hardware, software, and license should be within 24 weeks • Installation & commissioning should be completed in next 8 weeks.		Refer to corrigendum
4	RFP	25	8.11 Penalty for default in delivery	Non Delivery of above at NPCI - at the rate of 0.5% of the total Purchase Order value for each week's delay beyond the stipulated delivery period subject to a maximum of 5% of the Purchase Order value, without prejudice to any other right or remedy available under the Purchase Order.	Request customer to please cap the max penalty to 10% of purchase order value		No change in RFP

5	RFP	28	8.15 Penalty on non- adherence to SLAs:	a) Penalty for Severity 1 Incidents: Any violation in meeting the above SLA requirements which leads to Severity 1 incident, NPCI shall impose a penalty of INR 10,000/- (Indian Rupees Ten Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 20,000 for each hour with a max cap of 5% of total AMC value. b) Penalty for Severity 2: Any violation in meeting the above SLA requirements which leads to Severity 2 incident, NPCI shall impose a penalty of INR 5,000/- (Indian Rupees Five Thousand only) for each hour of delay up to 12 hours, beyond 12 hours penalty would be INR 10,000 for each hour with a max cap of 5% of total AMC value. c) Penalty for Severity 3: Any violation in meeting the above SLA requirements which leads to Severity 3 incident, NPCI shall impose a penalty of INR 2,000/- (Indian Rupees Two Thousand only) per hour with a max cap of 2% of total AMC value.	a penalty of INR 500/- (Five hundred only) for each hour of delay up to 24 hours, beyond 24 hours penalty would be INR 1000 for each hour with a max cap of 5% of total AMC value. b) Penalty for Severity 2: Any	No Change in RFP
6	RFP	28	8.15 Penalty on non- adherence to SLAs:	 e) Further if the number of downtime instances during a month exceeds 3 times, an additional 0.50% downtime will be reduced from uptime and the penalty will be calculated accordingly. f) If a breach occurs even after a proper policy in solution is in place, a penalty of Rs. 10,000/ per event will be deducted or the loss due to the breach whichever is higher. The right to levy the penalty is in addition to and without prejudice to other rights / remedies available to the NPCI such as termination of contract, invoking performance guarantee and recovery of amount paid etc. 	Request customer to remove the clause as bidder is already imposed with the SLA penalties	No Change in RFP

				The proposed solution should have the ability to be deployed in the following	kindly modify this clause as " The proposed solution should have the	No change in RFP
7	RFP	37	Section 9 - Technical Specifications	modes: - inline blocking - inline monitoring and, - SPAN mode. All necessary additional devices, licenses required for such configuration should be quoted as part of the solution.	ability to be deployed in the following modes: - MTA/BCC - integration with gateway security devices/Firewall, - SPAN mode. All necessary additional devices, licenses required for such configuration should be quoted as part of the solution."	
8	RFP	38	Section 9 - Technical Specifications	The proposed solution should support at least 100+ protocols for inspection	Protocol inspection is a IPS functionality, APT appliances are configured for static and dynamic analysis of files for malware detection.	Refer to corrigendum
9	RFP	38	Section 9 - Technical Specifications	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis	is it ok if we achieve this function through integration with our NGFW solution, please clarify	No change in RFP. APT solution should be able to achieve this independent of external devices or solution.
10	RFP	38	Section 9 - Technical Specifications	Must support full redundancy solution (Acti ve-Passi ve, Active-Active)	kindly modify this clause as " Must support full redundancy solution (Acti ve-Active,)"	No Change in RFP (Should support both mode of deployment).
11	RFP	38	Section 9 - Technical Specifications	The proposed APT solution must support Layer 2 Fallback option to bypass traffic even with the power on, in event of un-recoverable internal software error such as firmware corruption, memory errors	Why this function is required if we are providing the solution in High Availability (Active/Active). Please remove this clause so other OEM can also participate in the RFP.	Refer to corrigendum
12	RFP	38	Section 9 - Technical Specifications	APT must have a power failure Built-in / External bypass modular as option that can support hot swappable function which allows traffic to bypass even after a modular get unplugged out of APT Box during the RMA procedures	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	No change in RFP. APT solution should be able to achieve this independent of external devices or solution.
13	RFP	38	Section 9 - Technical Specifications	The APT filter must support network action set such as Block (drop packet), Block (TCP Reset), Permit, Trust, Notify, Trace(Packet Capture), Rate Limit and Quarantine	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	No change in RFP. APT solution should be able to achieve this independent of external devices or solution.

14	RFP	39	Section 9 - Technical Specifications	The proposed APT should support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW		Refer to corrigendum
15	RFP	39	Section 9 - Technical Specifications	The proposed APT must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc.,	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	A b ti e	to change in RFP. APT solution should be able to achieve his independent of external devices or olution.
16	RFP	39	Section 9 - Technical Specifications	Must have the ability to correlate the monitored attacks to the APT filters number and recommended action	please share more clarity for this clause.		Refer to corrigendum
17	RFP	40	Section 9 - Technical Specifications	The proposed management system support 3rd party VA scanners(Qualys, Foundstone, Nexus) to fine tune the APT policy	kindly let us know what is the use case for this clause. Request you to remove this clause from the RFP for maximum participation.		Refer to corrigendum
18	RFP	40	Section 9 - Technical Specifications	Sandboxing Appliance should support Active/Passive or Active-Active deployment and should support configuring cluster for High Availability	kindly modify this clause as "Sandboxing Appliance should support Active/Active deployment and should support configuring cluster for High Availability"	 A SI A P d	No change in RFP. The Network Anti- NPT solution should support Active- Active, Active- Passive Jeployment on- premises".
19	RFP	41	Section 9 - Technical Specifications	Solution should inspect https traffic (Full Deep Packet / SSL Traffic) and must provide decryption of unverified encrypted traffic for scanning and then re encrypt it before sending	sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle	N A b ti e	No change in RFP. APT solution should be able to achieve his independent of external devices or olution.
20	RFP	41	Section 9 - Technical Specifications	tegrate with any existing Proxy solution of NPC	which is the existing proxy solution at NPCI and is it support for ICAP integration	d	hould able to be deployed inline vith proxy solution.
21	RFP	41	Section 9 - Technical Specifications	SSL functionality should be available on the proposed inline APT appliance	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW		Refer to corrigendum

				The proposed solution for network Anti-APT	we can achieve this function through	No change in RFP.
				should have built-in SSL	sandbox integration and collaboration	
				Intercept capability (100% SSL traffic	with our NGFW firewall and hence	APT solution should
22	RFP	41	Section 9 - Technical	performance) to examine	please let us know if we can bundle	be able to achieve
1			Specifications	encrypted user bound traffic to detect threats	the solution alongwith the NGFW	this independent of
				(such as CnC traffic and		external devices or
				data exfiltration) that attackers may hide in		solution.
				encrypted streams		
				Fully support transparent (bump in wire) mode	5	No change in RFP.
					sandbox integration and collaboration	APT solution should
			Section 9 - Technical		with our NGFW firewall and hence	be able to achieve
23	RFP	41	Specifications		please let us know if we can bundle	this independent of
			specifications		the solution alongwith the NGFW	external devices or
						solution.
				The solution must support TLS fingerprint	we can achieve this function through	No change in RFP.
				detection detects malicious	sandbox integration and collaboration	
				communication by TLS fingerprinting with JA3	with our NGFW firewall and hence	APT solution should
24	RFP	41	Section 9 - Technical	between the client and	please let us know if we can bundle	be able to achieve
24	KEP	41	Specifications	server	the solution alongwith the NGFW	this independent of
						external devices or
						solution.
$\left \right $				Single box solution can both decrypt and re-	we can achieve this function through	No change in RFP.
				encrypt (full duplex) in all modes	sandbox integration and collaboration	APT solution should
					with our NGFW firewall and hence	be able to achieve
25	RFP	41	Section 9 - Technical		please let us know if we can bundle	this independent of
			Specifications		the solution alongwith the NGFW	external devices or
						solution.
$\left \right $				Ability to automatically intercept all SSL/TLS	we can achieve this function through	Refer to
				based flows, also on	sandbox integration and collaboration	corrigendum
		44	Section 9 - Technical	other ports and protocols (not only HTTPS)	with our NGFW firewall and hence	
26	RFP	41	Specifications		please let us know if we can bundle	
					the solution alongwith the NGFW	
\vdash				Ability to import server side certificates and	we can achieve this function through	No change in RFP.
				private keys for decryption	sandbox integration and collaboration	APT solution should
			Section O. Technical		with our NGFW firewall and hence	be able to achieve
27	RFP	41	Section 9 - Technical		please let us know if we can bundle	this independent of
			Specifications		the solution alongwith the NGFW	external devices or
					_	solution.
$\left - \right $				Ability to cache dynamically generated	we can achieve this function through	No change in RFP.
				certificates for reuse on subsequent	sandbox integration and collaboration	-
				connections	with our NGFW firewall and hence	APT solution should
			Section 9 - Technical		please let us know if we can bundle	be able to achieve
28	RFP	41	Specifications		the solution alongwith the NGFW	this independent of
						external devices or
						solution.

				port multiple active-inline devices simultaneou	this deployment introduce the	Refer to
					latency and impact on overall	corrigendum
29	RFP	41	Section 9 - Technical		application performance , hence	corrigendum
_ /			Specifications		request you to remove this clause	
					from the RFP.	
				Ability to configure encryption/decryption	we can achieve this function through	Refer to
				policy (incl. block/pass through) based on	sandbox integration and collaboration	corrigendum
			Section 9 - Technical	source/destination ip/por	with our NGFW firewall and hence	corrigendam
30	RFP	41	Specifications	source/descination ip/poi	please let us know if we can bundle	
i I			specifications		the solution alongwith the NGFW	
					the solution alongwith the Norw	
-				Ability to configure encryption/decryption	we can achieve this function through	Refer to
				policy (incl. block/pass through) based on	sandbox integration and collaboration	corrigendum
			Section 9 - Technical	host/URL categorization	with our NGFW firewall and hence	conigendum
31	RFP	41	Specifications	hose one categorization	please let us know if we can bundle	
			specifications		the solution alongwith the NGFW	
					the solution atongwith the right	
-+				Ability to configure encryption/decryption	we can achieve this function through	Refer to
				policy (incl. block/pass through) based on	sandbox integration and collaboration	corrigendum
			Section 9 - Technical	threat intelligence	with our NGFW firewall and hence	g
32	RFP	41	Specifications		please let us know if we can bundle	
			speemeations		the solution alongwith the NGFW	
				Ability to configure encryption/decryption	we can achieve this function through	Refer to
				policy (incl. block/pass through) based on CA	sandbox integration and collaboration	corrigendum
			Section 9 - Technical	stat	with our NGFW firewall and hence	J
33	RFP	41	Specifications		please let us know if we can bundle	
					the solution alongwith the NGFW	
					5	
				Ability to configure encryption/decryption	we can achieve this function through	Refer to
				policy (incl. block/pass through) based on	sandbox integration and collaboration	corrigendum
24	RFP	41	Section 9 - Technical	Subject / Domain Nam	with our NGFW firewall and hence	
34	KFP	41	Specifications		please let us know if we can bundle	
					the solution alongwith the NGFW	
T				Ability to configure encryption/decryption	we can achieve this function through	Refer to
				policy (incl. block/pass through) based on	sandbox integration and collaboration	corrigendum
35	RFP	41	Section 9 - Technical	Cipher Suite and Key Stre	with our NGFW firewall and hence	
22	IN F	''	Specifications		please let us know if we can bundle	
					the solution alongwith the NGFW	
				k/pass through) based on grouped or pre-	we can achieve this function through	No change in RFP.
				configured lists of above	sandbox integration and collaboration	APT solution should
					with our NGFW firewall and hence	be able to achieve
36	RFP	41	Section 9 - Technical		please let us know if we can bundle	this independent of
			Specifications		the solution alongwith the NGFW	external devices or
						solution.
		1			I	1

37	RFP	41	Section 9 - Technical Specifications	Support for Fail-to-wire/fail-to-open hardware, traffic bypass filters (in the event of in-line security device failure) and configurable link state monitoring/mirroring?	RFP already asked for HighAvailability (Active/Passive) deployment, also in- line deployment will introduce the latency and impact on overall performance. hence request you to remove this clause from the RFP.	Refer to corrigendum
38	RFP	41	Section 9 - Technical Specifications	Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, SSL3, and SSL2 encryption protocols?	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	Refer to corrigendum
39	RFP	42	Section 9 - Technical Specifications	Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	Refer to corrigendum
40	RFP	42	Section 9 - Technical Specifications	Support MDS, SHA-1, and SHA-256 hash algorithms?	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	Refer to corrigendum
41	RFP	42	Section 9 - Technical Specifications	Full Key length support (upto 4096 bit key lengths)	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	No change in RFP. APT solution should be able to achieve this independent of external devices or solution.
42	RFP	42	Section 9 - Technical Specifications	Ability to customize trusted CA list?	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	No change in RFP. APT solution should be able to achieve this independent of external devices or solution.
43	RFP	42	Section 9 - Technical Specifications	Ability to do CA revocation management	we can achieve this function through sandbox integration and collaboration with our NGFW firewall and hence please let us know if we can bundle the solution alongwith the NGFW	No change in RFP. APT solution should be able to achieve this independent of external devices or solution.

4	I RFP	62	Section 9 - Technical Specifications	The proposed solution should be able to run at least 50 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	Kindly modify this clause as "The proposed solution should be able to run at least 50 parallel VMs for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis"	No change in RFP, sandboxes refers to parallel VMs.
4	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	ТВ	For Network Anti-APT solution where the analysis has to done at wire speed on the traffic with aggressive packet capture, it is recommended that the Network Anti-APT appliance should have minimum 2 HDD with atleast 4TB of capacity to ensure the analysis to complete in near real- time. Hence in the benefit of NPCI which falls in National critical infrastructure should have minimum 2 x 4TB HDD and request amendment to the clause to: "Hardware should have minimum 2 HDD with atleast 4TB of capacity	Refer to corrigendum

				The proposed solution must be available as on	NPCI being an National Critical	Refer to
					Infrastructure of India where	corrigendum
				premise physical appliances with sandboxing		corrigendum
				capability	information is very sensitive it is	
					recommended to have complete	
					analysis to be performed by the	
					Network Anti-APT on premises. The	
					overall solution architecture should	
					be such that the complete sandboxing	
					must be performed on-premises & no	
					objects/files should be sent to the	
					vendor cloud as they may contain	
					either confidential data or Personally	
					identifiable information (PII) Data.	
					We would like to bring it to NPCI	
46					notice that as the clause does not	
					state complete sandboxing	
					environment on premises including	
					various operating systems &	
					applications like Windows OS & its	
					applications, Linux OS & its	
					applications & MAC OS & its	
					applications in absence of this being	
					stated NPCI would not be able to	
					control the file/objects submissions	
					to on-premises sandbox only. This	
					may lead to vendors submiting the	
	Section 9 -				files to the cloud without NPCI's	
	Technical		Annexure J - Technical		knowledge.	
	Specifications	59	Compliance			
			· · · · ·	The proposed solution should have multiple		Need more clarity
				Virtual Machine for dynamic/sandboxing		í í
47	Section 9 -			analysis of payload in redundancy to ensure if		
	Technical		Annexure J - Technical	one appliance fails other appliance should be		
	Specifications	59	Compliance	able to support at similar capacity.		
			·	Proposed APT solution should perform	Clarification required, Should we	Refer to
				advanced network detection and analysis of	read the clause as?	corrigendum
				the enterprise's internal/External network		5
				data.	"Proposed APT solution should	
48					perform advanced network	
	Section 9 -				detection and analysis of the	
	Technical		Annexure J - Technical		enterprise's inbound/outbound	
	Specifications	59	Compliance		network traffic."	
	specifications	57	compliance			

				The proposed solution should support to	As per clause number 1 of the	No change in RFP
				monitor traffic from multiple segments	Technical Specifications the Network	no change in ta t
				simultaneously on single appliance (East-West,	Anti-APT solution should be able to	
				North-South).	handle 500Mbps of total traffic. In	
					any organization where North-South	
					(Internet Traffic) is typically based on	
					total internet bandwidth and is same	
					or less than the total internet	
					bandwidth, but East-West traffic	
					(Intranet Traffic) i.e. from	
					LAN/Client segment to Server	
					segment the traffic may be huge	
					somewhere around 1Gbps to 4Gbps as	
					it is internal traffic, this would	
					exceed 500Mbps appliance capacity	
49					anytime. Also North-South and East-	
					West segments are completely	
					different and may pass through	
					different Core Switches and may not	
					be feasible at times for connectivity.	
					Hence we would request NPCI to	
					please share North-South traffic	
					detail in Mbps/Gbps and East-West	
					traffic in Mbps/Gbps to ensure all the	
					traffic is covered by Network Anti-	
					APT solutions and also confirm if	
	Section 9 -				connectivity for North-South traffic	
	Technical		Annexure J - Technical		and East-West traffic is feasible or	
	Specifications	59	Compliance		not.	
				The proposed solution should be dedicated	Similar to point 11 which is in more	Need more clarity
				appliance and should not be enabled as	details, hence we request NPCI to	· ·
50	Section 9 -			additional licensed solution with proposed	remove this point as duplicate.	
	Technical		Annexure J - Technical	perimeter gateway devices such as firewall,		
	Specifications	59	Compliance	APT etc.		

				Security Vendor must have a Research/Labs	Reporting on Vulnerabilities is	Need more clarity
				-		Need more clarity
				organization and this organization must	primary function of Vulnerability	
				contribute and report on finding new Zero-Day	Assessment tools / Solution.	
				vulnerabilities being exploited in the wild.		
					As a Network Anti-APT solution the	
					primary & most important function is	
					to prevent Zero-Day exploits in the	
					wild from targeting the	
					vulnerabilities. Also in real world, the	
					zero day explots may not available at	
					the same time when the actual	
					vulnerabilitiy is identified, hence it is	
					important to detect & prevent zero	
					day explicits / payloads.	
51					day exprises / payroads.	
					Hence to benefit from the Network	
					Anti-APT we request NPCI to modify	
					this clause as:	
					tins clause as.	
					"Security Vendor must have a	
					Research/Labs organization and this	
					organization must contribute and	
					report on finding new Zero-Day	
					explicts being identified /	
1						
1	Section 9 -				discovered in the wild & should	
	Technical		Annexure J - Technical		automatically share the intel to the	
1		50			Network Anti-APT Solution".	
	Specifications	59	Compliance			

—						
				The proposed solution should be able to	Need for clarification on this point	Need more clarity
				detect any suspicious communication within	specifically Outside of Customers	
				and outside of Customer's network	Network as it typically false in the	
					requirement of perimeter solutions	
					like Firewall / IPS.	
					With regards to within the network	
					suspicious communications would	
					NPCI like to detect malicious post-	
					exploitation activities such as	
					attacker lateral movements between	
					user workstation & servers? as	
					Attackers frequently use SMB & SMB2	
					to carry their activity from	
					compromised endpoints and move to	
52					servers, hiding their activities in	
					normal traffic.	
					If Yes, we would recommend NPCI to	
					modify the clause to:	
					"The proposed network Anti-APT	
					solution should also be able to	
					detect malicious post-exploitation	
					activities such as attacker lateral	
					movements between user	
					workstation & Servers. Attackers	
					frequently use SMB & SMB2 to	
	Section 9 -				carry their activity from	
	Technical		Annexure J - Technical		compromised endpoints and move	
	Specifications	59	Compliance		to servers, hiding their activities	
				The Proposed solution should be able to	We would like to highlight this	Need more clarity
				detect communications to known command	requirement only mentions detection	
				and control centers.	of known Command and Control	
					Centers (C&C) only and not blocking	
					of the C&C as well it do not covers	
					unknown C&C detection and blocking.	
					Hence in the benefit of NPCI we	
					request the clause to be changed to:	
53						
					"The Proposed solution should be	
					able to detect communications to	
					known & unknown command and	
					control center initiated by internal	
					infected clients."	
	Section 9 -					
	Technical		Annexure J - Technical			
	Specifications	59	Compliance			
	speenieucions	<i></i>	compliance			

1			The proposed colution should be able to	Drimovily this requirement falls in the		Need mare clarity
				· ·		Need more clarity
			detect reputation of URL being accessed			
				reputation but it should be able to		
				analyze complete URL's in zero-trust		
				manner as attackers take advantage		
				of the URL reputation check tools to		
				launch sophisticated attacks and		
				compromise the Host/End-user.		
Section 9 -				Hence we recommend to remove or		
Technical		Annexure J - Technical		modify the clause.		
Specifications	59	Compliance				
			The proposed solution should support at least	In an Advanced Attack threat actors		Need more clarity
			100+ protocols for inspection	leverage C&C communication to		-
				command & control the victim		
				machine, hence it is important for an		
				-		
				, e		
				"The proposed solution for Network		
Section 9 -						
		Annexure J - Technical				
Specifications	59	Compliance				
	Technical Specifications Section 9 - Technical	Technical Specifications 59 Section 9 - Technical	Section 9 - Technical Annexure J - Technical Specifications 59 Compliance	Technical Specifications Annexure J - Technical Compliance The proposed solution should support at least 100+ protocols for inspection Section 9 - Technical Annexure J - Technical Image: Compliance	Section 9 - Technical Annexure J - Technical The proposed solution should support at least 100+ protocols for inspection In an Advanced Attack threat actors leverage C&C communications regardless of ports and protocols, and organization to block all malicious C&C communications regardless of ports and protocols, and protocols"	Section 9 - Technical Annexure J - Technical The proposed solution should support at least 100+ protocols for inspection In advanced Attack threat actors leverage C&C communications reguireless of ports and protocols, hence we request NPCI to change the clause to: Section 9 - Technical Annexure J - Technical The proposed solution should support at least 100+ protocols for inspection In an Advanced Attack threat actors leverage C&C communications to command a protocols, hence we request NPCI to change the clause to: Section 9 - Technical Annexure J - Technical The proposed solution should support at least 100+ protocols for inspection In an Advanced Attack threat actors leverage C&C communication to command £ control the victim machine, hence it is important for an organization to block all malicious C&C communications regardless of ports and protocols, hence we request NPCI to change the clause to: Section 9 - Technical Annexure J - Technical Annexure J - Technical

				Sandbox must have the ability to simulate the	There are various flavors of Sandbox	Refer to
				entire threat behavior.	environment used for analysis and	corrigendum
					not limited to just Windows OS but	conigendum
					also Linux, MAC OS with 32bit and	
					64bit architecture and various types	
					of applications targeted in the wild.	
					b) applications targeted in the wild.	
					Hence in the benefit of NPCI we	
					request the clause to be very specific	
					like:	
					"The proposed solution must be	
56					available as on premise physical	
					appliances with sandboxing	
					capability and must be able to	
					detect and report malware by	
					using multiple client environments	
					(operating systems with multiple	
					service pack levels) supporting	
					both x64 and x86 architectures	
					including Windows, Mac, CentOS	
	Section 9 -				based on premise Virtual Execution	
	Technical		Annexure J - Technical		Environment"	
	Specifications	59	Compliance			
				The proposed solution should have an built-in	OEM Specific Clause.	Refer to
				document vulnerabilities detection engine to		corrigendum
				assure analysis precision and analysis	We request removal of the clause as	
57				efficiency	the requirement gets addressed in	
	Section 9 -				detection of Zero-Day exploits	
	Technical		Annexure J - Technical		targeting vulnerabilities in the wild in	
	Specifications	59	Compliance		clause 19 and 20.	

		1		The proposed solution should support Multiple	Advanced attackers once establish	Refer to
				protocols for inspection. Example:- HTTP,	the foothold tries to move laterally	corrigendum
					and dump sophisticated tools on	
				protocols Internal direction: SMB ,Database	various systems connected in the	
					network detecting this tools and	
				device	identifying this tools and techniques	
					plays a very important and critical	
					role in early detection and incident	
					response.	
					Hence in the benefit of NPCI it is	
					important to get visibility of such activities of the threat for which we	
					request modification of the clause to below:	
58					below:	
					"The proposed solution should be	
					able to detect the activities of	
					attackers already resident in the	
					network core. The solution should	
					extracts malware and objects that	
					are transferred over HTTP, FTP &	
					other protocols and submit them to	
					the automated dynamic Analysis	
					engine for detonation and	
					confirmation on maliciousness. The	
					solution should extracts malware	
	Section 9 -				and objects that are transferred	
	Technical		Annexure J - Technical		over HTTP, FTP like protocols and	
	Specifications	59	Compliance		submit them to an automated	
			· ·	The Proposed solution should have a Co-	Duplicate point as all the previous	Refer to
59	Section 9 -			relation engine to automatically co-relate	clause covers the same.	corrigendum
39	Technical		Annexure J - Technical	across multiple protocol, multiple sessions and	Request removal of the clause.	
	Specifications	59	Compliance	volume traffic analysis		

				The proposed solution should be able to	Advanced attackers leverage various	Refer to
				detect and prevent the persistent threats	types of files to infiltrate in the	corrigendum
				which come through executable files, PDF	target environment and not just	5
				files, Flash files, RTF files and and/or other	executables, pdf, flash or RTF file	
				objects.	types hence it is very important that	
					dynamic analysis engine should be	
					able to analyze different filetypes	
					without depending on the signatures.	
					······································	
					Hence for critical infrastructure like	
					NPCI should ensure that various	
					filetypes which are leveraged by the	
					advanced attackers should be	
					dynamically analyzed without	
					depending upon the signatures alone,	
60					in the benefit of NPCI we request	
					modification of this clause as follows:	
					"The proposed solution should have	
					the ability to analyze, detect and	
					block malware in common file	
					formats including but not limited	
					to executables, JAVA, PDF, MS	
					Office documents, common	
					multimedia contents such as JPEG,	
					QuickTime, MP3 and	
					ZIP/RAR/7ZIP/TNEF archives, 3gp,	
	Section 9 -				asf, chm, com, dll, doc, docx, exe,	
	Technical		Annexure J - Technical		gif, hip, htm, ico, jar, jpeg, jpg,	
	Specifications	59	Compliance		mov, mps, mp4, pdf, png, ppsx,	

				The Proposed solution should be able to	In a sophisticated attack the	Refer to
				generate out of box reports to highlight	advanced attackers may or may not	corrigendum
				Infections, C&C behavior, Lateral Moment,	use malware, but they definitely use	configendam
				Asset and data discovery and Exfiltration	various techniques & methodologies	
				Asset and data discovery and Exiteration	to move laterally, hence it is	
					important for a solution to detect	
					TTP's and methodologies and alert	
					with timeline & date sliders with at	
					least 5 minutes of relevant network	
					activity data(layer 4-7) before and	
					after the attack.	
					Hence in the benefit of NPCI we	
					request modification of this clause	
					with must have capabilities as:	
61					then muse have capabilities as	
					Proposed Internal Network APT	
					should detects the following types of	
					malicious post-infection activities:	
					a) Internal Reconnaissance	
					b) Privilege Escalation	
					c) Credentials Dumping	
					d) Lateral Movement of Malware	
					e) Remote Task Execution	
					f) Data Exfiltration Detection	
					g) Callback activities	
					h) Bot-tracker features like File	
	Section 9 -				inspection, Packet flows, Signature	
	Technical		Annexure J - Technical		matching and statistics	
	Specifications	59	Compliance		i) Supports extensive metadata	
				The proposed APT must able to operate in	Analyzing asymmetric traffic results	Refer to
				Asymmetric traffic environment with	in ton's of false positive's and adds	corrigendum
				Vulnerability / Exploit filters for protection	unnecessary workload on validation	
					of such all the alerts resulting in Alert	
62					Fatigue on SOC team, hence we	
					request removal of such clause which	
	Section 9 -				adds overheads to security team and	
	Technical		Annexure J - Technical		miss on legitimate threats.	
	Specifications	59	Compliance			
	Section 9 -			The proposed APT solution must support	OEM Specific IPS Solution, Request	Refer to
63	Technical		Annexure J - Technical	Adaptive Filter Configuration(AFC) which will	removal of this clause.	corrigendum
		59		alert or disable ineffective filter in case of		
\vdash	Specifications	57	Compliance	noisy filters The APT filter must support network action	Duplicate Clause, Point 17 covers the	Refer to
				set such as Block (drop packet), Block (TCP	requirement hence we request	corrigendum
				Reset), Permit, Trust, Notify, Trace(Packet	removal of this clause.	
				Capture), Rate Limit and Quarantine	removal of this clause.	
64				Capture,, Nate Linnt and Quarantine	Also it is important for Anti-APT	
					solution to Block callback to C&C and	
	Section 9 -				malicious communications in inline	
	Technical		Annexure J - Technical		maticious communications in intine mode.	
	Specifications	59	Compliance		mode.	
1 1	speenications	57	comptiance			

				The proposed APT solution must support	Clause is OEM Specific IPS Solution	Refer to
				signatures, vulnerabilities and traffic filtering	which heavily depends upon signature	corrigendum
65	Section 9 -			methods to detect attacks and malicious	based detection.	compendant
"	Technical		Annexure J - Technical	traffic		
	Specifications	59	Compliance	lanc	We request removal of this clause	
			•	The APT filters must be categories into the	Clause is OEM Specific IPS Solution,	Refer to
				following categories for easy management:	Request removal of this clause.	corrigendum
				Exploits, Identity Theft/Phishing,		5
66	Section 9 -			Reconnaissance, Security Policy, Spyware,		
	Technical		Annexure J - Technical	virus, Vulnerabilities, Traffic		
	Specifications	59	Compliance	Normalization, P2P, IM, Streaming Media		
				Vulnerability based filter are known for most	Clause is OEM Specific IPS Solution &	Refer to
	Section 9 -			effectively for Zero Day Attack Protection and	only covers known attacks, Request	corrigendum
67	Technical		Annexure J - Technical	proposed solution must support vulnerability	removal of this clause.	•
	Specifications	59	Compliance	based filter		
	Section 9 -			The proposed APT should support the ability	Clause is OEM Specific IPS Solution,	Refer to
68	Technical		Annexure J - Technical	to mitigate Denial of Service (DoS/DDoS)	Request removal of this clause.	corrigendum
	Specifications	59	Compliance	attacks such as SYN floods		•
	Section 9 -			The proposed APT must provide bandwidth	Clause is OEM Specific IPS Solution,	Refer to
69	Technical		Annexure J - Technical	rate limit to control the unwanted/nuisance	Request removal of this clause.	corrigendum
	Specifications	59	Compliance	traffic such as P2P, Online Game, etc.,		
				The proposed APT must be able to use	Clause is OEM Specific IPS Solution &	Refer to
				Reputation Service such as IP address or DNS	only covers known attacks, Request	corrigendum
70	Section 9 -			to block traffic from or to 'known bad host'	removal of this clause.	
	Technical		Annexure J - Technical	such as spyware, phishing or Botnet C&C		
	Specifications	59	Compliance			
				The proposed APT must be able to control the	Clause is OEM Specific IPS Solution &	Refer to
				known bad host such as spyware, botnet C2	only covers known attacks, Request	corrigendum
71	Section 9 -			server, spam and so on based on country of	removal of this clause.	
	Technical		Annexure J - Technical	origin, exploit type and the reputation score		
	Specifications	59	Compliance			
				Must have the ability to correlate the	The clause adds lot of dependency on	Refer to
				monitored attacks to the APT filters number	the security teams to continuously	corrigendum
				and recommended action	monitor and keep on modifying	
					policies increasing overheads and	
					false positives, Anti-APT solution	
					should be able to take decision with	
72					its intelligence with simple	
					configuration to Block or Monitor the	
					threat.	
	Section 9 -				Hence in the benefit of the NPCI we	
	Technical		Annexure J - Technical		request modification/removal of this	
	Specifications	59	Compliance		clause	
	specifications	57	comptiance		lciause	

r						
				NG APT engine must be a smart enough to	Detecting traffic based on suspicion	Refer to
				inspect the traffic based on condition, If the	or deep packet inspection needs	corrigendum
				traffic is suspicious then it goes for the deep	patterns / signatures to take	
				packet inspection	decisions, Anti-APT solution should	
73					not just depend upon signatures but	
/3					it should have dynamic analysis	
					engine with signatureless detection	
	Section 9 -				and should create signatures in	
	Technical		Annexure J - Technical		Realtime and block the threats inline.	
	Specifications	59	Compliance			
			•	The proposed management system shall allow	Please correct our understanding	To be Integrated
				the update of global threat intelligence via	about local threat intelligence	with our TIP
				cloud and local Threat intelligence updates	sharing. Do you mean sharing	platform for threat
74				from proposed Network threat detection	intelligence from your existing Anti-	intelligence
1'	Section 9 -			solution automatically for inline blocking	APT solutions from Email & content	integration with
	Technical		Annexure J - Technical			other solutions
	Specifications	59	Compliance		scanning Anti-APT solutions to Anti-	
	specifications	72	compliance		APT for Network Security?	deployed.
				The management server must provide rich	Rate Limiting, Misuse & Abuse,	Refer to
				reporting capabilities include report for All	Traffic Threshold & DDoS reports do	corrigendum
				attacks, Specific & Top N attack, Source,	not fall in Anti-APT solution, these	
75				Destination, Misuse and Abuse report, Rate	are OEM specific and hence request	
	Section 9 -			limiting report, Traffic Threshold report,	NPCI to remove the same.	
	Technical		Annexure J - Technical	Device Traffic Statistics and Advance DDoS		
	Specifications	59	Compliance	report		
				The proposed management system must be	Critical infrastructure like NPCI may	Refer to
				able to support the syslog CEF format that	have various tools for event	corrigendum
				SIEM can support	correlation, automation,	
					orchestrations etc limiting to CEF	
					format only may limit integration	
					with other tools and result no	
					integration support. Hence we	
					request NPCI to modify the clause to	
					various types of log/event format but	
					not limited to CEF only.	
					not united to cer only.	
76					Clause Modification to:	
					clube mouncation to.	
					The proposed management system	
					must be able to support Common	
					Event Format (CEF), Log Event	
					Enhanced Format (LEEF), Comma-	
					Separated Values (CSV), XML,	
	Castian O				JSON, or Text format that SIEM	
	Section 9 -				and other tools like automation	
	Technical		Annexure J - Technical		and orchestration can support.	
	Specifications	59	Compliance	1	1	

77				The proposed management system shall have a big data engine that allows customers to provide faster security analytics and faster report generation	To integrate with Big Data Analytics the solution should support file formats that can be ingested in the Big Data Analytics tool, hence we request NPCI to modify the clause and not mandate with Big Data Engine which makes the clause to OEM Specific. Request modification in clause to: "The Management system should	Refer to corrigendum
	Section 9 - Technical	59	Annexure J - Technical Compliance		support file formats which can be ingested in Big Data Analytics Solution for faster report	
78	Specifications Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	Automatic detection and response against an ever-growing variety of threats, including fileless and ransomware	generation." This clause of Automatic detection and response requirement do not covers automatic prevention and integration with various other vectors of attack like Email, Endpoint EDR and File/content uploads from outside to respond to threats. In any enterprise organizations and critical infrastructure resilience defense strategy plays a very important role to defend against the advanced attack and hence should be in a Must Have category instead of Good to Have. Does NPCI wants to take benefit of Anti-APT for network security solution requirement with automatic prevention and integration with various vectors of attack capabilities and not just detection and response? If yes we request modification of the clause to: "The solution must have automatic detection, prevention, remediation and integration capabilities with various attack vectors not limited	Refer to corrigendum
79	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The industry's most timely virtual patching: Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployable.	Clause is OEM Specific IPS Solution, Request removal of this clause.	Refer to corrigendum

				The solution should consolidate (at	To support Advanced Defense		Okay, No change in
				centralized location) the administration,	Strategy and build advanced		RFP.
80	Castian O			reporting, and intelligence data sharing	resilience infrastructure for NPCI it's		
	Section 9 -		A	intelligence/IOC's between deployed Anti-APT	important clause.		
	Technical	50		Sensors/ solution at our organization (Email			
	Specifications	59	Compliance	Analysis, File Analysis & EDR)			
				Central Management should provide option to	To support Advanced Defense		No change in RFP
				create customized lists of IOCs received from	Strategy and build advanced		
				these feeds and use them as a custom	resilience infrastructure for NPCI it's		
				blacklist on the Central Management	important clause.		
81				appliance. The types of IOCs like URL			
				indicators, IP address indicators, domain			
				indicators, and indicators with hashes of			
	Section 9 -			malicious files, combine them into a standard			
	Technical			format called STIX (Structured Threat			
	Specifications	59	Compliance	Information Expression)			
				Centralized Sandboxing	OEM specific clause, some of the		No change in RFP.
					OEM's provide Built-in Sandboxing		Prefer to have built
82					solution and do not require any		in sandboxing
	Section 9 -				additional/external Sandboxing		capabilities for
	Technical		Annexure J - Technical		solution. Hence we request NPCI to		Network Anti-APT
	Specifications	59	Compliance		consider the same.	12	solutions.
				The proposed solution should be able to run at			Refer to
				least 50 parallel sandboxes for analysis of	methods and technology to run		corrigendum
				payload and on premise customized sandbox	dynamic analysis and should not		
				solution should have the capability to allow	mandate on 50 parallel sandboxes		
				manual submission of suspicious files for	instead it is important to have		
				analysis	multiple executions to run in parallel		
					for payload analysis automatically		
					and not manually.		
					Some of the OEM who have		
					NO\limited number of Sandboxes built		
83					in depend upon external sandboxes		
					which supports manual submission of		
					files, hence we request for		
					modification of the clause to:		
					"The colution should support 1000		
					"The solution should support 1000+		
					executions to analyze the payloads in		
					parallel depending on the		
	Section 9 -				performance capacity upto 500Mbps		
	Technical		Annexure J - Technical		of the appliance deployed on-		
	Specifications	59			premises"		
	specifications	J7	compliance				

				Sandboxing Appliance should support	Not applicable for built-in sandboxing	No change in RFP.
				Active/Passive or Active-Active deployment	solution hence we request	
				and should support configuring cluster for	modification of the clause to:	"The Network Anti-
				High Availability		APT solution should
84					"The Network Anti-APT solution	support Active-
					should support Active/Passive or	Active, Active-
	Section 9 -				Active passive deployment on-	Passive
	Technical		Annexure J - Technical		premises"	deployment on-
	Specifications	59	Compliance		ľ	premises".
				The proposed solution must be capable of	Advanced attackers leverage various	Refer to
				analysis of different file types, including	types of files to infiltrate in the	corrigendum
				portable executables (PEs), web content, Web	target environment especially	•
				objects, images, Java, network flows,	Webshell attacks on Web Servers and	
					manipulate the server and redirect to	
					malicious content.	
				multimedia etc. including all such file types		
				· · ·	Hence for critical infrastructure like	
					NPCI should ensure that various	
				channel, for initial compromise or backdoor or	filetypes which are leveraged by the	
					advanced attackers should be	
					dynamically analyzed without	
					depending upon the signatures alone,	
					in the benefit of NPCI we request	
85					modification of this clause as follows:	
					"Solution should provide	
					comprehensive support for user	
					interaction framework for web	
					shells, support for shell scripts	
					(e.g.; python, Perl, and Ruby etc.),	
					support for ELF binaries, Server-	
					side attack detection, complete user mode and kernel mode	
					monitoring from within and outside	
					the Guest Images, Web shell	
	Section 9 -				detection support for JSP, PHP,	
	Technical		Annexure J - Technical		and WAR (Web archive) file types etc."	
	Specifications	59	Compliance		ει	
	specificacions	57	comptiance			

				Sandbox appliance should have redundant	For Network Anti-APT solution where	Refer to
				power supply, 2 TB or more storage capacity	the analysis has to done at wire speed	corrigendum
				with dedicated management port	on the traffic with aggressive packet	corrigendum
				with dedicated management port	capture, it is recommended that the	
					Network Anti-APT appliance should	
					have minimum 2 HDD with atleast	
					4TB of capacity to ensure the	
					analysis to complete in near real-	
86					time.	
					Hence in the benefit of NPCI which	
					falls in National critical infrastructure	
					should have minimum 2 x 4TB HDD	
	Contine 0				and request amendment to the clause	
	Section 9 - Technical		Annexure J - Technical		to:	
		50			"Hardware should have minimum 2	
	Specifications Section 9 -	59	Compliance		HDD with atleast 4TB of capacity	
0.7	Technical		Annexure J - Technical	The Proposed Solution should be able to	Does NPCI only wants to detect	Refer to
87		59		detect known bad URL before sandboxing	known bad URL's only?	corrigendum
	Specifications	59	Compliance			
				The proposed solution should detect file-less	Attackers use encoded algorithms like	Refer to
				malware tools used for extracting plain text	XOR to hide password instead of plain	corrigendum
				passwords, hash, PIN codes and Kerberos	text, do NPCI would like to detect	
				tickets.	and extract passwords which are	
					encoded algorithm XOR instead of	
					just plain text? If yes,	
88					We request you to modify the clause	
					to:	
					"The proposed solution should	
					detect file-less malwares tools	
	Section 9 -				used for extracting	
	Technical		Annexure J - Technical		encoded/XOR'ed as well as plain	
	Specifications	59	Compliance		text passwords, hash, PIN codes	
<u> </u>	specifications	57	compliance		etc"	Defente
1				The Proposed solution should allow Admin be	Please provide clarification on the	Refer to
	Section 0					
89	Section 9 -		Appovuro I. Tochnical	able to inquire how many detections come	requirement.	corrigendum
89	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	able to inquire how many detections come from malicious password-protected files	requirement.	corrigendum

		T		The Proposed Sandboxing solution must	In Advanced Threat Landscape the	Refer to
				support of analysis of Windows & Linux	attacks are not limited to Windows &	corrigendum
				Operating System files	Linux environment only but MAC OS's	congendum
				operating system mes	and its applications are also targeted	
					with Zero-day attacks, attackers also	
					leverage Webshell attacks on Linux	
					servers, hence it is important that	
					sandboxing solution should have	
					Windows, Linux and MAC OS's for	
					conducting dynamic analysis on-	
					premises and create real-time threat	
					intelligence to block call	
					back/malicious communications with	
					C&C servers.	
90					We would like to know if NPCI wants	
					to detect and prevent attacks	
					targeted towards MAC and Linux	
					including Webshell injection attacks?	
					If yes, we request modification of the	
					clause to:	
					"The proposed Anti-APT solution	
					should include on-premises	
					sandboxing for dynamic analysis	
					for Windows, Linux and MAC OS's	
	Section 9 -				without any additional	
	Technical		Annexure J - Technical		requirement of licenses form OS's	
	Specifications	59	Compliance		and Applications from NPCI."	
				SSL Capabilities	Does NPCI wants dedicated SSL	Refer to
					solution for Network Anti-APT or are	corrigendum
					looking for built-in SSL decryption	
					capabilities in Network Anti-APT? as	
91					the requirement point/clause	
	Section 9 -				mentioned below are typically	
	Technical		Annexure J - Technical		available in dedicated SSL decryption	
	Specifications	59	Compliance		solution.	

				Colution should inspect bitter traffic (Full Deep	Advanced attackers uses Webshell	Refer to
				Solution should inspect https traffic (Full Deep		
				Packet / SSL Traffic) and must provide	inject attacks to compromise Web	corrigendum
				decryption of unverified encrypted traffic for	-	
				scanning and then re encrypt it before sending		
					capabilities? If yes please confirm and	
					amend/modify the same to the	
					requirement mentioned.	
					For Example the clause can be	
					modified as:	
92					"The proposed solution should	
					detect & prevent suspicious	
					Webshell files uploaded to web	
					servers through HTTP POST and	
					FTP protocols and also provide	
					mapping of methodology & alert	
					techniques to MITRE ATT&CK	
					framework. It should also detect	
	Section 9 -				attempted data exfiltration &	
	Technical		Annexure J - Technical		SSL/TLS handshake fingerprinting	
	Specifications	59	Compliance		at the minimum"	
				Integrate with any existing Proxy solution of	Please provide clarification on proxy	Should able to be
93	Section 9 -			NPCI.	and expectation on Integration with	deployed inline
93	Technical		Annexure J - Technical		Proxy.	with proxy solution.
	Specifications	59	Compliance			
				SSL functionality should be available on the	Duplicate to Point 93 which clearly	Refer to
				proposed inline APT appliance	states that the Anti-APT should have	corrigendum
					built-in SSL intercept capability	
					which itself makes SSL inline to	
94					Network Anti-APT, unless NPCI is	
					looking for dedicated SSL solution if	
	Section 9 -				yes, we would than propose	
	Technical		Annexure J - Technical		dedicated SSL decryption appliance	
	Specifications	59	Compliance		inline to Anti-APT.	
				The solution must support TLS fingerprint	Very important point where Anti-APT	No change in RFP
				detection detects malicious communication by		
				TLS fingerprinting with JA3 between the	malicious communication by TLS	
95				client and server.	Fingerprinting with JA3 inbetween	
					Client and Server. If it is good to have	
	Section 9 -				in that case NPCI may miss this	
	Technical		Annexure J - Technical		capability provided by some of the	
	Specifications	59	Compliance		Anti-APT solutions.	
				Ability to automatically intercept all SSL/TLS	Please Clarify on the clause, as TCP	Refer to
96	Section 9 -			based flows, also on other ports and protocols	ports have to be defined manually to	corrigendum
"	Technical		Annexure J - Technical	(not only HTTPS)	automatically intercept SSL/TLS or	
	Specifications	59	Compliance		HTTPS.	
	Section 9 -			Support multiple active-inline devices	Please provide more clarification	Refer to
97	Technical Specifications	59	Annexure J - Technical Compliance	simultaneously		corrigendum

				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				source/destination ip/port	interception solution, We request	
98	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	59	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				host/URL categorization	interception solution, We request	
99	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	59	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				threat intelligence	interception solution, We request	
100	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	59	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on CA	supported with dedicated SSL	corrigendum
				status	interception solution, We request	_
101					NPCI to confirm if they need	
	Section 9 -				dedicated SSL interception solution	
	Technical		Annexure J - Technical		to provide granular controls? Also	
	Specifications	59	Compliance		provide use case for the same	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
102				Subject / Domain Name	interception solution, We request	
102	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	59	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
103				Cipher Suite and Key Strength	interception solution, We request	
103	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	59	Compliance		to provide granular controls?	
				Support for Fail-to-wire/fail-to-open	Requirement depends on the port	Refer to
				hardware, traffic bypass filters (in the event	capability or external Active Failover	corrigendum
104	Section 9 -			of in-line security device failure) and	Kit is required, Please confirm of	
	Technical		Annexure J - Technical	configurable link state monitoring/mirroring?	NPCI needs external Bypass Kit to	
	Specifications	59	Compliance		support the same?	

				Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3,	SSL stands for Secure Socket Layer	Refer to
				SSL3, and SSL2 encryption protocols?	while TLS stands for Transport Layer	corrigendum
					Security. Both Secure Socket Layer	5
					and Transport Layer Security are the	
					protocols used to provide the security	
					between web browser and web	
					server.	
					The main differences between Secure	
					Socket Layer and Transport Layer	
					Security is that. In SSL (Secure Socket	
					Layer), Message digest is used to	
					create master secret and It provides	
					the basic security services which are	
105					Authentication and confidentiality.	
105					while In TLS (Transport Layer	
					Security), Pseudo-random function is	
					used to create master secret.	
					1) SSL (Secure Socket Layer) is the	
					3.0 version is equal to TLS	
					(Transport Layer Security) is the 1.0	
					version.	
					2) In SSL(Secure Socket Layer),	
					Message Authentication Code	
					protocol is used while in	
					TLS(Transport Layer Security),	
	Section 9 -				Hashed Message Authentication	
	Technical		Annexure J - Technical		Code protocol is used.	
	Specifications	59	Compliance		3) SSL (Secure Socket Layer) is less	

106 Section 9 - Technical Specifications 59 Annexure J - Technical Compliance Support RS, DHE, and ECDHE public key aligorithms? Duplicate as point 111 Covers the Cophers in details which are more precise than point 112 which is very generic. No change in RFP 108 Section 9 - Technical Specifications 59 Annexure J - Technical Compliance Support RS, DHE, and ECDHE public key aligorithms? Duplicate as point 111 Covers the Cophers in details which are more precise than point 112 which is very generic. No change in RFP					Columbian advanted assessment in basis of G and C	1	
106 Section 9 - Technical specifications Annexure J - Technical compliance Annexure J - Technical compliance Support RSA, DEE, DES, RC4, and Camellia support RSA, RES26, Section 44, 255 Duel Kasa, RES28, Section 44, 256 107 Section 9 - Technical specifications Annexure J - Technical Compliance Annexure J - Technical Compliance Support RSA, DES, DES, RC4, and Camellia Support RSA, RES26, SHA, 344, 255, SHA, 345 108 Section 9 - Technical specifications Annexure J - Technical Compliance Support RSA, DES, DES, DES, RC4, and Camellia Support RSA, RES26, SHA, 344, 255, SHA, 345 108 Section 9 - Technical specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duel Kasa, RES26, SHA AES226, SHA, 256 108 Section 9 - Technical specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duel Kasa, RES26, SHA AES226, SHA AES							No change in RFP
106 Section 9 - Technical Specifications 59 Annexure J - Technical Compliance Support AES, 30ES, DES, RC4, and Camellia are weak ciphers and dramelia result with are more precise than point 111 covers the compliance Support AES, 30ES, DES, RC4, and Camellia are weak ciphers and dramelia result with are more precise than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Annexure J - Technical Compliance Support AES, 30ES, DES, RC4, and Camellia are weak ciphers and hence in to generic. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Annexure J - Technical Compliance Support AES, 30ES, DES, RC4, and Camellia are weak ciphers and hence in to generic. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Support AES, 30ES, DES, RC4, and Camellia are weak ciphers and hence in to generic. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Support AES, 30ES, DES, RC4, and Camellia are weak ciphers and hence in to generic. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Support AES, 30ES, DES, RC4, and Camellia are weak ciphers and hence in to generic. Refer to corrigendum	1 1				•		
106 ECOHE ECOSA. A5226-GCM-SHA284 DHE-RSA. A5218 GCM-SHA284 DHE-RSA. A5218 GCM-SHA284 ECOHE ECOSA. A5276-SHA255 ECOHE ECOSA. A5276-SHA256 ECOHE ECOSA. A5276-SHA256 ECOHE ECOSA. A5276-SHA266 ECOHE ECOSA. A5276-SHA256 ECOHE ECOSA. A5276-SHA266 DIFE.RSA. A5276-SHA256 ECOHE ECOSA. A5276-SHA266 ECOHE ECOSA. A5276-SHA266 ECOHE ECOSA. A5276-SHA266 ECOHE ECOSA. A5276-SHA266 ECOHE ECOSA. A5276-SHA ECOHE ECOSA. A5276-SHA ECOHE ECOSA. A5276-SHA AE5128-SHA ECOHE ECOSA. A5276-SHA AE5128-SHA AE5128-SHA AE5128-SHA ECOHE ECOSA. A5276-SHA AE5128-SHA AE5128-SHA AE5128-SHA ECOHE ECOSA. A5276-SHA AE5128-SHA ECOHE ECOSA. A5276-SHA AE5128-SHA AE5128-SHA AE5128-SHA ECOHE ECOSA. A5276-SHA AE5128-SHA ECOHE ECOSA. A5276-SHA AIDE ECOSA. AE528-SHA ECOHE EC							
106 DHE-RSA-ASS128-CCM-SHA236 DHE-RSA-ASS128-SHA256 ECDHE-RSA-ASS128-SHA256 ECDHE-RSA-ASS128-SHA256 ECDHE-RSA-ASS128-SHA256 ECDHE-RSA-ASS128-SHA256 DHE-RSA-ASS128-SHA256 DHE-RSA-ASS128-SHA256 DHE-RSA-ASS128-SHA256 DHE-RSA-ASS128-SHA256 DHE-RSA-ASS128-SHA DHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA DHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA DHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA ECDHE-RSA-ASS128-SHA AES	1 1						
106 Section 9 - Technical Specifications Annexure J - Technical Specifications Support RSA, AES26 SHA256 107 Section 9 - Technical Specifications Support RSA, DEE, SA Dublic RSA, AES26 SHA256 108 Specifications 59 Compliance Duplicate as point 111 covers the Clipher Stape R256 SHA256 108 Specifications 59 Compliance Support RSA, DES, RC4, and Camellia are weak cliphers and hence in the benefit of MPC1 we request net to use hence merease in nounce multis which is were hence i					ECDHE-ECDSA-AES256-GCM-SHA384		
106 Section 9 - Technical Specifications Support RSA, DET, SA, AES236-SHA 2556-SHA 256					DHE-RSA-AES128-GCM-SHA256		
106 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia Specifications Support AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms? Duplicate as point 111 covers the Cupiers in details which are more precise than a corrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms? Duplicate as point 111 covers the Cupier to seal or orrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms? Duplicate as point 111 covers the Cupier to seal or orrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms? Support AES, 3DES, DES, RC4 and Camellia are weak ciphers and dense in the benefit of NPC1 we request not to use the seal in your environment. Refer to corrigendum					DHE-RSA-AES256-GCM-SHA384		
106 Section 9 - Technical Specifications Section 9 - Technical Specifications Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 overs the Compliance Support RSA, DHE, and SHA-256 have algorithms? 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support RSA, DHE, and SED, ES, RC4, and Camellia Symmetric key algorithms? Duplicate as point 111 overs the corrigendum Refer to corrigendum	1 1				ECDHE-RSA-AES128-SHA256		
106ECDHE-ECDS-AA5256-SHA384 DHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA256 ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA ECDHE-RSA-AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES256-SHA DHE-RSA-AES26-SHA AES256-SHA DHE-RSA-AES26-SHA DHE-RSA-AES26-SHA DHE-RSA-AES26-SHA DHE-RSA-AES26-SHA AES256-SHA DHE-RSA-AES26-SHA AES256-SHA DHE-RSA-AES26-SHA AES256-SHA DHE-RSA-AES26-SHA DHE-RSA-AES26-SHA AES256-SHA DHE-RSA-AES26-SHA AES256-SHA DHE-RSA-AES26-SHA AES256-SHA DHE-RSA-AES26-SHA AES256-SHA DHE-RSA-AES26-SHA AES256-SHA AES256-SHA DHE-RSA-AES26-SHA AES256-SHA AES256-SHA DHE-RSA-AES26-SHA AES2					ECDHE-ECDSA-AES128-SHA256		
106 Job Her, BSA, AES126-SHA256 106 DHE, BSA, AES126-SHA256 ECDHE, ESA, AES126-SHA256 ECDHE, ESA, AES126-SHA DHE, BSA, AES126-SHA ECDHE, ESA, AES126-SHA ECDHE, ESA, AES126-SHA DHE, BSA, AES126-SHA Annexure J - Technical Specifications 59 Compliance Support MSA, DHE, and ECDHE public key algorithms? Difference Support MSA, DHE, and ECDHE public key algorithms? Specifications 59 Compliance Compliance 107 Section 9 - Technical Specifications Annexure J - Technical Compliance Specifications 59 Annexure J - Technical Compliance Support MSS, DES, RC4, and Camellia Symmetric key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence wer equest removal of point 112 as duplicated. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J -					ECDHE-RSA-AES256-SHA384		
106 Job Her RSA AES126-SHA256 106 DHE RSA AES126-SHA256 ECDHE-RSA AES126-SHA256 ECDHE-RSA AES126-SHA BOHE-RSA AES128-SHA Annexure J - Technical Specifications 59 Compliance Support MSA, DHE, and ECDHE public key algorithms? Intersection 9 - Technical Annexure J - Technical Specifications 59 Compliance Support MSA, DHE, and ECDHE public key algorithms? Difference Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated. 108 Section 9 - Technical Specifications Support AES, DES, RC4, and Camellia symmetric key algorithms? Disp USE, RC4 and Camellia are weak ciphers and ence in the benefit of NPCI we request not ouse the same in your environment. Refer to corrigendum 108 Specifications 59 Compliance Support MDS, SHA-1, and SHA-256 hash algorithms? MDS being a weak ciphers and can be easily manip	1 1				ECDHE-ECDSA-AES256-SHA384		
106 DHE-RSA-AES236-SHA256 ECDHE-RSA-AES128-SHA ECDHE-CDSA-AES128-SHA ECDHE-CDSA-AES128-SHA ECDHE-RSA-AES126-SHA DHE-RSA							
105 Section 9 - Technical Specifications 59 Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers and paint 112 as duplicated. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers and hence in the benefit of NPC weak ciphers and hence in the benefit of NPC weak ciphers and hence in the aster in your environment. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Compliance Support RSS, SNA-1, and SNA-256 hash algorithms? More weak ciphers and hence in the benefit of NPC were consent. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Compliance Support AES, 3DES, DSS, NA-1, and SNA-256 hash algorithms? More werequest removal of point 112 as duplicated. Refer to corrigendum							
107 Section 9 - Technical Annexure J - Technical Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Support RSA, DHE, SA, AES3, DES, RC4, and Camellia Symmetric key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Support RSA, DHE, and SCDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms? Support AES, 3DES, DES, RC4 and Camellia Symmetric key algorithms? Buplicate as point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms? Support AES, 3DES, SIA-1, and SHA-256 hash Ausciphers and hence in the benefit of NPC we request not to use the same in your environment. Refer to corrigendum	106						
107 Section 9 - Technical Specifications Annexure J - Technical Specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers and deale which are more prefices than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more prefices than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum	1 1						
Image: section 9 - Technical SpecificationsAnnexure J - Technical SpecificationsSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum107Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum108Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum108Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum108Section 9 - Technical SpecificationsSupport MDS, SHA-1, and SHA-256 hash algorithms?MDS being a weak ciphers and can be easily manipulated we recommendRefer to corrigendum							
107 Section 9 - Technical Specifications Annexure J - Technical Specifications Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point Refer to corrigendum 107 Section 9 - Technical Specifications 59 Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia specifications Support AES, 3DES, DES, RC4, and Camellia are weak ciphers and hence in the some in your environment. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia are weak ciphers and hence in the some in your environment. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Support AES, 3DES, DES, RC4, and Camellia are weak ciphers and hence in the some in your environment. Support AES, SHA-1, and SHA-256 hash algorithms? Support AES hash algorithms? Refer to corrigendum							
107 Section 9 - Technical Specifications Annexure J - Technical Specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 107 Section 9 - Technical Specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum							
107 Section 9 - Technical Specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated. Refer to corrigendum 108 Section 9 - Technical Specifications 59 Support AES, 3DES, DES, RC4, and Camellia 3DES, DES, RC4 and Camellia 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia 3DES, DES, RC4 and Camellia 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Section 9 - Technical Specifications Support MDS, SHA-1, and SHA-256 hash algorithms? MDS being a weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum							
Section 9 · TechnicalSection 9 · TechnicalSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum107Section 9 · Technical SpecificationsAnnexure J · Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum108Section 9 · Technical SpecificationsSupport AES, 3DES, DES, RC4, and Camellia symetric key algorithms?Support AES, 3DES, DES, RC4, and Camellia symetric key algorithms?Refer to corrigendum108Section 9 · Technical SpecificationsAnnexure J · Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symetric key algorithms?Support AES, 3DES, DES, RC4, and Camellia and support AES, 3DES, DES, RC4, and Camellia agorithms?Refer to corrigendum108Section 9 · Technical SpecificationsSupport AES, 3DES, SHA, and SHA-256 hash algorithms?MDS being a weak ciphers and can be easily manipulated we recommendRefer to corrigendum	1 1						
Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceAnnexure J - Technical ComplianceAnnexure J - Technical AES256-SHADuplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic.Refer to corrigendum107Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic.Refer to corrigendum107Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum108Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum108Specifications59ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MDS being a weak ciphers and can be easily manipulated we recommendRefer to corrigendum							
Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceAES256-SHAAES256-SHA107Section 9 - Technical SpecificationsSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum107Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum108Section 9 - Technical SpecificationsSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?3DES, DES, RC4 and Camellia aspecificationsRefer to corrigendum108Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia aymetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum108Fer to complianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommendRefer to corrigendum							
Section 9 - Technical Specifications Annexure J - Technical Compliance AES128-SHA AES256-SHA 107 Section 9 - Technical Specifications Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated. Refer to corrigendum 107 Section 9 - Technical Specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia symetric key algorithms? 3DES, DES, RC4 and Camellia aspmetric key algorithms? BES, DES, RC4 and Camellia aspmetric key algorithms? BES, DES, NC4 and Camellia aspmetric key a	1 1						
Technical Specifications Annexure J - Technical Compliance Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 107 Section 9 - Technical Specifications Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia specifications Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia aveak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Support MDS, SHA-1, and SHA-256 hash algorithms? MDS being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum		Castian O					
Specifications 59 Compliance AL220-0114 107 Section 9 - Technical Specifications Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 107 Section 9 - Technical Specifications Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 108 Section 9 - Technical Specifications Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia asymmetric key algorithms? Refer to corrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia symmetric key algorithms? Benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Support MDS, SHA-1, and SHA-256 hash algorithms? MDS being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum	1 1						
107Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum108Section 9 - Technical SpecificationsSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?3DES, DES, RC4 and Camellia benefit of NPCI we request not to use the same in your environment.Refer to corrigendum108Section 9 - Technical SpecificationsAnnexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum108Support MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommendRefer to corrigendum					AES256-SHA		
107 Section 9 - Technical Specifications Annexure J - Technical Specifications Annexure J - Technical Specifications Annexure J - Technical Specifications Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated. Corrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum		Specifications	59	Compliance			
107 Section 9 - Technical Specifications - Annexure J - Technical Compliance -							
107 Section 9 - Technical Specifications Annexure J - Technical Compliance Annexure J - Technical Compliance Beneric. Hence we request removal of point 112 as duplicated. Hence we request removal of point 112 as duplicated. 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 108 Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum					algorithms?	1 ·	corrigendum
Section 9 - Technical Annexure J - Technical Hence we request removal of point Specifications 59 Compliance 112 as duplicated. 108 Section 9 - Section 9 - Support AES, 3DES, DES, RC4, and Camellia 3DES, DES, RC4 and Camellia Specifications 59 Compliance Support AES, 3DES, DES, RC4, and Camellia 3DES, DES, RC4 and Camellia Section 9 - Technical Annexure J - Technical Support AES, 3DES, DES, RC4, and Camellia 3DES, DES, RC4 and Camellia Section 9 - Corrigendum Specifications 59 Compliance Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum	107					P	
Specifications 59 Compliance 112 as duplicated. 108 Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum Image: Compliance Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum	107					15	
Section 9 - Technical Specifications Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia abenefit of NPCI we request not to use the same in your environment. Refer to corrigendum Image: Note of the symmetric key algorithms? Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum						Hence we request removal of point	
Section 9 - Technical Specifications Section 9 - Technical Specifications Section 9 - Specifications Manexure J - Technical Compliance Symmetric key algorithms? weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Corrigendum Image: Specifications 59 Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum		Specifications	59	Compliance			
108 Technical Specifications Annexure J - Technical Specifications Annexure J - Technical Compliance Number Rely algorithms Nume	ΙT				Support AES, 3DES, DES, RC4, and Camellia	3DES, DES, RC4 and Camellia are	Refer to
I echnical Annexure J - Technical benefit of NPCI we request not to use benefit of NPCI we request not to use Specifications 59 Compliance the same in your environment. benefit of NPCI we request not to use Image: Specifications 59 Compliance Support MDS, SHA-1, and SHA-256 hash MD5 being a weak ciphers and can be Refer to Image: Specifications algorithms? easily manipulated we recommend corrigendum	100				symmetric key algorithms?		corrigendum
Specifications 59 Compliance the same in your environment. Model Image: Specifications Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend Refer to corrigendum	100	Technical		Annexure J - Technical		benefit of NPCI we request not to use	
algorithms? easily manipulated we recommend corrigendum		Specifications	59	Compliance			
					Support MDS, SHA-1, and SHA-256 hash		Refer to
					algorithms?	easily manipulated we recommend	corrigendum
not to use the same and should be						not to use the same and should be	
Section 9 -	109	Section 9 -				removed from the clause as this	
Technical Annexure J - Technical would compromise security.		Technical		Annexure J - Technical			
Specifications 59 Compliance		Specifications	59	Compliance			

				Total Packet processing capacity of single	Conflicts with the requirement		Refer to
				Total Packet processing capacity of single			
				device should be 1 Gbps	mentioned in point 1 which mentions		corrigendum
					Hardware appliance should be able to		
					handle 500Mbps in total.		
					In total traffic of 500Mbps if we		
					consider 40-50% https traffic it comes		
110					to around 200-250Mbps of HTTPS		
					traffic.		
					Hence we request clarification on		
					actual requirement of HTTPS/SSL		
					decryption and encryption traffic		
	Section 9 -				capabilities on total 500Mbps traffic		
	Technical		Annexure J - Technical		mentioned in point 1.		
	Specifications	59	Compliance				
				The bidder should have reported minimum	We request to amend the caluse as "		No Change in RFP
				annual turnover of Rs. 5 crores in each of the	Should we have Positive NETWORTH	We request you to amend the caluse as Due	
				last 3 financial years and should have reported	instead of profit after tax in last 3	to Pandemic our Profit after Tax is not	
				profits (profit after tax) as per audited	financial years (FY 2018-19, 2019-20,	there in FY-20-21 however we have postive	
111	4.1 Eligibility	56		financial statements in last 3 financial years	2020-21). Or should be Profit After	networth. In lockdown the profit after tax	
	Criteria			(FY 2018-19, 2019-20, 2020-21).	Tax in any two FY.	affected due to many reason. All other PSU	
						BFSI considering this caluse and giving	
						relaxation for FY20-21. PLease help to	
			2.1			amend so that we can submit our BID.	
	Payment Terms:	29	8.19	AMC: Payment shall be made quarterly in	We request to amend the payment		No Change in RFP
				arrears within 30 days from the date of	term as Yearly Advance as it is		
				receipt of invoice along with submission of	software and need to bill on Year		
112				completion report/ necessary documents /	basis		
				Certificates / Reports duly verified by NPCI			
				officials.			
	Delivery schedule	25	8.1	Delivery of hardware, software, and license	Please help to amend this as delivery		No Change in RFP
113	· · ·	_,		should be within 6 weeks	in 8-10 weeks as now deliveies are		
					getting affected.		
				Technical Training should be arranged by OEM	Request NPCI to consider the "		Refer to
	Section 3 - Scope of			directly.	Technical Training should be		corrigendum
114	Work	10	Section 3.1: Scope of Work		arranged by OEM/ OEM Authorized		conigenaam
	WORK				Partners".		
				Appliance (APT)- minimum of 04 Nos. as active			Should have total of
					this requirement.		4 APT devices with
				active for two DC, followed by Management & Database servers.			
				Dalabase servers.			2 in DC and 2 in DR
							having Active-
		40					Active setup
115	3.1 Scope of work:	10					deployment.
							Setup for
							management and
							Database should be
							same for both DC &
							DR.

116	3.1 Scope of work:	10		The user license for the appliance is required to support 3000 Users in DC-DR Model with complete failover to 100% capacity at each site.	Are the Endpoint Users using any EDR Solution? Since NPCI has asked for Network APT solution, please help us on the Use case to support 3000 Users in DC-DR.	Count is only for amount of traffic to be supported at network APT.
117	3.1 Scope of work:	10		Integrate the solution with the NPCI's Active Directory system for authentication & other application based on rest APIs.	Request NPCI to share the details of Other application to be integrated based on REST API's, this will help us to define the effort estimates for 3rd party integration.	Integration with open source SOAR platform.
118	3.1 Scope of work:	10		Bidder should support the migration of the Network APT security policies and features and building new policies required by organization for the proposed solution during the implementation phase.	How many Policies & Features are currently configured & enabled in existing Network APT? request NPCI to sahre the details of Existing Network APT solution.	Details related to configuration will be shared with successful bidder.
	Section 5 - Instruction to Bidders	16	5.12 Signing of Bid	The Bid shall be signed by a person or persons duly authorized to sign on behalf of the Bidder. All pages of the bid, except for printed instruction manuals and specification sheets shall be initialed by the person or persons signing the bid.	Request NPCI to accept the degitally signed documents using as valid "Digital signing Certificate".	Digtilly signed documents are aceepted
120	7.3 Technical Scoring Matrix:	21	Proposed Solution Part - C, Point 1	Approach /Methodology /Quality of Sample reports and RFP documentation	Reuqest NPCI to elaborate on Quality of Sample reports and RFP documentation requirement since this can be provided by the winning bidder post implementation.	Yes
121	7.3 Technical Scoring Matrix:	21	Proposed Solution Part - C, Point 7	OEM Technical Training for NPCI officials (Detailed technical training before Project Kick off and 5 days Post Implementation Training)	Please share the count of personnel attending training from NPCI.	5-7 members from NPCI
122	Section 8 - Terms and Conditions	23	8.4 Performance Bank Guarantee	The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order (exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months from the date of expiry of the validity period of the Bank Guarantee (BG), as per statutory provisions in force. In case the successful bidder does not submit the PBG, NPCI shall be entitled to withhold an amount equal to the value of the PBG from the payments due to the successful bidder. PBG may be invoked in case of violation of any of the Terms and Conditions of this Purchase Order and also in case of deficiency of the services provided by successful bidder.	Request NPCI to limit the Value of PBG to 3 % of Contract value as per guidelines of Ministry of Finance, Department of Expenditure Procurement Policy Division (No. F.9/4/2020-PPD) dated 30th December 2021 which are applicable to all tenders/ contracts issued/ concluded till 31st March 2022.	No Change in RFP

	Section 8 - Terms and Conditions 8.8 Key Deliverables		8.8 Key Deliverables	Post Implementation: OEM is annually required to review the deployment and suggest fine tuning, a minimum 7-10 days per year review & fine tuning effort of the OEM needs to be factored for implemented solution. Detailed implementation reports, HLD's & LLD's, Throughput achievement, QAT (Quality Assurance Testing), Hardening documents for APT security, performance, quality and functioning.	Request NPCI to consider this clause as " Post Implementation: OEM/OEM Auhtorized Partner is annually required to review the deployment and suggest fine tuning, a minimum 7- 10 days per year review & fine tuning effort of the OEM/OEM Auhtorized Partner needs to be factored for implemented solution." Our understanding is this needs to be provided by the sucessful bidder? Pls clarify.	It should be reviewed by OEM only. Data collection can be done by bidder. Yes, documentation needs to be shared by successful bidder as a part of implementation.
125	Section 8 - Terms and Conditions	25	8.12 End of Sale	The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL) or would become EOSL during the contract period. Further, if any of the components is declared EOSL during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI.	Requust NPCI to consider the End of Sale (EOSL) period as maximum 1 year only as there will be revision and updage on products every year. Request NPCI to consider the clause as :- "The bidder is required to quote components of the Solution offered of the latest technology, version, make, model, etc. The bidder should not quote any component of the solution that has been declared as End of Sale (EOSL)-or would become EOSL during the contract period. Further, if any of the components is reached declared-End of Support EOSL during the contract period commencing from the submission of bid, it must be replaced by bidder with another of equivalent or higher configuration at no extra cost to NPCI."	No change in RFP
126	8.10 Delivery schedule	25		Delivery, Installation & commissioning of the solution should be completed within 12 weeks from the date of receipt of purchase order. • Delivery of hardware, software, and license should be within 6 weeks. • Installation & commissioning should be completed in next 6 weeks.	Reques NPCI to change this to "Delivery, Installation & commissioning of the solution should be completed within 18 weeks from the date of receipt of purchase order. • Delivery of hardware, software, and license should be within 8 weeks . • Installation & commissioning should be completed in next 10 weeks ."	Refer to corrigendum

				The successful bidder shall provide	Request NPCI to change this to "The	Refer to
				comprehensive on-site maintenance (AMC) of	successful bidder shall provide	corrigendum
				the solution for a period of 3 years with back	comprehensive on-site/Remote	
				to back support with the OEM, including	maintenance (AMC) of the solution	
127	8.14 Support	26		warranty period of 1 year and 2 years support	for a period of 3 years with back to	
				post expiry of the warranty period of 1 year.	back support with the OEM, including	
					warranty period of 1 year and 2 years	
					support post expiry of the warranty	
					period of 1 year."	
				The Bidder shall monitor and maintain the	Request NPCI to remove this clause	No change in RFP
				stated service levels to provide quality	Or the bidder can use existing SLA	
128	8.15 Service Level	27		service. Bidder to use automated tools to	tools provided by NPCI.	
120	Requirements (SLA)	21		provide the SLA Reports. Bidder to provide		
				access to NPCI or its designated personnel to		
				the tools used for SLA monitoring.		
				8.15 Penalty on non-adherence to SLAs: as per		No Change in RFP
129	Section 8 - Terms	28	8.15 Penalty on non-	RFP	maximum penalty due to non-	
/	and Conditions	20	adherence to SLAs:		adherence of SLA will not exceed 10%	
					of the total cost of the project.	
				NPCI reserves the right to place Purchase	Request NPCI to consider the repeat	No change in RFP
				Orders with the selected bidder(s) for any or	order validity as maximum 6 months	
	Section 8 - Terms			all of the deliverables included in the Solution	from the price discovery date.	
130	and Conditions	29	8.17 Repeat Order:	at the agreed unit rate for individual		
				categories of purchase order during the period		
				of 3 years from the date of award / 1st		
				Purchase Order.		
				Software/Licenses: Payment shall be released within 20 days after delivery of the	Request NPCI to confirm the 100%	No change in RFP
	Continu 9 Tarres			released within 30 days after delivery of the	Software payment released on	
131	Section 8 - Terms and Conditions	29	8.19 Payment Terms:	software /licenses along submission of correct		
	and conditions			invoice with necessary supporting documents	along with the submission of	
				and delivery/installation report duly signed by NPCI officials		

132	Section 8 - Terms and Conditions	30	8.22 Indemnity	all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting from any act or omission or negligence or misconduct of the bidder and its	We propose to modify the clause: The bidder shall indemnify, protect and save NPCI and hold NPCI harmless from and against all claims, losses, costs, damages, expenses, action suits and other proceedings, (including reasonable attorney fees), relating to or resulting from any act or omission or willfull negligence or misconduct of the bidder and its employees and representatives, breach of the terms and conditions of the agreement , false statement by the bidder, employment claims of employees of the bidder, third party claims arising due to infringement of intellectual property rights, death or personal injury attributable to acts or omission of bidder, violation of statutory and regulatory provisions including labour laws, laws related to information technology and intellectual property rights, breach of confidentiality obligations, breach of warranty, etc.		Minor changes hence acceptable
133	Section 8 - Terms and Conditions	30	8.23 Bidder's Liability	The selected Bidder will be liable for all the deliverables. The Bidder's aggregate liability in connection with obligations undertaken under the purchase order, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the value of the contract/purchase order.	The selected Bidder will be liable for all the deliverables. The Bidder's aggregate liability in connection with obligations undertaken under the purchase order, regardless of the form or nature of the action giving rise to such liability (whether in contract, tort or otherwise), shall be at actual and limited to the value of the contract/purchase order.Neither Party shall be liable to the other Party for loss of profit, loss of any contract or for any indirect or consequential loss or damage which may be suffered by the other Party regarding this Tender		Waiver of consequential damages is present in the RFP document already. No Change in RFP
134	RFP-for- procurement-of- Network APT- Solution	10	3.1 - Scope of Work	The bidder / OEM shall provide 24*7*365 basis post implementation technical support for the components supplied. Support center must be based in INDIA.		The bidder / OEM shall provide 16*5*365 basis post implementation technical support for the components supplied. Support center must be based in INDIA.	No Change in RFP

	RFP-for- procurement-of-	23	8.4 - Performance bank guarantee	The Successful bidder shall, within 14 working days of receipt of Purchase Order, submit a		The Successful bidder shall, within 14 working days of receipt of Purchase Order,	No Change in RFP
135	Network APT- Solution		Summer	Performance Bank Guarantee (PBG) equal to 10% of total value of the Purchase order		submit a Performance Bank Guarantee (PBG) equal to 3% of total value of the Purchase	
				(exclusive of taxes), valid for 1 year, with a claim period of 12 (twelve) months		order (exclusive of taxes), valid for 1 year, with a claim period of 3 months	
	RFP-for-	29	8.19 - Payment terms	AMC- Payment shall be made quarterly in			No Change in RFP
	procurement-of-			arrears within 30 days from the date of		advance within 30 days from the date of	
136	Network APT- Solution			receipt of invoice along with submission of completion report/ necessary documents / Certificates / Reports duly verified by NPCI officials.		receipt of invoice along with submission of completion report/ necessary documents / Certificates / Reports duly verified by NPCI officials.	
			8.1 Delivery Shedule	Delivery, Installation & commissioning of the		Please change - Delivery, Installation &	Refer to
137				solution should be completed within 12 weeks from the date of receipt of purchase order		commissioning of the solution should be completed within 14-16 weeks from the date of receipt of purchase order	corrigendum
(20				Delivery of hardware, software, and license			Refer to
138				should be within 6 weeks		should be within 8 weeks	corrigendum
139				Installation & commissioning should be		Installation & commissioning should be	Refer to
		37	Castian O. Tashaisal	completed in next 6 weeks	De succetions to allow so it to 4 Chara	completed in next 8 weeks	corrigendum
	RFP-for- procurement-of-	37	Section 9- Technical Specifications- Point no 1	Hardware Appliance must be able to handle minimum of 500 Mbps of traffic capacity for	Requesting to change it to 1 Gbps throughput as NPCI has asked for SSL		Minimum requirement is to
140	Network APT-		specifications Formenio 1	inspection & inline blocking	inspection throughput of 1 Gbps in		inspect 500 MBPS of
	Solution			hispection a mane blocking	the point no.119		traffic capacity.
	RFP-for-	41	Section 9- Technical	Ability to configure encryption/decryption	This specific point is of dedicated SSL		Refer to
	procurement-of-		Specifications-Point no 106	policy (incl. block/pass-through) based on	appliance whereas NPCI has asked for		corrigendum
141	Network APT-			Subject / Domain Name	the SSL capabilities on the inline APT		
	Solution				appliance. Hence, requesting the NPCI to dilute this point.		
	RFP-for-	41	Section 9- Technical	Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3,	SSLv2 is deprecated since 2011 due to		Refer to
142	procurement-of-		Specifications-Point no 110	SSL3, and SSL2 encryption protocols?	having several security flaws. Hence,		corrigendum
172	Network APT- Solution				requesting the NPCI team to remove SSL2 from this point.		
	RFP-for-	42	Section 9- Technical	Support MD5, SHA-1 & SHA-256 hash	MD5 is deprecated, hence, requesting		Refer to
143	procurement-of- Network APT-		Specifications-Point no 114	algorithms?	the NPCI team to remove MD5 from this point.		corrigendum
	Solution						
	RFP-for-	42	Section 9- Technical	Ability to support an integrate with any	Since NPCI has asked for the SSL		Solution should be
	procurement-of-		Specifications-Point no 116	existing CA solution and current PKI structure	capabilities on the APT appliance, it		able to integrate
	Network APT-				can import keys from existing		with existing NPCI
	Solution				solutions but no direct-integration		PKI solutions for
144					from the on-premise CA Solution		dash board
					appliance is possible as it is not a		preparation and CA
					dedicated SSL appliance. Hence, requesting the NPCI team to dilute		solution for incident
					this point.		management.

				Hardware should have minimum capacity of 1	For Network Anti-APT solution where	Refer to
				ТВ	the analysis has to done at wire speed	corrigendum
					on the traffic with aggressive packet	
					capture, it is recommended that the	
					Network Anti-APT appliance should	
					have minimum 2 HDD with atleast	
					4TB of capacity to ensure the	
					analysis to complete in near real-	
					time.	
145					une.	
145						
					Hence in the benefit of NPCI which	
					falls in National critical infrastructure	
					should have minimum 2 x 4TB HDD	
					and request amendment to the clause	
					to:	
					"Hardware should have minimum 2	
	Section 9 -				HDD with atleast 4TB of capacity	
	Technical		Annexure J - Technical			
	Specifications	37	Compliance			
				The proposed solution must be available as on	NPCI being an National Critical	Refer to
				premise physical appliances with sandboxing	Infrastructure of India where	corrigendum
				capability	information is very sensitive it is	-
					recommended to have complete	
					analysis to be performed by the	
					Network Anti-APT on premises. The	
					overall solution architecture should	
					be such that the complete sandboxing	
					must be performed on-premises & no	
					objects/files should be sent to the	
					vendor cloud as they may contain	
					either confidential data or Personally	
					identifiable information (PII) Data.	
146					We would like to bring it to NPCI	
'"					notice that as the clause does not	
1					state complete sandboxing	
1					environment on premises including	
					various operating systems &	
					applications like Windows OS & its	
1					applications, Linux OS & its	
1					applications & MAC OS & its	
					applications in absence of this being	
					stated NPCI would not be able to	
					control the file/objects submissions	
					to on-premises sandbox only. This	
					may lead to vendors submiting the	
1	Soction 0				files to the cloud without NPCI's	
1	Section 9 -				knowledge.	
	Technical	37	Annexure J - Technical		interreuse.	
	Specifications	37	Compliance			

		<u>г т</u>		Proposed APT solution should parform	Clarification required Should we	[No change in RFP.
				Proposed APT solution should perform advanced network detection and analysis of	Clarification required, Should we read the clause as?		Should able to
					read the clause as?		
1				the enterprise's internal/External network	"Drepend ADT solution should		perform detection
147				data.	"Proposed APT solution should		on Intenal (east-
	Section 9 -				perform advanced network		west), External
	Technical		Annexure J - Technical		detection and analysis of the		(inbound-outbound)
		37	Compliance		enterprise's inbound/outbound		traffic.
<u> </u>	Specifications	3/	compliance		network traffic."		
				The proposed solution should support to	As per clause number 1 of the		Refer to
				monitor traffic from multiple segments	Technical Specifications the Network		corrigendum
				simultaneously on single appliance (East-West			
				North-South).	handle 500Mbps of total traffic. In		
					any organization where North-South		
					(Internet Traffic) is typically based on		
					total internet bandwidth and is same		
					or less than the total internet		
					bandwidth, but East-West traffic		
					(Intranet Traffic) i.e. from		
					LAN/Client segment to Server		
					segment the traffic may be huge		
					somewhere around 1Gbps to 4Gbps as		
					it is internal traffic, this would		
148					exceed 500Mbps appliance capacity		
140					anytime. Also North-South and East-		
					West segments are completely		
					different and may pass through		
					different Core Switches and may not		
					be feasible at times for connectivity.		
					Hence we would request NPCI to		
					please share North-South traffic		
					detail in Mbps/Gbps and East-West		
					traffic in Mbps/Gbps to ensure all the		
					traffic is covered by Network Anti-		
					APT solutions and also confirm if		
1	Section 9 -				connectivity for North-South traffic		
	Technical		Annexure J - Technical		and East-West traffic is feasible or		
	Specifications	37	Compliance		not.		
				The proposed solution should be dedicated	Similar to point 11 which is in more		Refer to
1				appliance and should not be enabled as	details, hence we request NPCI to		corrigendum
149				additional licensed solution with proposed	remove this point as duplicate.		
1	Technical		Annexure J - Technical	perimeter gateway devices such as firewall,			
1	Specifications	37	Compliance	APT etc.			
				Security Vendor must have a Research/Labs	Reporting on Vulnerabilities is	Refer to	
------	----------------	----	------------------------	---	--	-------------	
				organization and this organization must	primary function of Vulnerability	corrigendum	
				contribute and report on finding new Zero-Day		conigenaam	
				vulnerabilities being exploited in the wild.			
				• •	As a Network Anti-APT solution the		
					primary & most important function is		
					to prevent Zero-Day exploits in the		
					wild from targeting the		
					vulnerabilities. Also in real world, the		
					zero day explots may not available at		
					the same time when the actual		
					vulnerabilitiy is identified, hence it is		
					important to detect & prevent zero		
150					day expliots / payloads.		
1.20							
					Hence to benefit from the Network		
					Anti-APT we request NPCI to modify		
					this clause as:		
					"Security Vendor must have a		
					Research/Labs organization and this		
					organization must contribute and		
					report on finding new Zero-Day		
					expliots being identified / discovered in the wild & should		
	Section 9 -				automatically share the intel to the		
	Technical		Annexure J - Technical		Network Anti-APT Solution".		
	Specifications	37	Compliance		ALL ALL ALL ALL SOLUTION .		

						1	
				The proposed solution should be able to	Need for clarification on this point		Refer to
				detect any suspicious communication within	specifically Outside of Customers		corrigendum
				and outside of Customer's network	Network as it typically false in the		
					requirement of perimeter solutions		
					like Firewall / IPS.		
					With regards to within the network		
					With regards to within the network		
					suspicious communications would		
					NPCI like to detect malicious post-		
					exploitation activities such as		
					attacker lateral movements between		
					user workstation & servers? as		
					Attackers frequently use SMB & SMB2		
					to carry their activity from		
151					compromised endpoints and move to		
1.21					servers, hiding their activities in		
					normal traffic.		
					If Yes, we would recommend NPCI to		
					modify the clause to:		
					"The proposed network Anti-APT		
					solution should also be able to		
					detect malicious post-exploitation		
					activities such as attacker lateral		
					movements between user		
					workstation & Servers. Attackers		
					frequently use SMB & SMB2 to		
	Section 9 -				carry their activity from		
	Technical		Annexure J - Technical		compromised endpoints and move		
	Specifications	37	Compliance		to servers, hiding their activities		
				The Proposed solution should be able to	We would like to highlight this		Refer to
1				detect communications to known command	requirement only mentions detection		corrigendum
1				and control centers.	of known Command and Control		
					Centers (C&C) only and not blocking		
					of the C&C as well it do not covers		
					unknown C&C detection and blocking.		
1					Hence in the benefit of NPCI we		
					request the clause to be changed to:		
152							
					"The Proposed solution should be		
1					able to detect communications to		
					known & unknown command and		
					control center initiated by internal		
					infected clients."		
	Section 9 -						
1	Technical		Annexure J - Technical				
	Specifications	37	Compliance				

				The proposed solution should be able to	Primarily this requirement falls in the	Refer to
				detect reputation of URL being accessed	category of Proxy Solution	corrigendum
				detect reputation of one being accessed	requirement where reputation of the	conigendum
					URL plays a very important role,	
					however in Network Anti-APT the	
					analysis is not limited to just URL	
					reputation but it should be able to	
					analyze complete URL's in zero-trust	
153					manner as attackers take advantage	
					of the URL reputation check tools to	
					launch sophisticated attacks and	
					compromise the Host/End-user.	
					compromise the host/ End user.	
	Section 9 -				Hence we recommend to remove or	
	Technical		Annexure J - Technical		modify the clause.	
	Specifications	37	Compliance			
			·	The proposed solution should support at least	In an Advanced Attack threat actors	Refer to
				100+ protocols for inspection	leverage C&C communication to	corrigendum
					command & control the victim	•
					machine, hence it is important for an	
					organization to block all malicious	
					C&C communications regardless of	
					ports and protocols, hence we	
154	+				request NPCI to change the clause to:	
					"The proposed solution for Network	
					Ani-APT should prevent any C&C	
					communications detected over North-	
	Section 9 -				South traffic regardless of ports and	
	Technical		Annexure J - Technical		protocols"	
	Specifications	38	Compliance			

				Sandbox must have the ability to simulate the	There are various flavors of Sandbox	Refer to
				entire threat behavior.	environment used for analysis and	corrigendum
					not limited to just Windows OS but	consendant
					also Linux, MAC OS with 32bit and	
					64bit architecture and various types	
					of applications targeted in the wild.	
					b) apprecisions targeted in the inter-	
					Hence in the benefit of NPCI we	
					request the clause to be very specific	
					like:	
					"The proposed solution must be	
155					available as on premise physical	
					appliances with sandboxing	
					capability and must be able to	
					detect and report malware by	
					using multiple client environments	
					(operating systems with multiple	
					service pack levels) supporting	
					both x64 and x86 architectures	
					including Windows, Mac, CentOS	
	Section 9 -				based on premise Virtual Execution	
	Technical		Annexure J - Technical		Environment"	
	Specifications	38	Compliance			
				The proposed solution should have an built-in	OEM Specific Clause.	Refer to
				document vulnerabilities detection engine to		corrigendum
				assure analysis precision and analysis	We request removal of the clause as	
156				efficiency	the requirement gets addressed in	
	Section 9 -				detection of Zero-Day exploits	
	Technical		Annexure J - Technical		targeting vulnerabilities in the wild in	
	Specifications	38	Compliance		clause 19 and 20.	

				The proposed solution should support Multiple	Advanced attackers once establish	Refer to
				protocols for inspection. Example:- HTTP,	the foothold tries to move laterally	corrigendum
					and dump sophisticated tools on	corrigendum
				protocols Internal direction: SMB ,Database	various systems connected in the	
					network detecting this tools and	
				device	identifying this tools and techniques	
					plays a very important and critical	
					role in early detection and incident	
					response.	
					Hence in the benefit of NPCI it is	
					important to get visibility of such	
					activities of the threat for which we	
					request modification of the clause to	
					below:	
157					below.	
					"The proposed solution should be	
					able to detect the activities of	
					attackers already resident in the	
					network core. The solution should	
					extracts malware and objects that	
					are transferred over HTTP, FTP &	
					other protocols and submit them to	
					the automated dynamic Analysis	
					engine for detonation and	
					confirmation on maliciousness. The	
					solution should extracts malware	
	Section 9 -				and objects that are transferred	
	Technical		Annexure J - Technical		over HTTP, FTP like protocols and	
	Specifications	38	Compliance		submit them to an automated	
			· ·	The Proposed solution should have a Co-	Duplicate point as all the previous	Refer to
158	Section 9 -			relation engine to automatically co-relate	clause covers the same.	corrigendum
100	Technical		Annexure J - Technical	across multiple protocol, multiple sessions and	Request removal of the clause.	
	Specifications	38	Compliance	volume traffic analysis		

				The proposed solution should be able to	Advanced attackers leverage various	Refer to
				detect and prevent the persistent threats	types of files to infiltrate in the	corrigendum
				which come through executable files, PDF	target environment and not just	5
				files, Flash files, RTF files and and/or other	executables, pdf, flash or RTF file	
				objects.	types hence it is very important that	
					dynamic analysis engine should be	
					able to analyze different filetypes	
					without depending on the signatures.	
					······································	
					Hence for critical infrastructure like	
					NPCI should ensure that various	
					filetypes which are leveraged by the	
					advanced attackers should be	
					dynamically analyzed without	
					depending upon the signatures alone,	
159					in the benefit of NPCI we request	
					modification of this clause as follows:	
					"The proposed solution should have	
					the ability to analyze, detect and	
					block malware in common file	
					formats including but not limited	
					to executables, JAVA, PDF, MS	
					Office documents, common	
					multimedia contents such as JPEG,	
					QuickTime, MP3 and	
					ZIP/RAR/7ZIP/TNEF archives, 3gp,	
	Section 9 -				asf, chm, com, dll, doc, docx, exe,	
	Technical		Annexure J - Technical		gif, hip, htm, ico, jar, jpeg, jpg,	
	Specifications	38	Compliance		mov, mps, mp4, pdf, png, ppsx,	

				The Proposed solution should be able to	In a sophisticated attack the	Refer to
				generate out of box reports to highlight	advanced attackers may or may not	corrigendum
				Infections, C&C behavior, Lateral Moment,	use malware, but they definitely use	
				Asset and data discovery and Exfiltration	various techniques & methodologies	
				Asset and data discovery and Exiteration	to move laterally, hence it is	
					important for a solution to detect	
					TTP's and methodologies and alert	
					with timeline & date sliders with at	
					least 5 minutes of relevant network	
					activity data(layer 4-7) before and	
					after the attack.	
					Hence in the benefit of NPCI we	
					request modification of this clause	
					with must have capabilities as:	
160					with must have capabilities as.	
					Proposed Internal Network APT	
					should detects the following types of	
					malicious post-infection activities:	
					a) Internal Reconnaissance	
					b) Privilege Escalation	
					c) Credentials Dumping	
					d) Lateral Movement of Malware	
					e) Remote Task Execution	
					f) Data Exfiltration Detection	
					g) Callback activities	
					h) Bot-tracker features like File	
	Section 9 -				inspection, Packet flows, Signature	
	Technical		Annexure J - Technical		matching and statistics	
	Specifications	38	Compliance		i) Supports extensive metadata	
			F	The proposed APT must able to operate in	Analyzing asymmetric traffic results	Refer to
				Asymmetric traffic environment with	in ton's of false positive's and adds	corrigendum
				Vulnerability / Exploit filters for protection	unnecessary workload on validation	-
					of such all the alerts resulting in Alert	
161					Fatigue on SOC team, hence we	
					request removal of such clause which	
	Section 9 -				adds overheads to security team and	
	Technical		Annexure J - Technical		miss on legitimate threats.	
	Specifications	38	Compliance		-	
ΙĪ		T		The proposed APT solution must support	OEM Specific IPS Solution, Request	Refer to
162	Section 9 -		Anna 1 7 1 1 1	Adaptive Filter Configuration(AFC) which will	removal of this clause.	corrigendum
	Technical	20	Annexure J - Technical	alert or disable ineffective filter in case of		
	Specifications	38	Compliance	noisy filters	Durkesta Clause D. 147	Defente
				The APT filter must support network action	Duplicate Clause, Point 17 covers the	Refer to
				set such as Block (drop packet), Block (TCP Bosot), Bormit, Trust, Notify, Traco(Backot	requirement hence we request removal of this clause.	corrigendum
				Reset), Permit, Trust, Notify, Trace(Packet Capture), Rate Limit and Quarantine	removal of this clause.	
163				Capture, Rate Linit and Quarantine	Also it is important for Anti-APT	
1 ¹⁰³					solution to Block callback to C&C and	
	Section 9 -				malicious communications in inline	
	Technical		Annexure J - Technical		maticious communications in intine mode.	
	Specifications	38	Compliance			
	specificacións	50	comptiance			1

				The proposed APT solution must support	Clause is OEM Specific IPS Solution	Refer to
				signatures, vulnerabilities and traffic filtering	which heavily depends upon signature	corrigendum
164	Section 9 -			methods to detect attacks and malicious	based detection.	-
	Technical		Annexure J - Technical	traffic		
	Specifications	38	Compliance		We request removal of this clause	
				The APT filters must be categories into the	Clause is OEM Specific IPS Solution,	Refer to
				following categories for easy management:	Request removal of this clause.	corrigendum
145				Exploits, Identity Theft/Phishing,		
165	Section 9 -			Reconnaissance, Security Policy, Spyware,		
	Technical		Annexure J - Technical	virus, Vulnerabilities, Traffic		
	Specifications	38	Compliance	Normalization, P2P, IM, Streaming Media		
				Vulnerability based filter are known for most	Clause is OEM Specific IPS Solution &	Refer to
166	Section 9 -			effectively for Zero Day Attack Protection and	only covers known attacks, Request	corrigendum
100	Technical		Annexure J - Technical	proposed solution must support vulnerability	removal of this clause.	
	Specifications	39	Compliance	based filter		
	Section 9 -			The proposed APT should support the ability	Clause is OEM Specific IPS Solution,	Refer to
167	Technical		Annexure J - Technical	to mitigate Denial of Service (DoS/DDoS)	Request removal of this clause.	corrigendum
	Specifications	39	Compliance	attacks such as SYN floods		-
	Section 9 -			The proposed APT must provide bandwidth	Clause is OEM Specific IPS Solution,	Refer to
168	Technical		Annexure J - Technical	rate limit to control the unwanted/nuisance	Request removal of this clause.	corrigendum
	Specifications	39	Compliance	traffic such as P2P, Online Game, etc.,		
				The proposed APT must be able to use	Clause is OEM Specific IPS Solution &	Refer to
				Reputation Service such as IP address or DNS	only covers known attacks, Request	corrigendum
169	Section 9 -			to block traffic from or to 'known bad host'	removal of this clause.	
	Technical		Annexure J - Technical	such as spyware, phishing or Botnet C&C		
	Specifications	39	Compliance			
				The proposed APT must be able to control the	Clause is OEM Specific IPS Solution &	Refer to
				known bad host such as spyware, botnet C2	only covers known attacks, Request	corrigendum
170	Section 9 -			server, spam and so on based on country of	removal of this clause.	
	Technical		Annexure J - Technical	origin, exploit type and the reputation score		
	Specifications	39	Compliance			
				Must have the ability to correlate the	The clause adds lot of dependency on	Refer to
				monitored attacks to the APT filters number	the security teams to continuously	corrigendum
				and recommended action	monitor and keep on modifying	
					policies increasing overheads and	
					false positives, Anti-APT solution	
					should be able to take decision with	
171					its intelligence with simple	
					configuration to Block or Monitor the	
					threat.	
	Section 9 -				Hence in the benefit of the NPCI we	
	Technical		Annexure J - Technical		request modification/removal of this	
	Specifications	39	Compliance		clause	

						
				NG APT engine must be a smart enough to	Detecting traffic based on suspicion	Refer to
				inspect the traffic based on condition, If the	or deep packet inspection needs	corrigendum
				traffic is suspicious then it goes for the deep	patterns / signatures to take	
				packet inspection	decisions, Anti-APT solution should	
172					not just depend upon signatures but	
1/2					it should have dynamic analysis	
					engine with signatureless detection	
	Section 9 -				and should create signatures in	
	Technical		Annexure J - Technical		Realtime and block the threats inline.	
	Specifications	39	Compliance			
			•	The proposed management system shall allow	Please correct our understanding	To be Integrated
				the update of global threat intelligence via	about local threat intelligence	with our TIP
				cloud and local Threat intelligence updates	sharing. Do you mean sharing	platform for threat
173				from proposed Network threat detection	intelligence from your existing Anti-	intelligence
'''	Section 9 -			solution automatically for inline blocking	APT solutions from Email & content	integration with
	Technical		Annexure J - Technical	solution automatically for intine blocking	scanning Anti-APT solutions to Anti-	other solutions
	Specifications	39	Compliance		5	
	specifications	57		The management convex must provide with	APT for Network Security?	deployed. Refer to
				The management server must provide rich	Rate Limiting, Misuse & Abuse,	
				reporting capabilities include report for All	Traffic Threshold & DDoS reports do	corrigendum
				attacks, Specific & Top N attack, Source,	not fall in Anti-APT solution, these	
174	c c			Destination, Misuse and Abuse report, Rate	are OEM specific and hence request	
	Section 9 -			limiting report, Traffic Threshold report,	NPCI to remove the same.	
	Technical			Device Traffic Statistics and Advance DDoS		
	Specifications	39	Compliance	report		
				The proposed management system must be	Critical infrastructure like NPCI may	Refer to
				able to support the syslog CEF format that	have various tools for event	corrigendum
				SIEM can support	correlation, automation,	
					orchestrations etc limiting to CEF	
					format only may limit integration	
					with other tools and result no	
					integration support. Hence we	
					request NPCI to modify the clause to	
					various types of log/event format but	
					not limited to CEF only.	
475						
175					Clause Modification to:	
					The proposed management system	
					must be able to support Common	
					Event Format (CEF), Log Event	
					Enhanced Format (LEEF), Comma-	
					Separated Values (CSV), XML,	
					JSON, or Text format that SIEM	
	Section 9 -				and other tools like automation	
	Technical		Annexure J - Technical			
	Specifications	39	Compliance		and orchestration can support.	
	specifications	72	comptiance			

176	Section 9 -			The proposed management system shall have a big data engine that allows customers to provide faster security analytics and faster report generation	To integrate with Big Data Analytics the solution should support file formats that can be ingested in the Big Data Analytics tool, hence we request NPCI to modify the clause and not mandate with Big Data Engine which makes the clause to OEM Specific. Request modification in clause to: "The Management system should support file formats which can be ingested in Big Data Analytics	Refer to corrigendum
	Technical Specifications	40	Annexure J - Technical Compliance		Solution for faster report generation."	
177				Automatic detection and response against an ever-growing variety of threats, including fileless and ransomware	This clause of Automatic detection and response requirement do not covers automatic prevention and integration with various other vectors of attack like Email, Endpoint EDR and File/content uploads from outside to respond to threats. In any enterprise organizations and critical infrastructure resilience defense strategy plays a very important role to defend against the advanced attack and hence should be in a Must Have category instead of Good to Have.	Refer to corrigendum
	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance		Does NPCI wants to take benefit of Anti-APT for network security solution requirement with automatic prevention and integration with various vectors of attack capabilities and not just detection and response? If yes we request modification of the clause to: "The solution must have automatic detection, prevention, remediation and integration capabilities with various attack vectors not limited	
			·	The industry's most timely virtual patching: Vulnerability Protection virtually patches	Clause is OEM Specific IPS Solution, Request removal of this clause.	Refer to corrigendum
178	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	known and unknown vulnerabilities, giving you instant protection, before a patch is available or deployable.		

				The solution should consolidate (at	To support Advanced Defense	
					To support Advanced Defense	Okay, No change in
				centralized location) the administration,	Strategy and build advanced	RFP.
179	Section 9 -			reporting, and intelligence data sharing	resilience infrastructure for NPCI it's	
			Annesium I. Technical	intelligence/IOC's between deployed Anti-APT	important clause.	
	Technical	10		Sensors/ solution at our organization (Email		
	Specifications	40	Compliance	Analysis, File Analysis & EDR)		
				Central Management should provide option to	To support Advanced Defense	No change in RFP
				create customized lists of IOCs received from	Strategy and build advanced	
				these feeds and use them as a custom	resilience infrastructure for NPCI it's	
				blacklist on the Central Management	important clause.	
180				appliance. The types of IOCs like URL		
100				indicators, IP address indicators, domain		
				indicators, and indicators with hashes of		
	Section 9 -			malicious files, combine them into a standard		
	Technical		Annexure J - Technical	format called STIX (Structured Threat		
	Specifications	40	Compliance	Information Expression)		
			· ·	Centralized Sandboxing	OEM specific clause, some of the	No change in RFP.
					OEM's provide Built-in Sandboxing	Prefer to have built
					solution and do not require any	in sandboxing
181	Section 9 -				additional/external Sandboxing	capabilities for
	Technical				solution. Hence we request NPCI to	Network Anti-APT
	Specifications				consider the same.	solutions.
	opeenreacions			The proposed solution should be able to run at		Refer to
				least 50 parallel sandboxes for analysis of	methods and technology to run	corrigendum
				payload and on premise customized sandbox	dynamic analysis and should not	corrigendum
				solution should have the capability to allow	mandate on 50 parallel sandboxes	
					1 · · · · · · · · · · · · · · · · · · ·	
				manual submission of suspicious files for	instead it is important to have	
				analysis	multiple executions to run in parallel	
					for payload analysis automatically	
					and not manually.	
					Some of the OEM who have	
					NO\limited number of Sandboxes built	
182					in depend upon external sandboxes	
					which supports manual submission of	
					files, hence we request for	
					modification of the clause to:	
					"The solution should support 1000+	
1					executions to analyze the payloads in	
1					parallel depending on the	
1					performance capacity upto 500Mbps	
1	Section 9 -				of the appliance deployed on-	
1	Technical		Annexure J - Technical		premises"	
1	Specifications	40	Compliance			

				Sandboxing Appliance should support	Not applicable for built-in sandboxing	No change in RFP.
				Active/Passive or Active-Active deployment	solution hence we request	
				and should support configuring cluster for	modification of the clause to:	"The Network Anti-
				High Availability		APT solution should
183					"The Network Anti-APT solution	support Active-
					should support Active/Passive or	Active, Active-
	Section 9 -				Active passive deployment on-	Passive
	Technical		Annexure J - Technical		premises"	deployment on-
	Specifications	40	Compliance		·	premises".
				The proposed solution must be capable of	Advanced attackers leverage various	Refer to
				analysis of different file types, including	types of files to infiltrate in the	corrigendum
				portable executables (PEs), web content, Web	target environment especially	•
				objects, images, Java, network flows,	Webshell attacks on Web Servers and	
					manipulate the server and redirect to	
					malicious content.	
				multimedia etc. including all such file types		
					Hence for critical infrastructure like	
					NPCI should ensure that various	
				channel, for initial compromise or backdoor or		
					advanced attackers should be	
					dynamically analyzed without	
					depending upon the signatures alone,	
					in the benefit of NPCI we request	
					modification of this clause as follows:	
184						
					"Solution should provide	
					comprehensive support for user	
					interaction framework for web	
					shells, support for shell scripts	
					(e.g.; python, Perl, and Ruby etc.),	
					support for ELF binaries, Server-	
					side attack detection, complete	
					user mode and kernel mode	
					monitoring from within and outside	
					the Guest Images, Web shell	
					detection support for JSP, PHP,	
	Section 9 -					
	Technical		Annexure J - Technical		and WAR (Web archive) file types etc."	
	Specifications	40	Compliance			
	specificacións	10	comptiance		I	

				Sandbox appliance should have redundant	For Network Anti-APT solution where	Refer to
				power supply, 2 TB or more storage capacity	the analysis has to done at wire speed	corrigendum
				with dedicated management port	on the traffic with aggressive packet	conigenaam
					capture, it is recommended that the	
					Network Anti-APT appliance should	
					have minimum 2 HDD with atleast	
					4TB of capacity to ensure the	
					analysis to complete in near real-	
185					time.	
105					cinc.	
					Hence in the benefit of NPCI which	
					falls in National critical infrastructure	
					should have minimum $2 \times 4TB HDD$	
					and request amendment to the clause	
	Section 9 -				to:	
	Technical		Annexure J - Technical		"Hardware should have minimum 2	
	Specifications	40	Compliance		HDD with atleast 4TB of capacity	
	Section 9 -			The Proposed Solution should be able to	Does NPCI only wants to detect	Refer to
186	Technical		Annexure J - Technical	detect known bad URL before sandboxing	known bad URL's only?	corrigendum
1.00	Specifications	40	Compliance			conigenaam
			•	The proposed solution should detect file-less	Attackers use encoded algorithms like	Refer to
				malware tools used for extracting plain text	XOR to hide password instead of plain	corrigendum
				passwords, hash, PIN codes and Kerberos	text, do NPCI would like to detect	J
				tickets.	and extract passwords which are	
					encoded algorithm XOR instead of	
					just plain text? If yes,	
187					We request you to modify the clause	
10/					to:	
					"The proposed solution should	
					detect file-less malwares tools	
					used for extracting	
	Section 9 -				encoded/XOR'ed as well as plain	
	Technical		Annexure J - Technical		text passwords, hash, PIN codes	
	Specifications	40	Compliance		etc"	
				The Proposed solution should allow Admin be	Please provide clarification on the	Refer to
188	Section 9 -			able to inquire how many detections come	requirement.	corrigendum
'00	Technical		Annexure J - Technical	from malicious password-protected files		
1	Specifications	40	Compliance			

				The Proposed Sandboxing solution must	In Advanced Threat Landscape the	Refer to
				support of analysis of Windows & Linux	attacks are not limited to Windows &	corrigendum
				Operating System files	Linux environment only but MAC OS's	corrigendum
				operating system mes		
					and its applications are also targeted	
					with Zero-day attacks, attackers also	
					leverage Webshell attacks on Linux	
					servers, hence it is important that	
					sandboxing solution should have	
					Windows, Linux and MAC OS's for	
					conducting dynamic analysis on-	
					premises and create real-time threat	
					intelligence to block call	
					back/malicious communications with	
					C&C servers.	
189						
					We would like to know if NPCI wants	
					to detect and prevent attacks	
					targeted towards MAC and Linux	
					including Webshell injection attacks?	
					If yes, we request modification of the	
					clause to:	
					"The proposed Anti ADT colution	
					"The proposed Anti-APT solution	
					should include on-premises	
					sandboxing for dynamic analysis	
	Castian O				for Windows, Linux and MAC OS's	
	Section 9 -				without any additional	
	Technical		Annexure J - Technical		requirement of licenses form OS's	
	Specifications	41	Compliance		and Applications from NPCI."	
	C C			The proposed solution should support X-Dst-		Need more clarity
190	Section 9 -			Forwarded-For header, so that Network		
'''	Technical		Annexure J - Technical	Security alerts displays the correct destination		
	Specifications	41	Compliance	IP address		
ΙT				The proposed solution should provide alert		Need more clarity
191	Section 9 -			details with mapping to the MITRE ATT&CK		
'''	Technical		Annexure J - Technical	Framework to give more context for attack		
	Specifications	41	Compliance	investigation and allow easier triaging		
				SSL Capabilities	Does NPCI wants dedicated SSL	Refer to
					solution for Network Anti-APT or are	corrigendum
					looking for built-in SSL decryption	5
					capabilities in Network Anti-APT? as	
192					the requirement point/clause	
	Section 9 -				mentioned below are typically	
	Technical				available in dedicated SSL decryption	
	Specifications					
	specifications				solution.	

				Solution should inspect https traffic (Full Deep	Advanced attackers uses Webshell	Refer to
						corrigendum
1 1				Packet / SSL Traffic) and must provide	inject attacks to compromise Web	corrigendum
				decryption of unverified encrypted traffic for		
				scanning and then re encrypt it before sending		
					capabilities? If yes please confirm and	
1 1					amend/modify the same to the	
					requirement mentioned.	
					For Example the clause can be	
1 1					modified as:	
193					"The proposed solution should	
1 1					detect & prevent suspicious	
1 1					Webshell files uploaded to web	
1 1					servers through HTTP POST and	
1 1					FTP protocols and also provide	
1 1					mapping of methodology & alert	
1 1					techniques to MITRE ATT&CK	
1 1					framework. It should also detect	
1 1	Section 9 -				attempted data exfiltration &	
1 1	Technical		Annexure J - Technical		SSL/TLS handshake fingerprinting	
	Specifications	41	Compliance		at the minimum"	
	•		-	Integrate with any existing Proxy solution of	Please provide clarification on proxy	Should able to be
1 1	Section 9 -			NPCI.	and expectation on Integration with	deployed inline
194	Technical		Annexure J - Technical		Proxy.	with proxy solution.
	Specifications	41	Compliance		i i oxy.	with proxy solution.
				SSL functionality should be available on the	Duplicate to Point 93 which clearly	Refer to
1 1				proposed inline APT appliance	states that the Anti-APT should have	corrigendum
1 1					built-in SSL intercept capability	
1 1					which itself makes SSL inline to	
195					Network Anti-APT, unless NPCI is	
1 1					looking for dedicated SSL solution if	
1 1	Section 9 -				yes, we would than propose	
	Technical		Annexure J - Technical		dedicated SSL decryption appliance	
	Specifications	41	Compliance		inline to Anti-APT.	
				The solution must support TLS fingerprint	Very important point where Anti-APT	No change in RFP
				detection detects malicious communication by		
				TLS fingerprinting with JA3 between the	malicious communication by TLS	
				client and server.	Fingerprinting with JA3 inbetween	
196					Client and Server. If it is good to have	
	Section 9 -				in that case NPCI may miss this	
	Technical		Annexure J - Technical		capability provided by some of the	
	Specifications	41	Compliance		Anti-APT solutions.	
			- p	Ability to automatically intercept all SSL/TLS	Please Clarify on the clause, as TCP	Refer to
	Section 9 -			based flows, also on other ports and protocols	ports have to be defined manually to	corrigendum
197	Technical		Annexure J - Technical	(not only HTTPS)	automatically intercept SSL/TLS or	50.000
	Specifications	41	Compliance		HTTPS.	
	Section 9 -			Support multiple active-inline devices	Please provide more clarification	Refer to
198	Technical		Annexure J - Technical	simultaneously		corrigendum
	Specifications	41	Compliance			
					I	

				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				source/destination ip/port	interception solution, We request	-
199	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				host/URL categorization	interception solution, We request	5
200	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
\neg	•		·	Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
_				threat intelligence	interception solution, We request	.
201	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
	•		·	Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on CA	supported with dedicated SSL	corrigendum
				status	interception solution, We request	5
202					NPCI to confirm if they need	
	Section 9 -				dedicated SSL interception solution	
	Technical		Annexure J - Technical		to provide granular controls? Also	
	Specifications	41	Compliance		provide use case for the same	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				Subject / Domain Name	interception solution, We request	
203	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
~~ l				Cipher Suite and Key Strength	interception solution, We request	
204	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
				Support for Fail-to-wire/fail-to-open	Requirement depends on the port	Refer to
				hardware, traffic bypass filters (in the event	capability or external Active Failover	corrigendum
205	Section 9 -			of in-line security device failure) and	Kit is required, Please confirm of	
	Technical		Annexure J - Technical	configurable link state monitoring/mirroring?	NPCI needs external Bypass Kit to	
- 1	Specifications	41	Compliance		support the same?	

Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, SSL stands for Secure Socket Layer	Refer to
SSL3, and SSL2 encryption protocols? while TLS stands for Transport Layer	
	corrigendum
Security. Both Secure Socket Layer	
and Transport Layer Security are the	
protocols used to provide the security	
between web browser and web	
server.	
The main differences between Secure	
Socket Layer and Transport Layer	
Security is that. In SSL (Secure Socket	
Layer), Message digest is used to	
create master secret and It provides	
the basic security services which are	
Authentication and confidentiality.	
while In TLS (Transport Layer	
Security), Pseudo-random function is	
used to create master secret.	
1) SSL (Secure Socket Layer) is the	
3.0 version is equal to TLS	
(Transport Layer Security) is the 1.0	
version.	
2) In SSL(Secure Socket Layer),	
Message Authentication Code	
protocol is used while in	
TLS(Transport Layer Security),	
Specifications 41 Compliance 3) SSL (Secure Socket Layer) is less Support RSA, DHE, and ECDHE public key Duplicate as point 111 covers the	Refer to
algorithms? Ciphers in details which are more	corrigendum
207 Section 9 - Section 9 -	
5 Series - S	
Thence we request removal of point	
Specifications 42 Compliance 112 as duplicated.	
Support AES, 3DES, DES, RC4, and Camellia 3DES, DES, RC4 and Camellia are	Refer to
Section 9 - symmetric key algorithms? weak ciphers and hence in the	corrigendum
Denent of NPCI we request not to use	
Specifications 42 Compliance the same in your environment.	
Support MDS, SHA-1, and SHA-256 hash MD5 being a weak ciphers and can be	Refer to
algorithms? easily manipulated we recommend	corrigendum
209 not to use the same and should be	
209 Section 9 - removed from the clause as this	1
Technical Annexure J - Technical would compromise security.	

				Total Packet processing capacity of single	Conflicts with the requirement	Refer to
				device should be 1 Gbps	mentioned in point 1 which mentions	corrigendum
				device should be i dops	Hardware appliance should be able to	corrigendum
					handle 500Mbps in total.	
					In total traffic of 500Mbps if we	
					consider 40-50% https traffic it comes	
210					to around 200-250Mbps of HTTPS	
12.1					traffic.	
					Hence we request clarification on	
					actual requirement of HTTPS/SSL	
					decryption and encryption traffic	
	Section 9 -				capabilities on total 500Mbps traffic	
	Technical		Annexure J - Technical		mentioned in point 1.	
	Specifications	42	Compliance			
				Hardware should have minimum capacity of 1	For Network Anti-APT solution where	Refer to
				ТВ	the analysis has to done at wire speed	corrigendum
					on the traffic with aggressive packet	-
					capture, it is recommended that the	
					Network Anti-APT appliance should	
					have minimum 2 HDD with atleast	
					4TB of capacity to ensure the	
					analysis to complete in near real-	
					time.	
21						
					Hence in the benefit of NPCI which	
					falls in National critical infrastructure	
					should have minimum 2 x 4TB HDD	
					and request amendment to the clause	
					to:	
					"Hardware should have minimum 2	
	Section 9 -				HDD with atleast 4TB of capacity	
	Technical		Annexure J - Technical		with atteast 416 of capacity	
		37				
	Specifications	37	Compliance			

		- 1		The proposed solution must be available as on	NPCI being an National Critical	Refer to
					Infrastructure of India where	corrigendum
				premise physical appliances with sandboxing	1	corrigendum
				capability	information is very sensitive it is	
					recommended to have complete	
					analysis to be performed by the	
					Network Anti-APT on premises. The	
					overall solution architecture should	
					be such that the complete sandboxing	
					must be performed on-premises & no	
					objects/files should be sent to the	
					vendor cloud as they may contain	
					either confidential data or Personally	
					identifiable information (PII) Data.	
					We would like to bring it to NPCI	
212					notice that as the clause does not	
					state complete sandboxing	
					environment on premises including	
					various operating systems &	
					applications like Windows OS & its	
					applications, Linux OS & its	
					applications & MAC OS & its	
					applications in absence of this being	
					stated NPCI would not be able to	
					control the file/objects submissions	
					to on-premises sandbox only. This	
					may lead to vendors submiting the	
	Section 9 -				files to the cloud without NPCI's	
	Technical		Annexure J - Technical		knowledge.	
	Specifications	37	Compliance			
				Proposed APT solution should perform	Clarification required, Should we	No change in RFP.
				advanced network detection and analysis of	read the clause as?	Should able to
				the enterprise's internal/External network		perform detection
213				data.	"Proposed APT solution should	on Intenal (east-
					perform advanced network	west), External
	Section 9 -				detection and analysis of the	(inbound-outbound)
	Technical		Annexure J - Technical		enterprise's inbound/outbound	traffic.
	Specifications	37	Compliance		network traffic."	

				The proposed solution should support to	As per clause number 1 of the	Refer to
				monitor traffic from multiple segments	Technical Specifications the Network	corrigendum
				simultaneously on single appliance (East-West,	· · ·	corrigendum
				North-South).	handle 500Mbps of total traffic. In	
					any organization where North-South	
					(Internet Traffic) is typically based on	
					total internet bandwidth and is same	
					or less than the total internet	
					bandwidth, but East-West traffic	
					(Intranet Traffic) i.e. from	
					LAN/Client segment to Server	
					segment the traffic may be huge	
					somewhere around 1Gbps to 4Gbps as	
					it is internal traffic, this would	
214					exceed 500Mbps appliance capacity	
214					anytime. Also North-South and East-	
					West segments are completely	
					different and may pass through	
					different Core Switches and may not	
					be feasible at times for connectivity.	
					Hence we would request NPCI to	
					please share North-South traffic	
					detail in Mbps/Gbps and East-West	
					traffic in Mbps/Gbps to ensure all the	
					traffic is covered by Network Anti-	
					APT solutions and also confirm if	
	Section 9 -				connectivity for North-South traffic	
	Technical		Annexure J - Technical		and East-West traffic is feasible or	
	Specifications	37	Compliance		not.	
	Specifications		compliance	The proposed solution should be dedicated	Similar to point 11 which is in more	Refer to
				appliance and should not be enabled as	details, hence we request NPCI to	corrigendum
215	Section 9 -			additional licensed solution with proposed	remove this point as duplicate.	corrigendum
215	Technical		Annexure J - Technical	perimeter gateway devices such as firewall,	i eniove unis point as dupticate.	
	Specifications	37	Compliance	APT etc.		
	pecifications	57	compliance	JAFT ELC.		1

				Security Vendor must have a Research/Labs	Reporting on Vulnerabilities is	Refer to
					primary function of Vulnerability	corrigendum
				contribute and report on finding new Zero-Day	Assessment tools / Solution.	
				vulnerabilities being exploited in the wild.		
					As a Network Anti-APT solution the	
					primary & most important function is	
					to prevent Zero-Day exploits in the	
					wild from targeting the	
					vulnerabilities. Also in real world, the	
					zero day explots may not available at	
					the same time when the actual	
					vulnerabilitiv is identified, hence it is	
					important to detect & prevent zero	
					day expliots / payloads.	
216						
					Hence to benefit from the Network	
					Anti-APT we request NPCI to modify	
					this clause as:	
					"Security Vendor must have a	
					Research/Labs organization and this	
					organization must contribute and	
					report on finding new Zero-Day	
					expliots being identified / discovered in the wild & should	
	Section 9 -					
	Technical		Annexure J - Technical		automatically share the intel to the	
		37			Network Anti-APT Solution".	
	Specifications	37	Compliance			

				L		
				The proposed solution should be able to	Need for clarification on this point	Refer to
				detect any suspicious communication within	specifically Outside of Customers	corrigendum
				and outside of Customer's network	Network as it typically false in the	
					requirement of perimeter solutions	
					like Firewall / IPS.	
					With regards to within the network	
					suspicious communications would	
					NPCI like to detect malicious post-	
					exploitation activities such as	
					attacker lateral movements between	
					user workstation & servers? as	
					Attackers frequently use SMB & SMB2	
					to carry their activity from	
					compromised endpoints and move to	
217					servers, hiding their activities in	
					normal traffic.	
					normat trainc.	
					If Yes, we would recommend NPCI to	
					modify the clause to:	
					"The proposed network Anti-APT	
					solution should also be able to	
					detect malicious post-exploitation	
					activities such as attacker lateral	
					movements between user	
					workstation & Servers. Attackers	
					frequently use SMB & SMB2 to	
	Section 9 -				carry their activity from	
	Technical		Annexure J - Technical		compromised endpoints and move	
	Specifications	37	Compliance		to servers, hiding their activities	
				The Proposed solution should be able to	We would like to highlight this	Refer to
				detect communications to known command	requirement only mentions detection	corrigendum
				and control centers.	of known Command and Control	
					Centers (C&C) only and not blocking	
					of the C&C as well it do not covers	
					unknown C&C detection and blocking.	
					Hence in the benefit of NPCI we	
					request the clause to be changed to:	
218					,	
					"The Proposed solution should be	
					able to detect communications to	
					known & unknown command and	
					control center initiated by internal	
					infected clients."	
	Section 9 -					
	Technical		Annexure J - Technical			
	Specifications	37	Compliance			

				The proposed solution should be able to	Primarily this requirement falls in the	Refer to
				detect reputation of URL being accessed	category of Proxy Solution	corrigendum
				detect reputation of one being accessed	requirement where reputation of the	conigendum
					URL plays a very important role,	
					however in Network Anti-APT the	
					analysis is not limited to just URL	
					reputation but it should be able to	
					analyze complete URL's in zero-trust	
21	9				manner as attackers take advantage	
					of the URL reputation check tools to	
					launch sophisticated attacks and	
					compromise the Host/End-user.	
					compromise the nose, End user.	
	Section 9 -				Hence we recommend to remove or	
	Technical		Annexure J - Technical		modify the clause.	
	Specifications	37	Compliance			
				The proposed solution should support at least	In an Advanced Attack threat actors	Refer to
				100+ protocols for inspection	leverage C&C communication to	corrigendum
					command & control the victim	-
					machine, hence it is important for an	
					organization to block all malicious	
					C&C communications regardless of	
					ports and protocols, hence we	
22					request NPCI to change the clause to:	
					"The proposed solution for Network	
					Ani-APT should prevent any C&C	
					communications detected over North-	
	Section 9 -				South traffic regardless of ports and	
	Technical		Annexure J - Technical		protocols"	
	Specifications	38	Compliance			

				Sandbox must have the ability to simulate the	There are various flavors of Sandbox	Refer to
				entire threat behavior.	environment used for analysis and	corrigendum
					not limited to just Windows OS but	g
					also Linux, MAC OS with 32bit and	
					64bit architecture and various types	
					of applications targeted in the wild.	
					, FF 5	
					Hence in the benefit of NPCI we	
					request the clause to be very specific	
					like:	
					"The proposed solution must be	
221					available as on premise physical	
					appliances with sandboxing	
					capability and must be able to	
					detect and report malware by	
					using multiple client environments	
					(operating systems with multiple	
					service pack levels) supporting	
					both x64 and x86 architectures	
					including Windows, Mac, CentOS	
	Section 9 -				based on premise Virtual Execution	
	Technical	20	Annexure J - Technical		Environment"	
	Specifications	38	Compliance			
					OEM Specific Clause.	Refer to
				document vulnerabilities detection engine to		corrigendum
					We request removal of the clause as	
222	Section 0			efficiency	the requirement gets addressed in	
	Section 9 -		Annexure J - Technical		detection of Zero-Day exploits	
	Technical Specifications	20			targeting vulnerabilities in the wild in	
	Specifications	38	Compliance		clause 19 and 20.	

				T		
				The proposed solution should support Multiple	Advanced attackers once establish	Refer to
				protocols for inspection. Example:- HTTP,	the foothold tries to move laterally	corrigendum
					and dump sophisticated tools on	
				protocols Internal direction: SMB ,Database	various systems connected in the	
				protocol (MySQL, MSSQL, Oracle) on a single	network detecting this tools and	
				device	identifying this tools and techniques	
					plays a very important and critical	
					role in early detection and incident	
					response.	
					Hence in the benefit of NPCI it is	
					important to get visibility of such	
					activities of the threat for which we	
					request modification of the clause to	
223					below:	
					"The proposed solution should be	
					able to detect the activities of	
					attackers already resident in the	
					network core. The solution should	
					extracts malware and objects that	
					are transferred over HTTP, FTP &	
					other protocols and submit them to	
					the automated dynamic Analysis	
					engine for detonation and	
					confirmation on maliciousness. The	
					solution should extracts malware	
	Section 9 -				and objects that are transferred	
	Technical		Annexure J - Technical		over HTTP, FTP like protocols and	
	Specifications	38	Compliance		submit them to an automated	
	specifications	50	comptiance	The Proposed solution should have a Co-	Duplicate point as all the previous	Refer to
	Section 9 -			_ ·	clause covers the same.	
224	Technical		Annexure J - Technical			corrigendum
	Specifications	38	Compliance	across multiple protocol, multiple sessions and	Request removal of the clause.	
	specifications	20	compliance	volume traffic analysis		

				The proposed solution should be able to	Advanced attackers leverage various	Refer to
				detect and prevent the persistent threats	types of files to infiltrate in the	corrigendum
				which come through executable files, PDF	target environment and not just	
				files , Flash files, RTF files and and/or other	executables, pdf, flash or RTF file	
				objects.	types hence it is very important that	
					dynamic analysis engine should be	
					able to analyze different filetypes	
					without depending on the signatures.	
					Hence for critical infrastructure like	
					NPCI should ensure that various	
					filetypes which are leveraged by the	
					advanced attackers should be	
					dynamically analyzed without	
0.00					depending upon the signatures alone,	
225					in the benefit of NPCI we request	
					modification of this clause as follows:	
					"The proposed solution should have	
					the ability to analyze, detect and	
					block malware in common file	
					formats including but not limited	
					to executables, JAVA, PDF, MS	
					Office documents, common	
					multimedia contents such as JPEG,	
					QuickTime, MP3 and	
					ZIP/RAR/7ZIP/TNEF archives, 3gp,	
	Section 9 -				asf, chm, com, dll, doc, docx, exe,	
	Technical		Annexure J - Technical		gif, hip, htm, ico, jar, jpeg, jpg,	
	Specifications	38	Compliance		mov, mps, mp4, pdf, png, ppsx,	

				The Proposed solution should be able to	In a sophisticated attack the	Refer to
				generate out of box reports to highlight	advanced attackers may or may not	corrigendum
				Infections, C&C behavior, Lateral Moment,	use malware, but they definitely use	conngentaum
				Asset and data discovery and Exfiltration	various techniques & methodologies	
				Asset and data discovery and Exiteration	to move laterally, hence it is	
					important for a solution to detect	
					TTP's and methodologies and alert	
					-	
					with timeline & date sliders with at least 5 minutes of relevant network	
					activity data(layer 4-7) before and	
					after the attack.	
					Hence in the benefit of NPCI we	
					request modification of this clause	
					with must have capabilities as:	
226						
					Proposed Internal Network APT	
					should detects the following types of	
					malicious post-infection activities:	
					a) Internal Reconnaissance	
					b) Privilege Escalation	
					c) Credentials Dumping	
					d) Lateral Movement of Malware	
					e) Remote Task Execution	
					f) Data Exfiltration Detection	
					g) Callback activities	
					h) Bot-tracker features like File	
	Section 9 -				inspection, Packet flows, Signature	
	Technical		Annexure J - Technical		matching and statistics	
	Specifications	38	Compliance		i) Supports extensive metadata	
				The proposed APT must able to operate in	Analyzing asymmetric traffic results	Refer to
				Asymmetric traffic environment with	in ton's of false positive's and adds	corrigendum
				Vulnerability / Exploit filters for protection	unnecessary workload on validation	
					of such all the alerts resulting in Alert	
227					Fatigue on SOC team, hence we	
					request removal of such clause which	
	Section 9 -				adds overheads to security team and	
	Technical		Annexure J - Technical		miss on legitimate threats.	
	Specifications	38	Compliance			
	Section 9 -			The proposed APT solution must support	OEM Specific IPS Solution, Request	Refer to
228	Technical		Annexure J - Technical	Adaptive Filter Configuration(AFC) which will	removal of this clause.	corrigendum
	Specifications	38	Compliance	alert or disable ineffective filter in case of		
$\left - \right $	specifications	50	Compliance	noisy filters The APT filter must support network action	Duplicate Clause, Point 17 covers the	Refer to
				set such as Block (drop packet), Block (TCP	requirement hence we request	corrigendum
				Reset), Permit, Trust, Notify, Trace(Packet	removal of this clause.	
				Capture), Rate Limit and Quarantine		
1 1					Also it is important for Anti-APT	
229						
229						
229	Section 9 -				solution to Block callback to C&C and	
229	Section 9 - Technical		Annexure J - Technical			

				The proposed APT solution must support	Clause is OEM Specific IPS Solution	Refer to
				signatures, vulnerabilities and traffic filtering	which heavily depends upon signature	corrigendum
230	Section 9 -			methods to detect attacks and malicious	based detection.	configendam
	Technical		Annexure J - Technical	traffic		
	Specifications	38	Compliance	tante	We request removal of this clause	
			·	The APT filters must be categories into the	Clause is OEM Specific IPS Solution,	Refer to
				following categories for easy management:	Request removal of this clause.	corrigendum
				Exploits, Identity Theft/Phishing,		•
231	Section 9 -			Reconnaissance, Security Policy, Spyware,		
	Technical		Annexure J - Technical	virus, Vulnerabilities, Traffic		
	Specifications	38	Compliance	Normalization, P2P, IM, Streaming Media		
				Vulnerability based filter are known for most	Clause is OEM Specific IPS Solution &	Refer to
222	Section 9 -			effectively for Zero Day Attack Protection and	only covers known attacks, Request	corrigendum
232	Technical		Annexure J - Technical	proposed solution must support vulnerability	removal of this clause.	
	Specifications	39	Compliance	based filter		
	Section 9 -			The proposed APT should support the ability	Clause is OEM Specific IPS Solution,	Refer to
233	Technical		Annexure J - Technical	to mitigate Denial of Service (DoS/DDoS)	Request removal of this clause.	corrigendum
	Specifications	39	Compliance	attacks such as SYN floods	-	-
	Section 9 -			The proposed APT must provide bandwidth	Clause is OEM Specific IPS Solution,	Refer to
234	Technical		Annexure J - Technical	rate limit to control the unwanted/nuisance	Request removal of this clause.	corrigendum
	Specifications	39	Compliance	traffic such as P2P, Online Game, etc.,		
				The proposed APT must be able to use	Clause is OEM Specific IPS Solution &	Refer to
				Reputation Service such as IP address or DNS	only covers known attacks, Request	corrigendum
235	Section 9 -			to block traffic from or to 'known bad host'	removal of this clause.	
	Technical		Annexure J - Technical	such as spyware, phishing or Botnet C&C		
	Specifications	39	Compliance			
				The proposed APT must be able to control the	Clause is OEM Specific IPS Solution &	Refer to
				known bad host such as spyware, botnet C2	only covers known attacks, Request	corrigendum
236	Section 9 -			server, spam and so on based on country of	removal of this clause.	
	Technical			origin, exploit type and the reputation score		
	Specifications	39	Compliance			
				Must have the ability to correlate the	The clause adds lot of dependency on	Refer to
				monitored attacks to the APT filters number	the security teams to continuously	corrigendum
				and recommended action	monitor and keep on modifying	
					policies increasing overheads and	
					false positives, Anti-APT solution	
					should be able to take decision with	
237					its intelligence with simple	
					configuration to Block or Monitor the	
					threat.	
	Section 9 -				Hence in the benefit of the NPCI we	
	Technical		Annexure J - Technical		request modification/removal of this	
	Specifications	39	Compliance		clause	

						I
				NG APT engine must be a smart enough to	Detecting traffic based on suspicion	Refer to
				inspect the traffic based on condition, If the	or deep packet inspection needs	corrigendum
				traffic is suspicious then it goes for the deep	patterns / signatures to take	
				packet inspection	decisions, Anti-APT solution should	
238					not just depend upon signatures but	
250					it should have dynamic analysis	
					engine with signatureless detection	
	Section 9 -				and should create signatures in	
	Technical		Annexure J - Technical		Realtime and block the threats inline.	
	Specifications	39	Compliance			
				The proposed management system shall allow	Please correct our understanding	To be Integrated
				the update of global threat intelligence via	about local threat intelligence	with our TIP
				cloud and local Threat intelligence updates	sharing. Do you mean sharing	platform for threat
239				from proposed Network threat detection	intelligence from your existing Anti-	intelligence
	Section 9 -			solution automatically for inline blocking	APT solutions from Email & content	integration with
	Technical		Annexure J - Technical	, , , , , , , , , , , , , , , , , , , ,	scanning Anti-APT solutions to Anti-	other solutions
	Specifications	39	Compliance		APT for Network Security?	deployed.
	•		·	The management server must provide rich	Rate Limiting, Misuse & Abuse,	Refer to
				reporting capabilities include report for All	Traffic Threshold & DDoS reports do	corrigendum
				attacks, Specific & Top N attack, Source,	not fall in Anti-APT solution, these	J. J
240				Destination, Misuse and Abuse report, Rate	are OEM specific and hence request	
	Section 9 -			limiting report, Traffic Threshold report,	NPCI to remove the same.	
	Technical		Annexure J - Technical	Device Traffic Statistics and Advance DDoS		
	Specifications	39	Compliance	report		
	•		•	The proposed management system must be	Critical infrastructure like NPCI may	Refer to
				able to support the syslog CEF format that	have various tools for event	corrigendum
				SIEM can support	correlation, automation,	g
					orchestrations etc limiting to CEF	
					format only may limit integration	
					with other tools and result no	
					integration support. Hence we	
					request NPCI to modify the clause to	
					various types of log/event format but	
					not limited to CEF only.	
					not timited to cer onty.	
241					Clause Modification to:	
					clause mounication to.	
					The proposed management system	
					must be able to support Common	
					Event Format (CEF), Log Event	
					Enhanced Format (LEEF), Comma-	
					Separated Values (CSV), XML,	
	Section 9 -				JSON, or Text format that SIEM	
	Technical		Annexure J - Technical		and other tools like automation	
	Specifications	39	Compliance		and orchestration can support.	
	specifications	37	compliance			

242	Section 9 -			The proposed management system shall have a big data engine that allows customers to provide faster security analytics and faster report generation	To integrate with Big Data Analytics the solution should support file formats that can be ingested in the Big Data Analytics tool, hence we request NPCI to modify the clause and not mandate with Big Data Engine which makes the clause to OEM Specific. Request modification in clause to: "The Management system should support file formats which can be ingested in Big Data Analytics	Refer to corrigendum
	Technical	40	Annexure J - Technical		Solution for faster report	
\vdash	Specifications	40	Compliance	Automatic detection and response against an	generation." This clause of Automatic detection	Refer to
				ever-growing variety of threats, including fileless and ransomware	and response requirement do not covers automatic prevention and integration with various other vectors of attack like Email, Endpoint EDR and File/content uploads from outside to respond to threats. In any enterprise organizations and critical infrastructure resilience defense strategy plays a very important role to defend against the	corrigendum
243					advanced attack and hence should be in a Must Have category instead of Good to Have. Does NPCI wants to take benefit of	
					Anti-APT for network security solution requirement with	
					automatic prevention and integration with various vectors of	
					attack capabilities and not just detection and response? If yes we	
					request modification of the clause	
					to:	
					"The solution must have automatic detection, prevention, remediation	
	Section 9 - Technical		Annexure J - Technical		and integration capabilities with	
	Specifications	40	Compliance		various attack vectors not limited	
244	Section 9 - Technical		Annexure J - Technical	The industry's most timely virtual patching: Vulnerability Protection virtually patches known and unknown vulnerabilities, giving you	Clause is OEM Specific IPS Solution, Request removal of this clause.	Refer to corrigendum
	Specifications	40	Compliance	instant protection, before a patch is available or deployable.		

				The colution should consolidate (at	To support Advanced Defense	Okay, No change in
				The solution should consolidate (at	Strategy and build advanced	RFP.
				centralized location) the administration,	resilience infrastructure for NPCI it's	KFP.
245	Section 9 -			reporting, and intelligence data sharing		
	Technical		Annexure J - Technical	intelligence/IOC's between deployed Anti-APT	important clause.	
		40		Sensors/ solution at our organization (Email		
	Specifications	40	Compliance	Analysis, File Analysis & EDR)		
				Central Management should provide option to	To support Advanced Defense	No change in RFP
				create customized lists of IOCs received from	Strategy and build advanced	
				these feeds and use them as a custom	resilience infrastructure for NPCI it's	
				blacklist on the Central Management	important clause.	
246				appliance. The types of IOCs like URL		
				indicators, IP address indicators, domain		
				indicators, and indicators with hashes of		
	Section 9 -			malicious files, combine them into a standard		
	Technical		Annexure J - Technical	format called STIX (Structured Threat		
	Specifications	40	Compliance	Information Expression)		
				Centralized Sandboxing	OEM specific clause, some of the	No change in RFP.
					OEM's provide Built-in Sandboxing	Prefer to have built
247					solution and do not require any	in sandboxing
24/	Section 9 -				additional/external Sandboxing	capabilities for
	Technical				solution. Hence we request NPCI to	Network Anti-APT
	Specifications				consider the same.	solutions.
				The proposed solution should be able to run at	Different OEM's have different	Refer to
				least 50 parallel sandboxes for analysis of	methods and technology to run	corrigendum
				payload and on premise customized sandbox	dynamic analysis and should not	
				solution should have the capability to allow	mandate on 50 parallel sandboxes	
				manual submission of suspicious files for	instead it is important to have	
				analysis	multiple executions to run in parallel	
					for payload analysis automatically	
					and not manually.	
					Some of the OEM who have	
					NO\limited number of Sandboxes built	
248					in depend upon external sandboxes	
					which supports manual submission of	
					files, hence we request for	
					modification of the clause to:	
					"The solution should support 1000+	
					executions to analyze the payloads in	
					parallel depending on the	
					performance capacity upto 500Mbps	
	Section 9 -				of the appliance deployed on-	
	Technical		Annexure J - Technical		premises"	
	Specifications	40	Compliance		P. 5	

				Sandboxing Appliance should support	Not applicable for built-in sandboxing	No change in RFP.
				Active/Passive or Active-Active deployment	solution hence we request	
				and should support configuring cluster for	modification of the clause to:	"The Network Anti-
				High Availability		APT solution should
249					"The Network Anti-APT solution	support Active-
					should support Active/Passive or	Active, Active-
	Section 9 -				Active passive deployment on-	Passive
	Technical		Annexure J - Technical		premises"	deployment on-
	Specifications	40	Compliance		ľ	premises".
				The proposed solution must be capable of	Advanced attackers leverage various	Refer to
				analysis of different file types, including	types of files to infiltrate in the	corrigendum
				portable executables (PEs), web content, Web	target environment especially	•
				objects, images, Java, network flows,	Webshell attacks on Web Servers and	
					manipulate the server and redirect to	
					malicious content.	
				multimedia etc. including all such file types		
					Hence for critical infrastructure like	
					NPCI should ensure that various	
				channel, for initial compromise or backdoor or		
					advanced attackers should be	
					dynamically analyzed without	
					depending upon the signatures alone,	
					in the benefit of NPCI we request	
					modification of this clause as follows:	
250					inouncation of this clause as follows.	
					"Solution should provide	
					comprehensive support for user	
					interaction framework for web	
					shells, support for shell scripts	
					(e.g.; python, Perl, and Ruby etc.),	
					support for ELF binaries, Server-	
					side attack detection, complete	
					user mode and kernel mode	
					monitoring from within and outside	
					the Guest Images, Web shell	
					• •	
	Section 9 -				detection support for JSP, PHP,	
	Technical		Annexure J - Technical		and WAR (Web archive) file types	
	Specifications	40	Compliance		etc."	
	specifications	-U	compliance			

				Sandbox appliance should have redundant	For Network Anti-APT solution where	Refer to
				power supply, 2 TB or more storage capacity	the analysis has to done at wire speed	corrigendum
				with dedicated management port	on the traffic with aggressive packet	
					capture, it is recommended that the	
					Network Anti-APT appliance should	
					have minimum 2 HDD with atleast	
					4TB of capacity to ensure the	
					analysis to complete in near real-	
251					time.	
					Hence in the benefit of NPCI which	
					falls in National critical infrastructure	
					should have minimum $2 \times 4TB HDD$	
					and request amendment to the clause	
	Section 9 -				to:	
	Technical		Annexure J - Technical		"Hardware should have minimum 2	
	Specifications	40	Compliance		HDD with atleast 4TB of capacity	
	Section 9 -		•	The Proposed Solution should be able to	Does NPCI only wants to detect	Refer to
252	Technical		Annexure J - Technical	detect known bad URL before sandboxing	known bad URL's only?	corrigendum
	Specifications	40	Compliance			
				The proposed solution should detect file-less	Attackers use encoded algorithms like	Refer to
				malware tools used for extracting plain text	XOR to hide password instead of plain	corrigendum
				passwords, hash, PIN codes and Kerberos	text, do NPCI would like to detect	
				tickets.	and extract passwords which are	
					encoded algorithm XOR instead of	
					just plain text? If yes,	
253					We request you to modify the clause	
					to:	
					"The proposed solution should	
					detect file-less malwares tools	
	Section 9 -				used for extracting	
	Technical		Annexure J - Technical		encoded/XOR'ed as well as plain	
	Specifications	40	Compliance		text passwords, hash, PIN codes	
\vdash	specifications	40	compliance		etc"	Defente
	Section 9 -			The Proposed solution should allow Admin be	Please provide clarification on the	Refer to
254	Technical		Annexure J - Technical	able to inquire how many detections come	requirement.	corrigendum
	Specifications	40	Compliance	from malicious password-protected files		
i I	specifications	40	compliance			

				The Proposed Sandboxing solution must	In Advanced Threat Landscape the	Refer to
				support of analysis of Windows & Linux	attacks are not limited to Windows &	corrigendum
				Operating System files	Linux environment only but MAC OS's	corrigendum
				operating system mes	and its applications are also targeted	
					with Zero-day attacks, attackers also	
					leverage Webshell attacks on Linux	
					servers, hence it is important that	
					sandboxing solution should have	
					Windows, Linux and MAC OS's for	
					conducting dynamic analysis on-	
					premises and create real-time threat	
					intelligence to block call	
					back/malicious communications with	
255					C&C servers.	
255					We would like to know if NPCI wants	
					to detect and prevent attacks	
					targeted towards MAC and Linux	
					including Webshell injection attacks?	
					If yes, we request modification of the	
					clause to:	
					clause to.	
					"The proposed Anti-APT solution	
					should include on-premises	
					sandboxing for dynamic analysis	
					for Windows, Linux and MAC OS's	
	Section 9 -				without any additional	
	Technical		Annexure J - Technical		requirement of licenses form OS's	
	Specifications	41	Compliance		and Applications from NPCI."	
ΙĪ	Castian 0			The proposed solution should support X-Dst-		Need more clarity
256	Section 9 -			Forwarded-For header, so that Network		
]	Technical		Annexure J - Technical	Security alerts displays the correct destination		
	Specifications	41	Compliance	IP address		
	Continue O			The proposed solution should provide alert		Need more clarity
257	Section 9 -			details with mapping to the MITRE ATT&CK		
	Technical		Annexure J - Technical	Framework to give more context for attack		
\vdash	Specifications	41	Compliance	investigation and allow easier triaging		
				SSL Capabilities	Does NPCI wants dedicated SSL	Refer to
					solution for Network Anti-APT or are	corrigendum
					looking for built-in SSL decryption	
258					capabilities in Network Anti-APT? as	
	c c				the requirement point/clause	
	Section 9 -				mentioned below are typically	
	Technical				available in dedicated SSL decryption	
	Specifications				solution.	

				Solution should inspect https traffic (Full Deep	Advanced attackers uses Webshell	Refer to
				Packet / SSL Traffic) and must provide	inject attacks to compromise Web	corrigendum
				· ·		corrigendum
					Servers, would NPCI like to also have	
				scanning and then re encrypt it before sending		
					capabilities? If yes please confirm and	
					amend/modify the same to the	
					requirement mentioned.	
					For Example the clause can be	
					modified as:	
259					"The proposed solution should	
					detect & prevent suspicious	
					Webshell files uploaded to web	
					servers through HTTP POST and	
					FTP protocols and also provide	
					mapping of methodology & alert	
					techniques to MITRE ATT&CK	
					framework. It should also detect	
	Section 9 -				, attempted data exfiltration &	
	Technical		Annexure J - Technical		SSL/TLS handshake fingerprinting	
	Specifications	41	Compliance		at the minimum"	
			•	Integrate with any existing Proxy solution of	Please provide clarification on proxy	Should able to be
	Section 9 -			NPCI.	and expectation on Integration with	deployed inline
260	Technical		Annexure J - Technical		Proxy.	with proxy solution.
	Specifications	41	Compliance			
				SSL functionality should be available on the	Duplicate to Point 93 which clearly	Refer to
				proposed inline APT appliance	states that the Anti-APT should have	corrigendum
					built-in SSL intercept capability	
					which itself makes SSL inline to	
261					Network Anti-APT, unless NPCI is	
					looking for dedicated SSL solution if	
	Section 9 -				yes, we would than propose	
	Technical		Annexure J - Technical		dedicated SSL decryption appliance	
	Specifications	41	Compliance		inline to Anti-APT.	
				The solution must support TLS fingerprint	Very important point where Anti-APT	No change in RFP
				detection detects malicious communication by		
				TLS fingerprinting with JA3 between the	malicious communication by TLS	
				client and server.	Fingerprinting with JA3 inbetween	
262					Client and Server. If it is good to have	
	Section 9 -				in that case NPCI may miss this	
	Technical		Annexure J - Technical		capability provided by some of the	
	Specifications	41	Compliance		Anti-APT solutions.	
				Ability to automatically intercept all SSL/TLS	Please Clarify on the clause, as TCP	Refer to
	Section 9 -			based flows, also on other ports and protocols	ports have to be defined manually to	corrigendum
263	Technical		Annexure J - Technical	(not only HTTPS)	automatically intercept SSL/TLS or	con general
	Specifications	41	Compliance		HTTPS.	
	Section 9 -			Support multiple active-inline devices	Please provide more clarification	Refer to
264	Technical		Annexure J - Technical	simultaneously		corrigendum
	Specifications	41	Compliance	Sindedicousty		conigendum
\square	speenreacions		estuptionee	1		

Т				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
265				source/destination ip/port	interception solution, We request	
200	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				host/URL categorization	interception solution, We request	
66	Section 9 -			-	NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
\neg				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				threat intelligence	interception solution, We request	
67	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on CA	supported with dedicated SSL	corrigendum
				status	interception solution, We request	5
68					NPCI to confirm if they need	
	Section 9 -				dedicated SSL interception solution	
	Technical		Annexure J - Technical		to provide granular controls? Also	
	Specifications	41	Compliance		provide use case for the same	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				Subject / Domain Name	interception solution, We request	
69	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
				Ability to configure encryption/decryption	These requirements can only be	Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL	corrigendum
				Cipher Suite and Key Strength	interception solution, We request	
70	Section 9 -				NPCI to confirm if they need	
	Technical		Annexure J - Technical		dedicated SSL interception solution	
	Specifications	41	Compliance		to provide granular controls?	
				Support for Fail-to-wire/fail-to-open	Requirement depends on the port	Refer to
				hardware, traffic bypass filters (in the event	capability or external Active Failover	corrigendum
271	Section 9 -			of in-line security device failure) and	Kit is required, Please confirm of	
	Technical		Annexure J - Technical	configurable link state monitoring/mirroring?	NPCI needs external Bypass Kit to	
	Specifications	41	Compliance		support the same?	
—		I				
----------	----------------	----------	------------------------	---	---	-------------
1 1				Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3,	SSL stands for Secure Socket Layer	Refer to
1 1				SSL3, and SSL2 encryption protocols?	while TLS stands for Transport Layer	corrigendum
1 1					Security. Both Secure Socket Layer	
					and Transport Layer Security are the	
					protocols used to provide the security	
					between web browser and web	
1 1					server.	
1 1						
1 1					The main differences between Secure	
1 1					Socket Layer and Transport Layer	
1 1					Security is that. In SSL (Secure Socket	
1 1					Layer), Message digest is used to	
1 1					create master secret and It provides	
1 1						
1 1					the basic security services which are	
272					Authentication and confidentiality.	
					while In TLS (Transport Layer	
1 1					Security), Pseudo-random function is	
1 1					used to create master secret.	
1 1						
1 1					1) SSL (Secure Socket Layer) is the	
1 1					3.0 version is equal to TLS	
1 1					(Transport Layer Security) is the 1.0	
1 1					version.	
1 1					2) In SSL(Secure Socket Layer),	
1 1					Message Authentication Code	
1 1					protocol is used while in	
1 1					TLS(Transport Layer Security),	
1 1	Section 9 -				Hashed Message Authentication	
1 1	Technical		Annexure J - Technical		Code protocol is used.	
1 1		44			3) SSL (Secure Socket Layer) is less	
\vdash	Specifications	41	Compliance			
				Support RSA, DHE, and ECDHE public key	Duplicate as point 111 covers the	Refer to
				algorithms?	Ciphers in details which are more	corrigendum
273					precise than point 112 which is very	
	Section 9 -				generic.	
	Technical		Annexure J - Technical		Hence we request removal of point	
	Specifications	42	Compliance		112 as duplicated.	
				Support AES, 3DES, DES, RC4, and Camellia	3DES, DES, RC4 and Camellia are	Refer to
274	Section 9 -			symmetric key algorithms?	weak ciphers and hence in the	corrigendum
2/4	Technical		Annexure J - Technical		benefit of NPCI we request not to use	
	Specifications	42	Compliance		the same in your environment.	
				Support MDS, SHA-1, and SHA-256 hash	MD5 being a weak ciphers and can be	Refer to
				algorithms?	easily manipulated we recommend	corrigendum
					not to use the same and should be	
275	Section 9 -				removed from the clause as this	
	Technical		Annexure J - Technical		would compromise security.	
	Specifications	42	Compliance		would compromise security.	
	specifications	44	compliance			

27	Section 9 - Technical Specifications	42	Annexure J - Technical Compliance	Total Packet processing capacity of single device should be 1 Gbps	Conflicts with the requirement mentioned in point 1 which mentions Hardware appliance should be able to handle 500Mbps in total. In total traffic of 500Mbps if we consider 40-50% https traffic it comes to around 200-250Mbps of HTTPS traffic. Hence we request clarification on actual requirement of HTTPS/SSL decryption and encryption traffic capabilities on total 500Mbps traffic mentioned in point 1.	Refer to corrigendum
27	Section 7 Bid Evaluation	21	7.3 Technical Scoring Matrix:	Customer BFSI reference in India (Bidder & OEM) Please provide at least 2 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	Request Department to amend this caluse as - Customer BFSI reference in India (Bidder / OEM) Please provide at least 2 India References including a. Customer name b. Industry (Manufacturing, Insurance, financial, etc.) c. Size d. How long have they been consuming service? e. Contact name, title, email and direct telephone number	No change in RFP. Bidder should have experience of implementing network APT solution in at least 2 BFSI companies.
27	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	Hardware should have minimum capacity of 1 TB	For Network Anti-APT solution where the analysis has to done at wire speed on the traffic with aggressive packet capture, it is recommended that the Network Anti-APT appliance should have minimum 2 HDD with atleast 4TB of capacity to ensure the analysis to complete in near real- time. Hence in the benefit of NPCI which falls in National critical infrastructure should have minimum 2 x 4TB HDD and request amendment to the clause to: "Hardware should have minimum 2 HDD with atleast 4TB of capacity	Refer to corrigendum

					5	Refer to
				premise physical appliances with sandboxing	Infrastructure of India where	corrigendum
				capability	information is very sensitive it is	
					recommended to have complete	
					analysis to be performed by the	
					Network Anti-APT on premises. The	
					overall solution architecture should	
					be such that the complete sandboxing	
					must be performed on-premises & no	
					objects/files should be sent to the	
					vendor cloud as they may contain	
					either confidential data or Personally	
					identifiable information (PII) Data.	
	Section 9 -		Annexure J - Technical		We would like to bring it to NPCI	
27	9 Technical	37	Compliance		notice that as the clause does not	
	Specifications		compliance		state complete sandboxing	
					environment on premises including	
					various operating systems &	
					applications like Windows OS & its	
					applications, Linux OS & its	
					applications & MAC OS & its	
					applications in absence of this being	
					stated NPCI would not be able to	
					control the file/objects submissions	
					to on-premises sandbox only. This	
					may lead to vendors submiting the	
					files to the cloud without NPCI's	
					knowledge.	
				Proposed APT solution should perform	Clarification required, Should we	No change in RFP.
				advanced network detection and analysis of	read the clause as?	Should able to
	Section 9 -			the enterprise's internal/External network		perform detection
28		37	Annexure J - Technical	data.	"Proposed APT solution should	on Intenal (east-
120	Specifications	57	Compliance		perform advanced network	west), External
	specifications				detection and analysis of the	(inbound-outbound)
					enterprise's inbound/outbound	traffic.
					network traffic."	

				The proposed solution should support to	As per clause number 1 of the	Refer to
				monitor traffic from multiple segments	Technical Specifications the Network	corrigendum
				simultaneously on single appliance (East-West,	Anti-APT solution should be able to	
				North-South).	handle 500Mbps of total traffic. In	
					any organization where North-South	
					(Internet Traffic) is typically based on	
					total internet bandwidth and is same	
					or less than the total internet	
					bandwidth, but East-West traffic	
					(Intranet Traffic) i.e. from	
					LAN/Client segment to Server	
					segment the traffic may be huge	
					somewhere around 1Gbps to 4Gbps as	
					it is internal traffic, this would	
	Section 9 -		Annexure J - Technical		exceed 500Mbps appliance capacity	
281	Technical	37	Compliance		anytime. Also North-South and East-	
	Specifications				West segments are completely	
					different and may pass through	
					different Core Switches and may not	
					be feasible at times for connectivity.	
					Hence we would request NPCI to	
					please share North-South traffic	
					detail in Mbps/Gbps and East-West	
					traffic in Mbps/Gbps to ensure all the	
					traffic is covered by Network Anti-	
					APT solutions and also confirm if	
					connectivity for North-South traffic	
					and East-West traffic is feasible or	
					not.	
				The proposed solution should be dedicated	Similar to point 11 which is in more	Refer to
	Section 9 -		Annexure J - Technical	appliance and should not be enabled as	details, hence we request NPCI to	corrigendum
282	Technical	37	Compliance	additional licensed solution with proposed	remove this point as duplicate.	
	Specifications		Compliance	perimeter gateway devices such as firewall,		
				APT etc.		

				Security Vendor must have a Research/Labs	Reporting on Vulnerabilities is	Refer to
				organization and this organization must	primary function of Vulnerability	corrigendum
				contribute and report on finding new Zero-Day	Assessment tools / Solution.	
				vulnerabilities being exploited in the wild.		
					As a Network Anti-APT solution the	
					primary & most important function is	
					to prevent Zero-Day exploits in the	
					wild from targeting the	
					vulnerabilities. Also in real world, the	
					zero day explots may not available at	
					the same time when the actual	
					vulnerabilitiy is identified, hence it is	
	Section 9 -				important to detect & prevent zero	
283	Technical	37	Annexure J - Technical		day expliots / payloads.	
	Specifications	57	Compliance			
	opeenieations				Hence to benefit from the Network	
					Anti-APT we request NPCI to modify	
					this clause as:	
					"Security Vendor must have a	
					Research/Labs organization and this	
					organization must contribute and	
					report on finding new Zero-Day	
					expliots being identified /	
					discovered in the wild & should	
					automatically share the intel to the	
					Network Anti-APT Solution".	

				The proposed solution should be able to	Need for clarification on this point	Refer to
				detect any suspicious communication within	specifically Outside of Customers	corrigendum
				and outside of Customer's network	Network as it typically false in the	
					requirement of perimeter solutions	
					like Firewall / IPS.	
					With regards to within the network	
					suspicious communications would	
					NPCI like to detect malicious post-	
					exploitation activities such as	
					attacker lateral movements between	
					user workstation & servers? as	
					Attackers frequently use SMB & SMB2	
	Section 9 -				to carry their activity from	
284	Technical	37	Annexure J - Technical		compromised endpoints and move to	
	Specifications	5.	Compliance		servers, hiding their activities in	
	specifications				normal traffic.	
					If Yes, we would recommend NPCI to	
					modify the clause to:	
					"The proposed network Anti-APT	
					solution should also be able to	
					detect malicious post-exploitation	
					activities such as attacker lateral	
					movements between user	
					workstation & Servers. Attackers	
					frequently use SMB & SMB2 to	
					carry their activity from	
					compromised endpoints and move	
					to servers, hiding their activities	
				The Proposed solution should be able to	We would like to highlight this	Refer to
				detect communications to known command	requirement only mentions detection	corrigendum
				and control centers.	of known Command and Control	5
					Centers (C&C) only and not blocking	
					of the C&C as well it do not covers	
					unknown C&C detection and blocking.	
	Section 9 -				Hence in the benefit of NPCI we	
285	Technical	37	Annexure J - Technical		request the clause to be changed to:	
	Specifications		Compliance		"The Proposed solution should be	
					able to detect communications to	
					known & unknown command and	
					control center initiated by internal	
					infected clients."	
					injected chemis.	

<u> </u>				The proposed solution should be able to	Primarily this requirement falls in the	Refer to
				detect reputation of URL being accessed	category of Proxy Solution	corrigendum
				detect reputation of ORL being accessed		corrigendum
					requirement where reputation of the	
					URL plays a very important role,	
					however in Network Anti-APT the	
					analysis is not limited to just URL	
	Section 9 -				reputation but it should be able to	
28	Technical	37	Annexure J - Technical		analyze complete URL's in zero-trust	
	Specifications		Compliance		manner as attackers take advantage	
	opeenieations				of the URL reputation check tools to	
					launch sophisticated attacks and	
					compromise the Host/End-user.	
					Hence we recommend to remove or	
					modify the clause.	
				The proposed solution should support at least	In an Advanced Attack threat actors	Refer to
				100+ protocols for inspection	leverage C&C communication to	corrigendum
					command & control the victim	
					machine, hence it is important for an	
					organization to block all malicious	
					C&C communications regardless of	
	Section 9 -				ports and protocols, hence we	
28	Technical	38	Annexure J - Technical		request NPCI to change the clause to:	
	Specifications		Compliance			
					"The proposed solution for Network	
					Ani-APT should prevent any C&C	
					communications detected over North-	
					South traffic regardless of ports and	
					protocols"	
	1			1		

				Sandbox must have the ability to simulate the	There are various flavors of Sandbox	Refer to
				entire threat behavior.	environment used for analysis and	corrigendum
					not limited to just Windows OS but	
					also Linux, MAC OS with 32bit and	
					64bit architecture and various types	
					of applications targeted in the wild.	
					Hence in the benefit of NPCI we	
					request the clause to be very specific	
					like:	
	Section 9 -				"The proposed solution must be	
288	Technical	38	Annexure J - Technical		available as on premise physical	
	Specifications		Compliance		appliances with sandboxing	
					capability and must be able to	
					detect and report malware by	
					using multiple client environments	
					(operating systems with multiple	
					service pack levels) supporting	
					both x64 and x86 architectures	
					including Windows, Mac, CentOS	
					based on premise Virtual Execution	
1					Environment"	
				The proposed solution should have an built-in	OEM Specific Clause.	Refer to
				document vulnerabilities detection engine to		corrigendum
	Section 9 -		Annexure J - Technical	assure analysis precision and analysis	We request removal of the clause as	
289	Technical	38	Compliance	efficiency	the requirement gets addressed in	
	Specifications		comptiance		detection of Zero-Day exploits	
					targeting vulnerabilities in the wild in	
					clause 19 and 20.	

				The proposed solution should support Multiple	Advanced attackers once establish	Refer to
					the foothold tries to move laterally	corrigendum
					and dump sophisticated tools on	
				protocols Internal direction: SMB ,Database	various systems connected in the	
					network detecting this tools and	
					identifying this tools and techniques	
					plays a very important and critical	
					role in early detection and incident	
					response.	
					Hence in the benefit of NPCI it is	
					important to get visibility of such	
					activities of the threat for which we	
	Section 9 -				request modification of the clause to	
290		38	Annexure J - Technical		below:	
	Specifications		Compliance			
	opeenreacions				"The proposed solution should be	
					able to detect the activities of	
					attackers already resident in the	
					network core. The solution should	
					extracts malware and objects that	
					are transferred over HTTP, FTP &	
					other protocols and submit them to	
					the automated dynamic Analysis	
					engine for detonation and	
					confirmation on maliciousness. The	
					solution should extracts malware	
					and objects that are transferred	
					over HTTP, FTP like protocols and	
					submit them to an automated	
	Section 9 -			The Proposed solution should have a Co-	Duplicate point as all the previous	Refer to
291	Technical	38	Annexure J - Technical		clause covers the same.	corrigendum
	Specifications	50	Compliance	across multiple protocol, multiple sessions and	Request removal of the clause.	
	specifications			volume traffic analysis		

				The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF	Advanced attackers leverage various types of files to infiltrate in the target environment and not just	Refer to corrigendum
				files , Flash files, RTF files and and/or other	executables, pdf, flash or RTF file	
				objects.	types hence it is very important that	
					dynamic analysis engine should be	
					able to analyze different filetypes	
					without depending on the signatures.	
					Hence for critical infrastructure like	
					NPCI should ensure that various	
					filetypes which are leveraged by the	
					advanced attackers should be	
	Section 9 -				dynamically analyzed without	
292	Technical	38	Annexure J - Technical		depending upon the signatures alone,	
	Specifications	50	Compliance		in the benefit of NPCI we request	
	specifications				modification of this clause as follows:	
					"The proposed solution should have	
					the ability to analyze, detect and	
					block malware in common file	
					formats including but not limited	
					to executables, JAVA, PDF, MS	
					Office documents, common	
					multimedia contents such as JPEG,	
					QuickTime, MP3 and	
					ZIP/RAR/7ZIP/TNEF archives, 3gp,	
					asf, chm, com, dll, doc, docx, exe,	
					gif, hip, htm, ico, jar, jpeg, jpg,	
					mov, mps, mp4, pdf, png, ppsx,	

				The Dropogod colution should be able to	In a combination to distance the	Defer to
				The Proposed solution should be able to	In a sophisticated attack the	Refer to
				generate out of box reports to highlight	advanced attackers may or may not	corrigendum
				Infections, C&C behavior, Lateral Moment,	use malware, but they definitely use	
				Asset and data discovery and Exfiltration	various techniques & methodologies	
					to move laterally, hence it is	
					important for a solution to detect	
					TTP's and methodologies and alert	
					with timeline & date sliders with at	
					least 5 minutes of relevant network	
					activity data(layer 4-7) before and	
					after the attack.	
					Hence in the benefit of NPCI we	
					request modification of this clause	
	Section 9 -		Annexure J - Technical		with must have capabilities as:	
293	Technical	38	Compliance		indi mase nave capabilities as.	
	Specifications		comprisie		Proposed Internal Network APT	
					should detects the following types of	
					malicious post-infection activities:	
					a) Internal Reconnaissance	
					b) Privilege Escalation	
					c) Credentials Dumping	
					d) Lateral Movement of Malware	
					e) Remote Task Execution	
					f) Data Exfiltration Detection	
					g) Callback activities	
					h) Bot-tracker features like File	
					inspection, Packet flows, Signature	
					matching and statistics	
					i) Supports extensive metadata	
				The proposed APT must able to operate in	Analyzing asymmetric traffic results	Refer to
				Asymmetric traffic environment with	in ton's of false positive's and adds	corrigendum
				Vulnerability / Exploit filters for protection	unnecessary workload on validation	-
	Section 9 -		Anna anna I. Tachail I		of such all the alerts resulting in Alert	
294	Technical	38	Annexure J - Technical		Fatigue on SOC team, hence we	
	Specifications		Compliance		request removal of such clause which	
					adds overheads to security team and	
					miss on legitimate threats.	
\vdash				The proposed APT solution must support	OEM Specific IPS Solution, Request	Refer to
	Section 9 -		Annexure J - Technical	Adaptive Filter Configuration(AFC) which will	removal of this clause.	corrigendum
295	Technical	38	Compliance	alert or disable ineffective filter in case of		
	Specifications		comptiance	noisy filters		
\vdash				The APT filter must support network action	Duplicate Clause, Point 17 covers the	Refer to
				set such as Block (drop packet), Block (TCP	requirement hence we request	corrigendum
				Reset), Permit, Trust, Notify, Trace(Packet	removal of this clause.	
	Section 9 -			Capture), Rate Limit and Quarantine		
296	Technical	38	Annexure J - Technical		Also it is important for Anti-APT	
	Specifications		Compliance		solution to Block callback to C&C and	
					malicious communications in inline	
						1
					Imode.	

297	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed APT solution must support signatures, vulnerabilities and traffic filtering methods to detect attacks and malicious traffic	Clause is OEM Specific IPS Solution which heavily depends upon signature based detection. We request removal of this clause	Refer to corrigendum
298	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The APT filters must be categories into the following categories for easy management: Exploits, Identity Theft/Phishing, Reconnaissance, Security Policy, Spyware, virus, Vulnerabilities, Traffic Normalization,P2P, IM, Streaming Media	Clause is OEM Specific IPS Solution, Request removal of this clause.	Refer to corrigendum
299	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	Vulnerability based filter are known for most effectively for Zero Day Attack Protection and proposed solution must support vulnerability based filter	Clause is OEM Specific IPS Solution & only covers known attacks, Request removal of this clause.	Refer to corrigendum
300	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	The proposed APT should support the ability to mitigate Denial of Service (DoS/DDoS) attacks such as SYN floods	Clause is OEM Specific IPS Solution, Request removal of this clause.	Refer to corrigendum
301	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	The proposed APT must provide bandwidth rate limit to control the unwanted/nuisance traffic such as P2P, Online Game, etc.,	Clause is OEM Specific IPS Solution, Request removal of this clause.	Refer to corrigendum
302	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	The proposed APT must be able to use Reputation Service such as IP address or DNS to block traffic from or to 'known bad host' such as spyware, phishing or Botnet C&C	Clause is OEM Specific IPS Solution & only covers known attacks, Request removal of this clause.	Refer to corrigendum
303	Section 9 - Technical Specifications	39			Clause is OEM Specific IPS Solution & only covers known attacks, Request removal of this clause.	Refer to corrigendum
304	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance		The clause adds lot of dependency on the security teams to continuously monitor and keep on modifying policies increasing overheads and false positives, Anti-APT solution should be able to take decision with its intelligence with simple configuration to Block or Monitor the threat. Hence in the benefit of the NPCI we request modification/removal of this clause	Refer to corrigendum

305	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	NG APT engine must be a smart enough to inspect the traffic based on condition, If the traffic is suspicious then it goes for the deep packet inspection	Detecting traffic based on suspicion or deep packet inspection needs patterns / signatures to take decisions, Anti-APT solution should not just depend upon signatures but it should have dynamic analysis engine with signatureless detection and should create signatures in Realtime and block the threats inline.	Refer to corrigendum
306	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	The proposed management system shall allow the update of global threat intelligence via cloud and local Threat intelligence updates from proposed Network threat detection solution automatically for inline blocking	Please correct our understanding about local threat intelligence sharing. Do you mean sharing intelligence from your existing Anti- APT solutions from Email & content scanning Anti-APT solutions to Anti- APT for Network Security?	To be Integrated with our TIP platform for threat intelligence integration with other solutions deployed.
307	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	The management server must provide rich reporting capabilities include report for All attacks, Specific & Top N attack, Source, Destination, Misuse and Abuse report, Rate limiting report, Traffic Threshold report, Device Traffic Statistics and Advance DDoS report	Rate Limiting, Misuse & Abuse, Traffic Threshold & DDoS reports do not fall in Anti-APT solution, these are OEM specific and hence request NPCI to remove the same.	Refer to corrigendum
308	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	The proposed management system must be able to support the syslog CEF format that SIEM can support	Critical infrastructure like NPCI may have various tools for event correlation, automation, orchestrations etc limiting to CEF format only may limit integration with other tools and result no integration support. Hence we request NPCI to modify the clause to various types of log/event format but not limited to CEF only. Clause Modification to: The proposed management system must be able to support Common Event Format (CEF), Log Event Enhanced Format (LEEF), Comma- Separated Values (CSV), XML, JSON, or Text format that SIEM and other tools like automation and orchestration can support.	Refer to corrigendum

309	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	a big data engine that allows customers to provide faster security analytics and faster report generation	To integrate with Big Data Analytics the solution should support file formats that can be ingested in the Big Data Analytics tool, hence we request NPCI to modify the clause and not mandate with Big Data Engine which makes the clause to OEM Specific. Request modification in clause to: "The Management system should support file formats which can be ingested in Big Data Analytics Solution for faster report generation."	Refer to corrigendum
310	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	ever-growing variety of threats, including fileless and ransomware	This clause of Automatic detection and response requirement do not covers automatic prevention and integration with various other vectors of attack like Email, Endpoint EDR and File/content uploads from outside to respond to threats. In any enterprise organizations and critical infrastructure resilience defense strategy plays a very important role to defend against the advanced attack and hence should be in a Must Have category instead of Good to Have. Does NPCI wants to take benefit of Anti-APT for network security solution requirement with automatic prevention and integration with various vectors of attack capabilities and not just detection and response? If yes we request modification of the clause to: "The solution must have automatic detection, prevention, remediation and integration capabilities with various attack vectors not limited	Refer to corrigendum
311	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance		Clause is OEM Specific IPS Solution, Request removal of this clause.	Refer to corrigendum

312	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The solution should consolidate (at centralized location) the administration, reporting, and intelligence data sharing intelligence/IOC's between deployed Anti-APT Sensors/ solution at our organization (Email Analysis, File Analysis & EDR)	To support Advanced Defense Strategy and build advanced resilience infrastructure for NPCI it's important clause.	Okay, No change in RFP.
313	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	Central Management should provide option to create customized lists of IOCs received from these feeds and use them as a custom blacklist on the Central Management appliance. The types of IOCs like URL indicators, IP address indicators, domain indicators, and indicators with hashes of malicious files, combine them into a standard format called STIX (Structured Threat Information Expression)	To support Advanced Defense Strategy and build advanced resilience infrastructure for NPCI it's important clause.	No change in RFP
314	Section 9 - Technical Specifications			Centralized Sandboxing	OEM specific clause, some of the OEM's provide Built-in Sandboxing solution and do not require any additional/external Sandboxing solution. Hence we request NPCI to consider the same.	No change in RFP. Prefer to have built in sandboxing capabilities for Network Anti-APT solutions.
315	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The proposed solution should be able to run at least 50 parallel sandboxes for analysis of payload and on premise customized sandbox solution should have the capability to allow manual submission of suspicious files for analysis	Different OEM's have different methods and technology to run dynamic analysis and should not mandate on 50 parallel sandboxes instead it is important to have multiple executions to run in parallel for payload analysis automatically and not manually. Some of the OEM who have NO\limited number of Sandboxes built in depend upon external sandboxes which supports manual submission of files, hence we request for modification of the clause to: "The solution should support 1000+ executions to analyze the payloads in parallel depending on the performance capacity upto 500Mbps of the appliance deployed on- premises"	Refer to corrigendum

31	Section 9 - 5 Technical Specifications	40	Annexure J - Technical Compliance	Sandboxing Appliance should support Active/Passive or Active-Active deployment and should support configuring cluster for High Availability	Not applicable for built-in sandboxing solution hence we request modification of the clause to: "The Network Anti-APT solution should support Active/Passive or Active passive deployment on- premises"	No change in RFP. "The Network Anti- APT solution should support Active- Active, Active- Passive deployment on- premises".
31	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The proposed solution must be capable of analysis of different file types, including portable executables (PEs), web content, Web objects, images, Java, network flows, Microsoft and Adobe applications, PHP, WAR, JSP, ASP, and ASPX, archive files and multimedia etc. including all such file types which have shown presence in historic advance attackers profile, as a delivery channel, for initial compromise or backdoor or malicious dropper delivery.	Webshell attacks on Web Servers and manipulate the server and redirect to malicious content. Hence for critical infrastructure like NPCI should ensure that various	Refer to corrigendum

						Refer to
				Sandbox appliance should have redundant	For Network Anti-APT solution where	
				power supply, 2 TB or more storage capacity	the analysis has to done at wire speed	corrigendum
				with dedicated management port	on the traffic with aggressive packet	
					capture, it is recommended that the	
					Network Anti-APT appliance should	
					have minimum 2 HDD with atleast	
					4TB of capacity to ensure the	
	Section 9 -		Annexure J - Technical		analysis to complete in near real-	
318	Technical Specifications	40	Compliance		time.	
					Hence in the benefit of NPCI which	
					falls in National critical infrastructure	
					should have minimum 2 x 4TB HDD	
					and request amendment to the clause	
					to:	
					"Hardware should have minimum 2	
					HDD with atleast 4TB of capacity	
	Section 9 -		Annexure J - Technical	The Proposed Solution should be able to	Does NPCI only wants to detect	Refer to
319	Technical	40	Compliance	detect known bad URL before sandboxing	known bad URL's only?	corrigendum
	Specifications		comptance			
				The proposed solution should detect file-less	Attackers use encoded algorithms like	Refer to
				malware tools used for extracting plain text	XOR to hide password instead of plain	corrigendum
				passwords, hash, PIN codes and Kerberos	text, do NPCI would like to detect	
				tickets.	and extract passwords which are	
					encoded algorithm XOR instead of	
					just plain text? If yes,	
	Section 9 -		Annexure J - Technical		We request you to modify the clause	
320	Technical	40	Compliance		to:	
	Specifications		·			
					"The proposed solution should	
					detect file-less malwares tools	
					used for extracting	
					encoded/XOR'ed as well as plain	
					text passwords, hash, PIN codes	
					etc"	
	Section 9 -			The Proposed solution should allow Admin be	Please provide clarification on the	Refer to
321	Technical	40	Annexure J - Technical	able to inquire how many detections come	requirement.	corrigendum
JZI		40	Compliance	from malicious password-protected files		
	Specifications					

—						
					In Advanced Threat Landscape the	Refer to
				support of analysis of Windows & Linux	attacks are not limited to Windows &	corrigendum
				Operating System files	Linux environment only but MAC OS's	
					and its applications are also targeted	
					with Zero-day attacks, attackers also	
					leverage Webshell attacks on Linux	
					servers, hence it is important that	
					sandboxing solution should have	
					Windows, Linux and MAC OS's for	
					conducting dynamic analysis on-	
					premises and create real-time threat	
					intelligence to block call	
					back/malicious communications with	
	Continu 0					
322	Section 9 - Technical	41	Annexure J - Technical		C&C servers.	
JZZ	Specifications	1	Compliance		We would like to know if NPCI wants	
					to detect and prevent attacks	
					targeted towards MAC and Linux	
					including Webshell injection attacks?	
					If yes, we request modification of the	
					clause to:	
					"The proposed Anti-APT solution	
					should include on-premises	
					sandboxing for dynamic analysis	
					for Windows, Linux and MAC OS's	
					without any additional	
					requirement of licenses form OS's	
					and Applications from NPCI."	
	Castian O			The proposed solution should support X-Dst-		Need more clarity
	Section 9 -		Annexure J - Technical	Forwarded-For header, so that Network		
323	Technical	41	Compliance	Security alerts displays the correct destination		
	Specifications		· · · · · ·	IP address		
	Section 9 -			The proposed solution should provide alert		Need more clarity
324	Technical	41	Annexure J - Technical	details with mapping to the MITRE ATT&CK		
1 24	Specifications	1	Compliance	Framework to give more context for attack		
	specifications			investigation and allow easier triaging		
				SSL Capabilities	Does NPCI wants dedicated SSL	Refer to
					solution for Network Anti-APT or are	corrigendum
					looking for built-in SSL decryption	
	Section 9 -				capabilities in Network Anti-APT? as	
325	Technical				the requirement point/clause	
	Specifications				mentioned below are typically	
					available in dedicated SSL decryption	
					solution.	
1						

				Solution should inspect https traffic (Full Deep	Advanced attackers uses Websholl	Refer to
				Packet / SSL Traffic) and must provide	inject attacks to compromise Web	corrigendum
				decryption of unverified encrypted traffic for	Servers, would NPCI like to also have	corrigendum
				scanning and then re encrypt it before sending		
					capabilities? If yes please confirm and	
					amend/modify the same to the	
					requirement mentioned.	
					For Example the clause can be	
	Section 9 -				modified as:	
326	Technical	41	Annexure J - Technical		"The proposed solution should	
520	Specifications		Compliance		detect & prevent suspicious	
	specifications				Webshell files uploaded to web	
					servers through HTTP POST and	
					FTP protocols and also provide	
					mapping of methodology & alert	
					techniques to MITRE ATT&CK	
1 1					framework. It should also detect	
1 1					attempted data exfiltration &	
					SSL/TLS handshake fingerprinting	
					at the minimum"	
	Section 9 -			Integrate with any existing Proxy solution of	Please provide clarification on proxy	Should able to be
227		44	Annexure J - Technical	NPCI.	and expectation on Integration with	deployed inline
327	Technical	41	Compliance		Proxy.	with proxy solution.
	Specifications					
				SSL functionality should be available on the	Duplicate to Point 93 which clearly	Refer to
				proposed inline APT appliance	states that the Anti-APT should have	corrigendum
1 1					built-in SSL intercept capability	
	Section 9 -		Annexure J - Technical		which itself makes SSL inline to	
328	Technical	41	Compliance		Network Anti-APT, unless NPCI is	
1 1	Specifications		compliance		looking for dedicated SSL solution if	
1 1					yes, we would than propose	
					dedicated SSL decryption appliance	
					inline to Anti-APT.	
				The solution must support TLS fingerprint	Very important point where Anti-APT	No change in RFP
				detection detects malicious communication by	solution should be able to detect	
	Contine 0			TLS fingerprinting with JA3 between the	malicious communication by TLS	
329	Section 9 -	41	Annexure J - Technical	client and server.	Fingerprinting with JA3 inbetween	
329	Technical	41	Compliance		Client and Server. If it is good to have	
	Specifications		-		in that case NPCI may miss this	
					capability provided by some of the	
					Anti-APT solutions.	
	Section 9 -			Ability to automatically intercept all SSL/TLS	Please Clarify on the clause, as TCP	Refer to
330	Technical	41	Annexure J - Technical	based flows, also on other ports and protocols	ports have to be defined manually to	corrigendum
330		41	Compliance	(not only HTTPS)	automatically intercept SSL/TLS or	
	Specifications				HTTPS.	
Ī	Section 9 -		Annexure J - Technical	Support multiple active-inline devices	Please provide more clarification	Refer to
331	Technical	41	Compliance	simultaneously		corrigendum
	Specifications		compliance			

	Section 9 -			Ability to configure encryption/decryption policy (incl. block/pass-through) based on	These requirements can only be supported with dedicated SSL		Refer to corrigendum
332	Technical	41	Annexure J - Technical	source/destination ip/port	interception solution, We request		
552	Specifications		Compliance		NPCI to confirm if they need		
	specifications				dedicated SSL interception solution		
					to provide granular controls?		
				Ability to configure encryption/decryption	These requirements can only be		Refer to
	Section 9 -			policy (incl. block/pass-through) based on	supported with dedicated SSL		corrigendum
333	Technical	41	Annexure J - Technical	host/URL categorization	interception solution, We request		
555	Specifications	- 1	Compliance		NPCI to confirm if they need		
	specifications				dedicated SSL interception solution		
					to provide granular controls?		
				Ability to configure encryption/decryption	These requirements can only be	F	Refer to
	Section 9 -			policy (incl. block/pass-through) based on	supported with dedicated SSL		corrigendum
		44	Annexure J - Technical	threat intelligence	interception solution, We request		
334	Technical	41	Compliance	-	NPCI to confirm if they need		
	Specifications				dedicated SSL interception solution		
					to provide granular controls?		
				Ability to configure encryption/decryption	These requirements can only be	F	Refer to
	Section 9 - Technical Specifications			policy (incl. block/pass-through) based on CA	supported with dedicated SSL		corrigendum
				status	interception solution, We request		J
335		41	Annexure J - Technical Compliance		NPCI to confirm if they need		
					dedicated SSL interception solution		
	opeenieaciono				to provide granular controls? Also		
					provide use case for the same		
-				Ability to configure encryption/decryption	These requirements can only be		Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL		corrigendum
	Section 9 -		Annexure J - Technical	Subject / Domain Name	interception solution, We request		lonigendum
336	Technical	41	Compliance		NPCI to confirm if they need		
	Specifications		comptiance		dedicated SSL interception solution		
					to provide granular controls?		
-				Ability to configure encryption/decryption	These requirements can only be		Refer to
				policy (incl. block/pass-through) based on	supported with dedicated SSL		corrigendum
	Section 9 -		Annexure J - Technical	Cipher Suite and Key Strength	interception solution, We request	le l	Johngendum
337	Technical	41	Compliance	Cipiler Suite and Key Strength	NPCI to confirm if they need		
	Specifications		Comptiance		dedicated SSL interception solution		
					· · ·		
_				Support for Eail to wire (fail to open	to provide granular controls?		Refer to
	Castian O			Support for Fail-to-wire/fail-to-open	Requirement depends on the port		
	Section 9 -		Annexure J - Technical	hardware, traffic bypass filters (in the event	capability or external Active Failover		corrigendum
338	Technical	41	Compliance	of in-line security device failure) and	Kit is required, Please confirm of		
	Specifications		i	configurable link state monitoring/mirroring?	NPCI needs external Bypass Kit to		
					support the same?		

30 Section 9. Technical Specifications 41 Amezure J - Technical Compliance Support RSA, DHE, and ECDHE public key agent may make security. Secure Socket Layer and Transport Layer Society and the security between web browser and web server. Section 9. Technical Specifications 41 Amezure J - Technical Compliance Support RSA, DHE, and ECDHE public key agent may					Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3,	SSL stands for Secure Socket Layer	Refer to
339 Section 9 - Technical 340 41 Amexure J - Technical Compliance Support RSA, DHE, and ECDHE public Key algorithms? Support RSA, DHE, and ECDHE public Key algorithms? Support RSA, DHE, and SHA 256 hath algorithms? 3055, DE5, RC4, and Camellia Specifications 41 Amexure J - Technical Compliance Support RSA, DHE, and SHA 256 hath algorithms? 3055, DE5, RC4, and Camellia Specifications 41 Amexure J - Technical Compliance Support RSA, DHE, and SHA 256 hath algorithms? 3055, DE5, RC4, and Camellia Specifications 3055, DE5, RC4, and Camellia Specifications Support RSA, DHE, and SHA 256 hath algorithms? 3055, DE5, RC4, and Camellia Specifications 3055, DE5, RC4, and						· · · · · ·	
339 Section 9 - Technical 339 41 Amexure J - Technical Compliance Image:					sses, and ssez encryption protocots:		
339 Section 9 - Technical Specifications 41 Amexure J - Technical Compliance Amexure J - Technical Compliance Image: Protocol Support Application of the Sup							
339 Section 9 - Technical Specifications 41 Annexure J - Technical Compliance Image: Specification Specifications 41 Annexure J - Technical Compliance The main differences between Secure Socket Layer) is the advective switch are Authentication and confidentiality. Write In TLS (Carangport Layer Socurity is that in SSL (Secure Socket Layer) is the advective switch are Authentication and confidentiality. Write In TLS (Transport Layer Socurity is the 1.0 msc of the basis care Socket Layer). Neurosci se socket Layer) is the advective switch are Authentication and confidentiality. Security Secure Secket Layer) is Iss Security Security Se							
339 Section 9 - Technical Specifications 41 Annexure J - Technical Compliance Image: Section 9 - Compliance The main differences between Secure Security is that. In SSL (Secure Socket Layer), Nessage digets is used to create master secret and it provides that is must be able to support tayer Security, Nessage digets is used to create master secret. 1) SSL (Secure Socket Layer), Nessage digets is used to create master secret. 1) SSL (Secure Socket Layer), Nessage digets is used to create master secret. 1) SSL (Secure Socket Layer), Nessage digets is used to create master secret. 1) SSL (Secure Socket Layer) is the 3.0 versions sequal to TLS (Transport Layer Socurity), Hashed Message Authentication Code protocol is used Muthelia (Tay Transport Layer Socurity), Hashed Message Authentication Code protocol is used Authentication Code protocol is used Authentication Code protocol is used Authentication Code protocol is used Authentication Code protocol is used Authentication Code protocol is used Authentication Code protocol is used Authentication Code protocol is used Authentication Authenticatio Authentication Authentication Authenticati							
339 Section 9 - Technical Specifications 41 Amesure J - Technical Compliance The main differences between Secure Socket Layer, Nasyer and Transport Layer Security is bat. In SU, Gecure Socket Layer, Nasyer digets is use to create master security services which are Authentication and confidentiality, while in TLS (Transport Layer Security), Feudor-andom function is used to create master secret. 11 SSL (Secure Socket Layer), Is subject to the basic security services which are Authentication and confidentiality. 300 Section 9 - Technical Specifications 42 Amesure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Diplete the public key algorithms? Support RSA, DHE, and ECDHE public key algorithms? Diplete the public key algorithms? Refer to corrigendum security while in the public key algorithms? Support RSA, DHE, and ECDHE public key algorithms? Support RSA, DHE, and ECDHE public key algorithms? Diplete applic the public key algorithms? Refer to corrigendum security while in the public key algorithms? Support RSA, DHE, and ECDHE public key algorithms? Support RSA, DHE, and ECDHE public key algorithms? Support RSA, DHE, and ECDHE public key algorithms? Diplete applic the public key algorithms? Refer to corrigendum section support approximation weak ciphers and hence in the beenit of PHC we request removal of point 112 as duplicated Refer to corrigendum removed from the clase as this Refer to corrigendum removed from the clase as this Refer to corrigendum						1	
339Section 9 - Technical Specifications41Annexure J - Technical ComplianceSociety is that in SQL (Secure Societ Layer), Message digest is used to create master secret and it provides the basis security is that in SQL (Secure Societ Layer), Message digest is used to create master secret.Society is that its is the second security is that its is the second survival is the its is used to create master secret.Its is is is its is its is its is its is security is the 1.0 version is equal to TLS (Transport Layer Security) is the 1.0 version is equal to TLS (Transport Layer Security), Hashed while in transport Layer Security), Hashed while in transport Layer Security), Hashed while in transport Layer Security), Hashed With Im transport Layer Security), Hashed Mitting Hassa transport Layer Security), Hashed Massa transport Layer Securit						server.	
339Section 9- Technical Specifications41Annexure J - Technical ComplianceAnnexure J - Technical ComplianceSection 9- ComplianceAnnexure J - Technical ComplianceSection 9- ComplianceAnnexure J - Technical ComplianceSection 9- ComplianceSection 9- ComplianceSupport RSA, DHE, and ECDHE public key Security is the 10- Version.Section 9- ComplianceSupport RSA, DHE, and ECDHE public key Security is the 10- Version.Section 9- ComplianceSupport RSA, DHE, and ECDHE public key Security is the 10- Version.Support RSA, DHE, and ECDHE public key Security is the 10- Version.Section 9- ComplianceRefer to Corrigendum340Section 9- Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia Support AES, 3DES, DES, RC4, and Camellia Section 9- Technical SpecificationsSupport AES, 3DES, DES, RC4, and Camellia ComplianceSupport AES, 3DES, DES, RC4, and Camellia ComplianceRefer to Corrigendum340Section 9- Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia ComplianceSupport AES, 3DES, DES, RC4, and Camellia ComplianceRefer to CorrigendumRefer to Corrigendum341Sectio						The main differences between Secure	
339Section 9 - Technical Specifications41Annexure J - Technical ComplianceAnnexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key Support RSA, DHE, and ECDHE public key ComplianceDist (Secure Socket Layer) is the 3.0 Code protocol is used Anite more precise than point 112 which is very precise than point 112 w						Socket Layer and Transport Layer	
339Section 9 - Technical Specifications41Annexure J - Technical ComplianceAnnexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key Support RSA, DHE, and ECDHE public key ComplianceDist (Secure Socket Layer) is the 3.0 Code protocol is used Anite more precise than point 112 which is very precise than point 112 w						Security is that. In SSL (Secure Socket	
339Section 9 - Technical Specifications41Annexure J - Technical ComplianceAnnexure J - Technical ComplianceAnnexure J - Technical ComplianceAnnexure J - Technical ComplianceAnnexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Deplicate as point His oversion is equal to TUS (Transport Layer Security) service (Transport Layer Security) services (Transport Layer Security) is used.Refer to corrigendum340Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Clipters in details which are more precise than point 12 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and SHA-256 hash algorithms?Support RSA, PHE, and SHA-256 hash algorithms?Support RSA, PHE, and SHA-256 hash algorithms?Support RSA, DHE, and SHA-256 hash algorithms?Support RSA, DHE, and SHA-256 hash algorithms?Support RSA, DHE, and SHA-256 hash algorithms?Support RSA, PHE, and SHA-256 hash algorithms?Support RSA, SHA-1, and SHA-256 hash algorithms?Support R							
339Section 9 - Technical Specifications41Annexure J - Technical ComplianceAnnexure J - Technical ComplianceSupport ASS, DHE, and ECDHE public key algorithms?Upport ASS, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Clipter and the received t							
339 Section 9 - Technical Specifications 41 Annexure J - Technical Compliance Authentication and confidentiality. while in TLS (Transport Layer Security). Psudo random function is used to create master secret. Image: Section 9 - 1 SSL (Secure Socket Layer) is the 3.0 version. Image: Section 9 - 1 SSL (Secure Socket Layer) is the 1.0 version. 340 Section 9 - Technical Specifications 42 Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 341 Section 9 - Technical Specifications 42 Annexure J - Technical Compliance Support RSA, DHE, and ECDHE public key algorithms? Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Refer to corrigendum 341 Section 9 - Technical Specifications 42 Annexure J - Technical Compliance Support ASS, 3DES, DES, RC4, and Camellia symmetric key algorithms? 305S, SES, RC4 and Camellia symmetric key algorithms? 305S, SES, RC4 and Camellia specifications Refer to corrigendum 341 Section 9 - Technical Specifications 42 Annexure J - Technical Compliance Support MDS, SHA-1, and SHA-256 hash algorithms? 305S being a weak ciphers and can be easily a weak ciphers and can be easily a weak ciphers and can be easily a weak ciphers and can be easin y a weak ciphers and can							
339Technical Specifications41Compliancewhile in TLS (Transport Layer Security), Pseudo-random function is used to create master secret. 1) SSL (Secure Socket Layer) is the 3.0 version is equal to TLS (Transport Layer Security) is the 1.0 version. 2) in SSL (Secure Socket Layer), Message Authentication Code protocol is used while in TLS(Transport Layer Security) is the 1.0 version. 2) in SSL (Secure Socket Layer), Message Authentication Code protocol is used while in TLS(Transport Layer Security) is the 3.0 version. 2) in SSL (Secure Socket Layer), Message Authentication Code protocol is used while in TLS(Transport Layer Security), Hashed Message Authentication Code protocol is used. 3) SSL (Secure Socket Layer) is lessRefer to corrigendum340Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the clipticate as point 112 which is very generic. Hence we request removal of point 112 as dupicated. 125, DES, RC4 and Canellia to useRefer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?Support AES, 3DES, DES, RC4 and Camellia algorithms?Refer to corrigendumRefer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport ADS, SHA-1, and SHA-256 hash algorithms?MDS being a weak (cliphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to <td></td> <td></td> <td></td> <td></td> <td></td> <td></td> <td></td>							
SpecificationsAAmexandSecurity, Pseudo-random function is used to create master secret.1) SL (Secure Socket Layer) is the 3, Oversion is equal to TLS (Transport Layer Security) is the 1.0 	339	Technical	41			· · · · · ·	
Image: Part of the section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 112 which is very generic. Hence we request removal of point 112 which is very generic. Hence we request removal and hence in the beside in your environment. Hence we request removal for the same and should be removed from the clause as the same and		Specifications		compliance			
Image: Section 9 - 1 34042Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symetric key algorithms?Support AES, 3DES, DES, RC4, and Camellia algorithms?Denetic of MPC and Camellia are weak ciphers and came weak ciphers and came algorithms?Refer to corrigendum340Section 9 - 1 Sections42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia algorithms?3DES, DES, RC4 and Camellia are weak ciphers and came be algorithms?Refer to corrigendum341Section 9 - 1 Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia algorithms?3DES, DES, RC4 and Camellia are weak ciphers and came be algorithms?Refer to corrigendum342Section 9 - 1 Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same and should be corrigendumRefer to corrigendum342Section 9 - 1 Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, NE4, and SHA-256 hash algorithms?MDS being a and abould be removed for the cause as thisRefer to corrigendum							
Image: Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers and hence in the banefit of NPCI we request not to use the same and should be in your environment.Refer to corrigendum340Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers and can be easily manipulated we recommend not to use the same and should be in your environment.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHS, NHA, and SHA-256 hash algorithms?DES, DES, RC4, and Camellia are weak ciphers and hence in the banefit of NPCI we request not to use the same and should be in your environment.Refer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MDS being a weak ciphers and hence in the banefit of NPCI we request not to use the same and should be removed from the clause as thisRefer to corrigendum						used to create master secret.	
Image: Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 112 which is very generic. Hence we request not to use the same in your environment.Refer to corrigendum340Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the ciper sin details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?Support AES, 3DES, DES, RC4 and Camellia weak ciphers and hence in the benefit of NPC1 we request not to use the same in your environment.Refer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport ADS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum						1) SSL (Secure Socket Layer) is the	
Annexure J · Technical Specifications42Annexure J · Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?Support AES, 3DES, DES, RC4, and Camellia add Camellia SpecificationsSupport AES, 3DES, DES, RC4, and Camellia add SpecificationsSupport AES, 3DES, DES, RC4, and SHA-256 hash algorithms?Message Authentication Code protocol is used. 3) SSL (Secure Socket Layer), Message Authentication Code protocol is used. 3) SSL (Secure Socket Layer) is lessRefer to corrigendum340Section 9 · Technical Specifications42Annexure J · Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?Support AES, 3DES, DES, RC4, and Camellia adgrithms?Section 9 · manuel AI Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. MDS being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum						3.0 version is equal to TLS	
kkk						(Transport Layer Security) is the 1.0	
Annexure J - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum340Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport ABS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum						version.	
Image: Problem of the state						2) In SSL(Secure Socket Layer),	
Image: Problem of the state						Message Authentication Code	
Image: Section 9 - 340Annexure J - Technical SpecificationsSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum340Section 9 - 34142Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms?3055, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia as symmetric key algorithms?3055, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - 342Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum							
Image: Section 9 - 340Annexure J - Technical SpecificationsSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum340Section 9 - 34142Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms?3055, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia as symmetric key algorithms?3055, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - 342Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum						TLS(Transport Laver Security).	
Image: Constraint of the section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia Symmetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and SHA-256 hash algorithms?3DES being a weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and hence he easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum							
Image: section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia Specifications3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia Support NDS, SHA-1, and SHA-256 hash algorithms?More support NDS is an anney compliance weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum						-	
340Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport RSA, DHE, and ECDHE public key algorithms?Duplicate as point 111 covers the Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?30ES, DES, RC4 and Camellia algorithms?30ES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MDS being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum							
340Section 9 - Technical Specifications42Annexure J - Technical Compliancealgorithms?Ciphers in details which are more precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport ADS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum	\vdash				Support RSA, DHE, and ECDHE public key	, , , , , , , , , , , , , , , , , , ,	Refer to
340Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?Precise than point 112 which is very generic. Hence we request removal of point 112 as duplicated.341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - Technical SpecificationsSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum						1 · · ·	
340Technical Specifications42Compliancegeneric. Hence we request removal of point 112 as duplicated.341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum				Annexure J - Technical		1 .	
Specifications Specifications 42 Annexure J - Technical Compliance Support AES, 3DES, DES, RC4, and Camellia symmetric key algorithms? 3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment. Refer to corrigendum 342 Section 9 - Technical Specifications 42 Annexure J - Technical Compliance Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as this Refer to corrigendum	340		42				
Image: section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum		Specifications				5	
341Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport AES, 3DES, DES, RC4, and Camellia symmetric key algorithms?3DES, DES, RC4 and Camellia are weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.Refer to corrigendum342Section 9 - Technical Specifications42Annexure J - Technical ComplianceSupport MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum							
341Section 9 - Technical Specifications42Annexure J - Technical Compliancesymmetric key algorithms?weak ciphers and hence in the benefit of NPCI we request not to use the same in your environment.corrigendum342Section 9 - Technical Technical42Annexure J - Technical algorithms?Support MDS, SHA-1, and SHA-256 hash algorithms?MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as thisRefer to corrigendum	\vdash				Support AES, 3DES, DES, RC4, and Camellia		Refer to
341 Technical Specifications 42 Compliance benefit of NPCI we request not to use the same in your environment. 342 Section 9 - Technical Specifications 42 Annexure J - Technical Compliance Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as this Refer to corrigendum				Annexure J - Technical			
Specifications Specifications Image: Complexity of the symplexity of the symp	341		42			1 · · ·	
342 Section 9 - Technical Specifications 42 Annexure J - Technical Compliance Support MDS, SHA-1, and SHA-256 hash algorithms? MD5 being a weak ciphers and can be easily manipulated we recommend not to use the same and should be removed from the clause as this Refer to corrigendum		Specifications		Compliance		· · ·	
342 Section 9 - Technical 42 Annexure J - Technical Compliance 42 Annexure J - Technical Compliance easily manipulated we recommend not to use the same and should be removed from the clause as this corrigendum	\vdash				Support MDS, SHA-1, and SHA-256 hash		Refer to
Becching - Image: Section 9 - Imag							corrigendum
342 Technical 42 Specifications Compliance removed from the clause as this				Annexure J - Technical			
Specifications I I I I I I I I I I I I I I I I I I I	342		42				
House compromise security.		Specifications					

				Total Packet processing capacity of single	Conflicts with the requirement	Refer to
				device should be 1 Gbps	mentioned in point 1 which mentions	corrigendum
					Hardware appliance should be able to	
					handle 500Mbps in total.	
					In total traffic of 500Mbps if we	
	Section 9 -				consider 40-50% https traffic it comes	
343		42	Annexure J - Technical		to around 200-250Mbps of HTTPS	
545	Specifications		Compliance		traffic.	
	specificacions					
					Hence we request clarification on	
					actual requirement of HTTPS/SSL	
					decryption and encryption traffic	
					capabilities on total 500Mbps traffic	
					mentioned in point 1.	