RFP for procurement of Network APT Solution - RFP # NPCI/RFP/2021-22/IT/18 dated 04.03.2022."							
Consolidated list of Replies to Pre-bid Queries							
S.No	**Document Reference**	**Page No**	**Clause No**	**Description in RFP**	**Clarification Sought**	**Additional Remarks (if any)**	**NPCI 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 telephone number	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 direct telephone number		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:	▫ Bidder should ensure availability of on-site resource if required for troubleshooting and resolution of technical issues back-to-back support from OEM.	Request customer to please specify the requirement		Bidder should be available on NPCI site (Chennai/Hyderabad) 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.	Request customer to please amend the Penalty clause as below: 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 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 violation in meeting the above SLA requirements which leads to Severity 2 incident, NPCI shall impose 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. 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 500/- (Indian Rupees Two Thousand only) per hour with a max cap of 2% of total AMC value.		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

7	RFP	37	Section 9 - Technical Specifications	The proposed solution should have the ability to be deployed in the following 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.	kindly modify this clause as " **The proposed solution should have the 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."**		No change in RFP
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		No change in RFP. APT solution should be able to achieve this independent of external devices or solution.
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"**		No change in RFP. "The Network Anti-APT solution should support Active-Active, Active-Passive deployment 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	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.
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		Should able to be deployed inline with 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

22	RFP	41	Section 9 - Technical Specifications	The proposed solution for network Anti-APT should have built-in SSL Intercept capability (100% SSL traffic performance) to examine encrypted user bound traffic to detect threats (such as CnC traffic and data exfiltration) that attackers may hide in encrypted streams	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.
23	RFP	41	Section 9 - Technical Specifications	Fully support transparent (bump in wire) mode	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.
24	RFP	41	Section 9 - Technical Specifications	The solution must support TLS fingerprint detection detects malicious communication by TLS fingerprinting with JA3 between the client and server	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.
25	RFP	41	Section 9 - Technical Specifications	Single box solution can both decrypt and re-encrypt (full duplex) in all modes	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.
26	RFP	41	Section 9 - Technical Specifications	Ability to automatically intercept all SSL/TLS based flows, also on other ports and protocols (not only HTTPS)	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
27	RFP	41	Section 9 - Technical Specifications	Ability to import server side certificates and private keys for decryption	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.
28	RFP	41	Section 9 - Technical Specifications	Ability to cache dynamically generated certificates for reuse on subsequent connections	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.

29	RFP	41	Section 9 - Technical Specifications	pport multiple active-inline devices simultaneou	this deployment introduce the latency and impact on overall application performance , hence request you to remove this clause from the RFP.		Refer to corrigendum
30	RFP	41	Section 9 - Technical Specifications	Ability to configure encryption/decryption policy (incl. block/pass through) based on source/destination ip/por	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
31	RFP	41	Section 9 - Technical Specifications	Ability to configure encryption/decryption policy (incl. block/pass through) based on host/URL categorization	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
32	RFP	41	Section 9 - Technical Specifications	Ability to configure encryption/decryption policy (incl. block/pass through) based on threat intelligence	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
33	RFP	41	Section 9 - Technical Specifications	Ability to configure encryption/decryption policy (incl. block/pass through) based on CA stat	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
34	RFP	41	Section 9 - Technical Specifications	Ability to configure encryption/decryption policy (incl. block/pass through) based on Subject / Domain Nam	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
35	RFP	41	Section 9 - Technical Specifications	Ability to configure encryption/decryption policy (incl. block/pass through) based on Cipher Suite and Key Stre	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
36	RFP	41	Section 9 - Technical Specifications	k/pass through) based on grouped or pre-configured lists of above	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.

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.

44	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.
45	Section 9 - Technical Specifications	59	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

46	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution must be available as on premise physical appliances with sandboxing capability	NPCI being an National Critical Infrastructure of India where 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 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 files to the cloud without NPCI's knowledge.		Refer to corrigendum
47	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should have multiple Virtual Machine for dynamic/sandboxing analysis of payload in redundancy to ensure if one appliance fails other appliance should be able to support at similar capacity.			Need more clarity
48	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	Proposed APT solution should perform advanced network detection and analysis of the enterprise's internal/External network data.	Clarification required, Should we read the clause as? ***"Proposed APT solution should perform advanced network detection and analysis of the enterprise's inbound/outbound network traffic."***		Refer to corrigendum

49	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should support to monitor traffic from multiple segments simultaneously on single appliance (East-West, North-South).	As per clause number 1 of the Technical Specifications the Network Anti-APT solution should be able to 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 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 connectivity for North-South traffic and East-West traffic is feasible or not.		No change in RFP
50	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should be dedicated appliance and should not be enabled as additional licensed solution with proposed perimeter gateway devices such as firewall, APT etc.	Similar to point 11 which is in more details, hence we request NPCI to remove this point as duplicate.		Need more clarity

51	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	Security Vendor must have a Research/Labs organization and this organization must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild.	Reporting on Vulnerabilities is primary function of Vulnerability Assessment tools / Solution. 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 expliots / payloads. 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**".		Need more clarity

52	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should be able to detect any suspicious communication within and outside of Customer's network	Need for clarification on this point specifically Outside of Customers 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 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 carry their activity from compromised endpoints and move to servers, hiding their activities***		Need more clarity
53	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The Proposed solution should be able to detect communications to known command and control centers.	We would like to highlight this requirement only mentions detection 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: ***"The Proposed solution should be able to detect communications to known & unknown command and control center initiated by internal infected clients."***		Need more clarity

54	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should be able to detect reputation of URL being accessed	Primarily this requirement falls in the category of Proxy Solution requirement where reputation of the 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 manner as attackers take advantage 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.		Need more clarity
55	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	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: "The proposed solution for Network Ani-APT should prevent any C&C communications detected over North-South traffic regardless of ports and protocols"		Need more clarity

56	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	Sandbox must have the ability to simulate the entire threat behavior.	*There are various flavors of Sandbox environment used for analysis and 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:* ***"The proposed solution must be 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 based on premise Virtual Execution Environment"***		Refer to corrigendum
57	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency	OEM Specific Clause. We request removal of the clause as the requirement gets addressed in detection of Zero-Day exploits targeting vulnerabilities in the wild in clause 19 and 20.		Refer to corrigendum

58	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should support Multiple protocols for inspection. Example:- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction: SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device	Advanced attackers once establish the foothold tries to move laterally and dump sophisticated tools on 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 request modification of the clause to 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 and objects that are transferred over HTTP, FTP like protocols and submit them to an automated***		Refer to corrigendum
59	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis	Duplicate point as all the previous clause covers the same. Request removal of the clause.		Refer to corrigendum

60	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.	Advanced attackers leverage various types of files to infiltrate in the target environment and not just executables, pdf, flash or RTF file 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, 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, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx,***		Refer to corrigendum

61	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and Exfiltration	In a sophisticated attack the advanced attackers may or may not use malware, but they definitely use 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 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 inspection, Packet flows, Signature matching and statistics i) Supports extensive metadata		Refer to corrigendum
62	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed APT must able to operate in Asymmetric traffic environment with Vulnerability / Exploit filters for protection	Analyzing asymmetric traffic results in ton's of false positive's and adds unnecessary workload on validation of such all the alerts resulting in Alert Fatigue on SOC team, hence we request removal of such clause which adds overheads to security team and miss on legitimate threats.		Refer to corrigendum
63	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed APT solution must support Adaptive Filter Configuration(AFC) which will alert or disable ineffective filter in case of noisy filters	OEM Specific IPS Solution, Request removal of this clause.		Refer to corrigendum
64	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	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	Duplicate Clause, Point 17 covers the requirement hence we request removal of this clause. Also it is important for Anti-APT solution to Block callback to C&C and malicious communications in inline mode.		Refer to corrigendum

65	Section 9 - Technical Specifications	59	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
66	Section 9 - Technical Specifications	59	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
67	Section 9 - Technical Specifications	59	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
68	Section 9 - Technical Specifications	59	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
69	Section 9 - Technical Specifications	59	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
70	Section 9 - Technical Specifications	59	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
71	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed APT must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score	Clause is OEM Specific IPS Solution & only covers known attacks, Request removal of this clause.		Refer to corrigendum
72	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	Must have the ability to correlate the monitored attacks to the APT filters number and recommended action	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

73	Section 9 - Technical Specifications	59	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
74	Section 9 - Technical Specifications	59	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.
75	Section 9 - Technical Specifications	59	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
76	Section 9 - Technical Specifications	59	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

77	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	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 Solution for faster report generation."***		Refer to corrigendum
78	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	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. **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

80	Section 9 - Technical Specifications	59	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.
81	Section 9 - Technical Specifications	59	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
82	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	**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.	12	No change in RFP. Prefer to have built in sandboxing capabilities for Network Anti-APT solutions.
83	Section 9 - Technical Specifications	59	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

84	Section 9 - Technical Specifications	59	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".
85	Section 9 - Technical Specifications	59	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.	Advanced attackers leverage various types of files to infiltrate in the target environment especially Webshell attacks on Web Servers and manipulate the server and redirect to malicious content. 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, in the benefit of NPCI we request 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 detection support for JSP, PHP, and WAR (Web archive) file types etc."***		Refer to corrigendum

86	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	Sandbox appliance should have redundant power supply, 2 TB or more storage capacity with dedicated management port	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
87	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The Proposed Solution should be able to detect known bad URL before sandboxing	Does NPCI only wants to detect known bad URL's only?		Refer to corrigendum
88	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The proposed solution should detect file-less malware tools used for extracting plain text passwords, hash, PIN codes and Kerberos tickets.	Attackers use encoded algorithms like XOR to hide password instead of plain text, do NPCI would like to detect and extract passwords which are encoded algorithm XOR instead of just plain text? If yes, We request you to modify the clause to: ***"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...."***		Refer to corrigendum
89	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The Proposed solution should allow Admin be able to inquire how many detections come from malicious password-protected files	Please provide clarification on the requirement.		Refer to corrigendum

90	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	The Proposed Sandboxing solution must support of analysis of Windows & Linux Operating System files	In Advanced Threat Landscape the attacks are not limited to Windows & 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 C&C servers. 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."***		Refer to corrigendum
91	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	**SSL Capabilities**	Does NPCI wants dedicated SSL solution for Network Anti-APT or are looking for built-in SSL decryption capabilities in Network Anti-APT? as the requirement point/clause mentioned below are typically available in dedicated SSL decryption solution.		Refer to corrigendum

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

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

105	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, SSL3, and SSL2 encryption protocols?	SSL stands for Secure Socket Layer while TLS stands for Transport Layer 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), Hashed Message Authentication Code protocol is used.** **3) SSL (Secure Socket Layer) is less**		Refer to corrigendum

106	Section 9 - Technical Specifications	59	Annexure J - Technical Compliance	Solution should support inbound & outbound ciphers like: ECDHE-RSA-AES128-GCM-SHA256 ECDHE-ECDSA-AES128-GCM-SHA256 ECDHE-RSA-AES256-GCM-SHA384 ECDHE-ECDSA-AES256-GCM-SHA384 DHE-RSA-AES128-GCM-SHA256 DHE-RSA-AES256-GCM-SHA384 ECDHE-RSA-AES128-SHA256 ECDHE-ECDSA-AES128-SHA256 ECDHE-RSA-AES256-SHA384 ECDHE-ECDSA-AES256-SHA384 DHE-RSA-AES128-SHA256 DHE-RSA-AES256-SHA256 ECDHE-RSA-AES128-SHA ECDHE-ECDSA-AES128-SHA ECDHE-RSA-AES256-SHA ECDHE-ECDSA-AES256-SHA DHE-RSA-AES128-SHA DHE-RSA-AES256-SHA AES128-GCM-SHA256 AES256-GCM-SHA384 AES128-SHA256 AES256-SHA256 AES128-SHA AES256-SHA			No change in RFP
107	Section 9 - Technical Specifications	59	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	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
109	Section 9 - Technical Specifications	59	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 would compromise security.		Refer to corrigendum

110	Section 9 - Technical Specifications	59	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
111	4.1 Eligibility Criteria	56	2.1	The bidder should have reported minimum annual turnover of Rs. 5 crores in each of the last 3 financial years and should have reported profits (profit after tax) as per audited financial statements in last 3 financial years (FY 2018-19, 2019-20, 2020-21).	We request to amend the caluse as " Should we have **Positive NETWORTH** instead of profit after tax in last 3 financial years (FY 2018-19, 2019-20, 2020-21). Or should be Profit **After Tax in any two FY.**	We request you to amend the caluse as Due to Pandemic our **Profit after Tax is not there in FY-20-21 however we have postive networth. In lockdown the profit after tax affected due to many reason**. All other PSU BFSI considering this caluse and giving relaxation for FY20-21. PLease help to amend so that we can submit our BID.	No Change in RFP
112	Payment Terms:	29	8.19	AMC: Payment shall be made quarterly in arrears within 30 days from the date of receipt of invoice along with submission of completion report/ necessary documents / Certificates / Reports duly verified by NPCI officials.	We request to amend the payment term as Yearly Advance as it is software and need to bill on Year basis		No Change in RFP
113	Delivery schedule	25	8.1	Delivery of hardware, software, and license should be within 6 weeks	Please help to amend this as delivery in 8-10 weeks as now deliveies are getting affected.		No Change in RFP
114	Section 3 – Scope of Work	10	Section 3.1: Scope of Work	Technical Training should be arranged by OEM directly.	Request NPCI to consider the " Technical Training should be arranged by OEM/ OEM Authorized Partners".		Refer to corrigendum
115	3.1 Scope of work:	10		Appliance (APT)- minimum of 04 Nos. as active-active for two DC, followed by Management & Database servers.	Request NPCi to ealborate more on this requirement.		Should have total of 4 APT devices with 2 in DC and 2 in DR having Active-Active setup 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.
119	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

123	Section 8 - Terms and Conditions	24	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.	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."		It should be reviewed by OEM only. Data collection can be done by bidder.
124	8.8 Key Deliverables	24	6	Detailed implementation reports, HLD's & LLD's, Throughput achievement, QAT (Quality Assurance Testing), Hardening documents for APT security, performance, quality and functioning.	Our understanding is this needs to be provided by the sucessful bidder? Pls clarify.		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.	Reqeust 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

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

132	Section 8 - Terms and Conditions	30	8.22 Indemnity	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 negligence or misconduct of the bidder and its employees and representatives, breach of the terms and conditions of the agreement or purchase order, 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..	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

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

145	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
146	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution must be available as on premise physical appliances with sandboxing capability	NPCI being an National Critical Infrastructure of India where 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 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 files to the cloud without NPCI's knowledge.		Refer to corrigendum

147	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	Proposed APT solution should perform advanced network detection and analysis of the enterprise's internal/External network data.	Clarification required, Should we read the clause as? ***"Proposed APT solution should perform advanced network detection and analysis of the enterprise's inbound/outbound network traffic."***		No change in RFP. Should able to perform detection on Intenal (east-west), External (inbound-outbound) traffic.
148	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should support to monitor traffic from multiple segments simultaneously on single appliance (East-West, North-South).	As per clause number 1 of the Technical Specifications the Network Anti-APT solution should be able to 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 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 connectivity for North-South traffic and East-West traffic is feasible or not.		Refer to corrigendum
149	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be dedicated appliance and should not be enabled as additional licensed solution with proposed perimeter gateway devices such as firewall, APT etc.	Similar to point 11 which is in more details, hence we request NPCI to remove this point as duplicate.		Refer to corrigendum

150	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	Security Vendor must have a Research/Labs organization and this organization must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild.	Reporting on Vulnerabilities is primary function of Vulnerability Assessment tools / Solution. 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 expliots / payloads. 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**".		Refer to corrigendum

151	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be able to detect any suspicious communication within and outside of Customer's network	Need for clarification on this point specifically Outside of Customers 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 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 carry their activity from compromised endpoints and move to servers, hiding their activities***		Refer to corrigendum
152	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The Proposed solution should be able to detect communications to known command and control centers.	We would like to highlight this requirement only mentions detection 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: ***"The Proposed solution should be able to detect communications to known & unknown command and control center initiated by internal infected clients."***		Refer to corrigendum

153	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be able to detect reputation of URL being accessed	Primarily this requirement falls in the category of Proxy Solution requirement where reputation of the 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 manner as attackers take advantage 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.		Refer to corrigendum
154	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	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: "The proposed solution for Network Ani-APT should prevent any C&C communications detected over North-South traffic regardless of ports and protocols"		Refer to corrigendum

155	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	Sandbox must have the ability to simulate the entire threat behavior.	*There are various flavors of Sandbox environment used for analysis and 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:* ***"The proposed solution must be 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 based on premise Virtual Execution Environment"***		Refer to corrigendum
156	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency	OEM Specific Clause. We request removal of the clause as the requirement gets addressed in detection of Zero-Day exploits targeting vulnerabilities in the wild in clause 19 and 20.		Refer to corrigendum

157	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should support Multiple protocols for inspection. Example:- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction: SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device	Advanced attackers once establish the foothold tries to move laterally and dump sophisticated tools on 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 request modification of the clause to 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 and objects that are transferred over HTTP, FTP like protocols and submit them to an automated***		Refer to corrigendum
158	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis	Duplicate point as all the previous clause covers the same. Request removal of the clause.		Refer to corrigendum

159	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.	Advanced attackers leverage various types of files to infiltrate in the target environment and not just executables, pdf, flash or RTF file 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, 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, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx,***		Refer to corrigendum

160	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and Exfiltration	In a sophisticated attack the advanced attackers may or may not use malware, but they definitely use 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 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 inspection, Packet flows, Signature matching and statistics i) Supports extensive metadata		Refer to corrigendum
161	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed APT must able to operate in Asymmetric traffic environment with Vulnerability / Exploit filters for protection	Analyzing asymmetric traffic results in ton's of false positive's and adds unnecessary workload on validation of such all the alerts resulting in Alert Fatigue on SOC team, hence we request removal of such clause which adds overheads to security team and miss on legitimate threats.		Refer to corrigendum
162	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed APT solution must support Adaptive Filter Configuration(AFC) which will alert or disable ineffective filter in case of noisy filters	OEM Specific IPS Solution, Request removal of this clause.		Refer to corrigendum
163	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	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	Duplicate Clause, Point 17 covers the requirement hence we request removal of this clause. Also it is important for Anti-APT solution to Block callback to C&C and malicious communications in inline mode.		Refer to corrigendum

164	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
165	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
166	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
167	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
168	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
169	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
170	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	The proposed APT must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score	Clause is OEM Specific IPS Solution & only covers known attacks, Request removal of this clause.		Refer to corrigendum
171	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	Must have the ability to correlate the monitored attacks to the APT filters number and recommended action	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

172	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
173	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.
174	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
175	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

176	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	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 Solution for faster report generation."***		Refer to corrigendum
177	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	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. **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
178	Section 9 - Technical Specifications	40	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

179	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.
180	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
181	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.
182	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

183	Section 9 - 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".
184	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.	Advanced attackers leverage various types of files to infiltrate in the target environment especially Webshell attacks on Web Servers and manipulate the server and redirect to malicious content. 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, in the benefit of NPCI we request 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 detection support for JSP, PHP, and WAR (Web archive) file types etc."***		Refer to corrigendum

185	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	Sandbox appliance should have redundant power supply, 2 TB or more storage capacity with dedicated management port	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
186	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The Proposed Solution should be able to detect known bad URL before sandboxing	Does NPCI only wants to detect known bad URL's only?		Refer to corrigendum
187	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The proposed solution should detect file-less malware tools used for extracting plain text passwords, hash, PIN codes and Kerberos tickets.	Attackers use encoded algorithms like XOR to hide password instead of plain text, do NPCI would like to detect and extract passwords which are encoded algorithm XOR instead of just plain text? If yes, We request you to modify the clause to: ***"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...."***		Refer to corrigendum
188	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The Proposed solution should allow Admin be able to inquire how many detections come from malicious password-protected files	Please provide clarification on the requirement.		Refer to corrigendum

189	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The Proposed Sandboxing solution must support of analysis of Windows & Linux Operating System files	In Advanced Threat Landscape the attacks are not limited to Windows & 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 C&C servers. 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."***		Refer to corrigendum
190	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The proposed solution should support X-Dst-Forwarded-For header, so that Network Security alerts displays the correct destination IP address			Need more clarity
191	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The proposed solution should provide alert details with mapping to the MITRE ATT&CK Framework to give more context for attack investigation and allow easier triaging			Need more clarity
192	Section 9 - Technical Specifications			**SSL Capabilities**	Does NPCI wants dedicated SSL solution for Network Anti-APT or are looking for built-in SSL decryption capabilities in Network Anti-APT? as the requirement point/clause mentioned below are typically available in dedicated SSL decryption solution.		Refer to corrigendum

193	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	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	Advanced attackers uses Webshell inject attacks to compromise Web Servers, would NPCI like to also have Webshell Attack detections capabilities? If yes please confirm and amend/modify the same to the requirement mentioned. For Example the clause can be modified as: ***"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 attempted data exfiltration & SSL/TLS handshake fingerprinting at the minimum"***		Refer to corrigendum
194	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Integrate with any existing Proxy solution of NPCI.	Please provide clarification on proxy and expectation on Integration with Proxy.		Should able to be deployed inline with proxy solution.
195	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	SSL functionality should be available on the proposed inline APT appliance	Duplicate to Point 93 which clearly states that the Anti-APT should have built-in SSL intercept capability which itself makes SSL inline to Network Anti-APT, unless NPCI is looking for dedicated SSL solution if yes, we would than propose dedicated SSL decryption appliance inline to Anti-APT.		Refer to corrigendum
196	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The solution must support TLS fingerprint detection detects malicious communication by TLS fingerprinting with JA3 between the client and server.	Very important point where Anti-APT solution should be able to detect malicious communication by TLS Fingerprinting with JA3 inbetween Client and Server. If it is good to have in that case NPCI may miss this capability provided by some of the Anti-APT solutions.		No change in RFP
197	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to automatically intercept all SSL/TLS based flows, also on other ports and protocols (not only HTTPS)	Please Clarify on the clause, as TCP ports have to be defined manually to automatically intercept SSL/TLS or HTTPS.		Refer to corrigendum
198	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Support multiple active-inline devices simultaneously	Please provide more clarification		Refer to corrigendum

199	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on source/destination ip/port	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
200	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on host/URL categorization	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
201	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on threat intelligence	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
202	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on CA status	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls? Also provide use case for the same		Refer to corrigendum
203	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on Subject / Domain Name	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
204	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on Cipher Suite and Key Strength	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
205	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	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?	Requirement depends on the port capability or external Active Failover Kit is required, Please confirm of NPCI needs external Bypass Kit to support the same?		Refer to corrigendum

206	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, SSL3, and SSL2 encryption protocols?	SSL stands for Secure Socket Layer while TLS stands for Transport Layer 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), Hashed Message Authentication Code protocol is used.** **3) SSL (Secure Socket Layer) is less**		Refer to corrigendum
207	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. Hence we request removal of point 112 as duplicated.		Refer to corrigendum
208	Section 9 - Technical 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
209	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 would compromise security.		Refer to corrigendum

210	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
211	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

212	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution must be available as on premise physical appliances with sandboxing capability	NPCI being an National Critical Infrastructure of India where 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 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 files to the cloud without NPCI's knowledge.		Refer to corrigendum
213	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	Proposed APT solution should perform advanced network detection and analysis of the enterprise's internal/External network data.	Clarification required, Should we read the clause as? ***"Proposed APT solution should perform advanced network detection and analysis of the enterprise's inbound/outbound network traffic."***		No change in RFP. Should able to perform detection on Intenal (east-west), External (inbound-outbound) traffic.

214	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should support to monitor traffic from multiple segments simultaneously on single appliance (East-West, North-South).	As per clause number 1 of the Technical Specifications the Network Anti-APT solution should be able to 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 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 connectivity for North-South traffic and East-West traffic is feasible or not.		Refer to corrigendum
215	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be dedicated appliance and should not be enabled as additional licensed solution with proposed perimeter gateway devices such as firewall, APT etc.	Similar to point 11 which is in more details, hence we request NPCI to remove this point as duplicate.		Refer to corrigendum

216	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	Security Vendor must have a Research/Labs organization and this organization must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild.	Reporting on Vulnerabilities is primary function of Vulnerability Assessment tools / Solution. 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 expliots / payloads. 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**".		Refer to corrigendum

217	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be able to detect any suspicious communication within and outside of Customer's network	Need for clarification on this point specifically Outside of Customers 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 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 carry their activity from compromised endpoints and move to servers, hiding their activities***		Refer to corrigendum
218	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The Proposed solution should be able to detect communications to known command and control centers.	We would like to highlight this requirement only mentions detection 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: ***"The Proposed solution should be able to detect communications to known & unknown command and control center initiated by internal infected clients."***		Refer to corrigendum

219	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be able to detect reputation of URL being accessed	Primarily this requirement falls in the category of Proxy Solution requirement where reputation of the 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 manner as attackers take advantage 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.		Refer to corrigendum
220	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	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: "The proposed solution for Network Ani-APT should prevent any C&C communications detected over North-South traffic regardless of ports and protocols"		Refer to corrigendum

221	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	Sandbox must have the ability to simulate the entire threat behavior.	*There are various flavors of Sandbox environment used for analysis and 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:* ***"The proposed solution must be 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 based on premise Virtual Execution Environment"***		Refer to corrigendum
222	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency	OEM Specific Clause. We request removal of the clause as the requirement gets addressed in detection of Zero-Day exploits targeting vulnerabilities in the wild in clause 19 and 20.		Refer to corrigendum

223	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should support Multiple protocols for inspection. Example:- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction: SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device	Advanced attackers once establish the foothold tries to move laterally and dump sophisticated tools on 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 request modification of the clause to 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 and objects that are transferred over HTTP, FTP like protocols and submit them to an automated***		Refer to corrigendum
224	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis	Duplicate point as all the previous clause covers the same. Request removal of the clause.		Refer to corrigendum

225	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.	Advanced attackers leverage various types of files to infiltrate in the target environment and not just executables, pdf, flash or RTF file 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, 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, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx,***		Refer to corrigendum

226	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and Exfiltration	In a sophisticated attack the advanced attackers may or may not use malware, but they definitely use 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 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 inspection, Packet flows, Signature matching and statistics i) Supports extensive metadata		Refer to corrigendum
227	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed APT must able to operate in Asymmetric traffic environment with Vulnerability / Exploit filters for protection	Analyzing asymmetric traffic results in ton's of false positive's and adds unnecessary workload on validation of such all the alerts resulting in Alert Fatigue on SOC team, hence we request removal of such clause which adds overheads to security team and miss on legitimate threats.		Refer to corrigendum
228	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed APT solution must support Adaptive Filter Configuration(AFC) which will alert or disable ineffective filter in case of noisy filters	OEM Specific IPS Solution, Request removal of this clause.		Refer to corrigendum
229	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	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	Duplicate Clause, Point 17 covers the requirement hence we request removal of this clause. Also it is important for Anti-APT solution to Block callback to C&C and malicious communications in inline mode.		Refer to corrigendum

230	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
231	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
232	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
233	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
234	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
235	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
236	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	The proposed APT must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score	Clause is OEM Specific IPS Solution & only covers known attacks, Request removal of this clause.		Refer to corrigendum
237	Section 9 - Technical Specifications	39	Annexure J - Technical Compliance	Must have the ability to correlate the monitored attacks to the APT filters number and recommended action	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

238	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
239	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.
240	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
241	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

242	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	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 Solution for faster report generation."***		Refer to corrigendum
243	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	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. **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
244	Section 9 - Technical Specifications	40	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

245	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.
246	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
247	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.
248	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

249	Section 9 - 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".
250	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.	Advanced attackers leverage various types of files to infiltrate in the target environment especially Webshell attacks on Web Servers and manipulate the server and redirect to malicious content. 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, in the benefit of NPCI we request 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 detection support for JSP, PHP, and WAR (Web archive) file types etc."***		Refer to corrigendum

251	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	Sandbox appliance should have redundant power supply, 2 TB or more storage capacity with dedicated management port	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
252	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The Proposed Solution should be able to detect known bad URL before sandboxing	Does NPCI only wants to detect known bad URL's only?		Refer to corrigendum
253	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The proposed solution should detect file-less malware tools used for extracting plain text passwords, hash, PIN codes and Kerberos tickets.	Attackers use encoded algorithms like XOR to hide password instead of plain text, do NPCI would like to detect and extract passwords which are encoded algorithm XOR instead of just plain text? If yes, We request you to modify the clause to: ***"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...."***		Refer to corrigendum
254	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The Proposed solution should allow Admin be able to inquire how many detections come from malicious password-protected files	Please provide clarification on the requirement.		Refer to corrigendum

255	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The Proposed Sandboxing solution must support of analysis of Windows & Linux Operating System files	In Advanced Threat Landscape the attacks are not limited to Windows & 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 C&C servers. 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."***		Refer to corrigendum
256	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The proposed solution should support X-Dst-Forwarded-For header, so that Network Security alerts displays the correct destination IP address			Need more clarity
257	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The proposed solution should provide alert details with mapping to the MITRE ATT&CK Framework to give more context for attack investigation and allow easier triaging			Need more clarity
258	Section 9 - Technical Specifications			**SSL Capabilities**	Does NPCI wants dedicated SSL solution for Network Anti-APT or are looking for built-in SSL decryption capabilities in Network Anti-APT? as the requirement point/clause mentioned below are typically available in dedicated SSL decryption solution.		Refer to corrigendum

259	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	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	Advanced attackers uses Webshell inject attacks to compromise Web Servers, would NPCI like to also have Webshell Attack detections capabilities? If yes please confirm and amend/modify the same to the requirement mentioned. For Example the clause can be modified as: ***"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 attempted data exfiltration & SSL/TLS handshake fingerprinting at the minimum"***		Refer to corrigendum
260	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Integrate with any existing Proxy solution of NPCI.	Please provide clarification on proxy and expectation on Integration with Proxy.		Should able to be deployed inline with proxy solution.
261	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	SSL functionality should be available on the proposed inline APT appliance	Duplicate to Point 93 which clearly states that the Anti-APT should have built-in SSL intercept capability which itself makes SSL inline to Network Anti-APT, unless NPCI is looking for dedicated SSL solution if yes, we would than propose dedicated SSL decryption appliance inline to Anti-APT.		Refer to corrigendum
262	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The solution must support TLS fingerprint detection detects malicious communication by TLS fingerprinting with JA3 between the client and server.	Very important point where Anti-APT solution should be able to detect malicious communication by TLS Fingerprinting with JA3 inbetween Client and Server. If it is good to have in that case NPCI may miss this capability provided by some of the Anti-APT solutions.		No change in RFP
263	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to automatically intercept all SSL/TLS based flows, also on other ports and protocols (not only HTTPS)	Please Clarify on the clause, as TCP ports have to be defined manually to automatically intercept SSL/TLS or HTTPS.		Refer to corrigendum
264	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Support multiple active-inline devices simultaneously	Please provide more clarification		Refer to corrigendum

265	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on source/destination ip/port	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
266	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on host/URL categorization	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
267	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on threat intelligence	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
268	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on CA status	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls? Also provide use case for the same		Refer to corrigendum
269	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on Subject / Domain Name	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
270	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on Cipher Suite and Key Strength	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
271	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	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?	Requirement depends on the port capability or external Active Failover Kit is required, Please confirm of NPCI needs external Bypass Kit to support the same?		Refer to corrigendum

272	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, SSL3, and SSL2 encryption protocols?	SSL stands for Secure Socket Layer while TLS stands for Transport Layer 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), Hashed Message Authentication Code protocol is used.** **3) SSL (Secure Socket Layer) is less**		Refer to corrigendum
273	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. Hence we request removal of point 112 as duplicated.		Refer to corrigendum
274	Section 9 - Technical 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
275	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 would compromise security.		Refer to corrigendum

276	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
277	**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.
278	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

279	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution must be available as on premise physical appliances with sandboxing capability	NPCI being an National Critical Infrastructure of India where 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 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 files to the cloud without NPCI's knowledge.		Refer to corrigendum
280	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	Proposed APT solution should perform advanced network detection and analysis of the enterprise's internal/External network data.	Clarification required, Should we read the clause as? ***"Proposed APT solution should perform advanced network detection and analysis of the enterprise's inbound/outbound network traffic."***		No change in RFP. Should able to perform detection on Intenal (east-west), External (inbound-outbound) traffic.

281	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should support to monitor traffic from multiple segments simultaneously on single appliance (East-West, North-South).	As per clause number 1 of the Technical Specifications the Network Anti-APT solution should be able to 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 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 connectivity for North-South traffic and East-West traffic is feasible or not.		Refer to corrigendum
282	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be dedicated appliance and should not be enabled as additional licensed solution with proposed perimeter gateway devices such as firewall, APT etc.	Similar to point 11 which is in more details, hence we request NPCI to remove this point as duplicate.		Refer to corrigendum

283	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	Security Vendor must have a Research/Labs organization and this organization must contribute and report on finding new Zero-Day vulnerabilities being exploited in the wild.	Reporting on Vulnerabilities is primary function of Vulnerability Assessment tools / Solution. 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 expliots / payloads. 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**".		Refer to corrigendum

284	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be able to detect any suspicious communication within and outside of Customer's network	Need for clarification on this point specifically Outside of Customers 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 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 carry their activity from compromised endpoints and move to servers, hiding their activities***		Refer to corrigendum
285	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The Proposed solution should be able to detect communications to known command and control centers.	We would like to highlight this requirement only mentions detection 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: ***"The Proposed solution should be able to detect communications to known & unknown command and control center initiated by internal infected clients."***		Refer to corrigendum

286	Section 9 - Technical Specifications	37	Annexure J - Technical Compliance	The proposed solution should be able to detect reputation of URL being accessed	Primarily this requirement falls in the category of Proxy Solution requirement where reputation of the 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 manner as attackers take advantage 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.		Refer to corrigendum
287	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	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: "The proposed solution for Network Ani-APT should prevent any C&C communications detected over North-South traffic regardless of ports and protocols"		Refer to corrigendum

288	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	Sandbox must have the ability to simulate the entire threat behavior.	*There are various flavors of Sandbox environment used for analysis and 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:* ***"The proposed solution must be 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 based on premise Virtual Execution Environment"***		Refer to corrigendum
289	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should have an built-in document vulnerabilities detection engine to assure analysis precision and analysis efficiency	OEM Specific Clause. We request removal of the clause as the requirement gets addressed in detection of Zero-Day exploits targeting vulnerabilities in the wild in clause 19 and 20.		Refer to corrigendum

290	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should support Multiple protocols for inspection. Example:- HTTP, FTP, SMTP, SNMP, IM ,IRC,DNS and P2P protocols Internal direction: SMB ,Database protocol (MySQL, MSSQL, Oracle) on a single device	Advanced attackers once establish the foothold tries to move laterally and dump sophisticated tools on 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 request modification of the clause to 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 and objects that are transferred over HTTP, FTP like protocols and submit them to an automated***		Refer to corrigendum
291	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The Proposed solution should have a Co-relation engine to automatically co-relate across multiple protocol, multiple sessions and volume traffic analysis	Duplicate point as all the previous clause covers the same. Request removal of the clause.		Refer to corrigendum

292	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed solution should be able to detect and prevent the persistent threats which come through executable files, PDF files , Flash files, RTF files and and/or other objects.	Advanced attackers leverage various types of files to infiltrate in the target environment and not just executables, pdf, flash or RTF file 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, 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, asf, chm, com, dll, doc, docx, exe, gif, hip, htm, ico, jar, jpeg, jpg, mov, mps, mp4, pdf, png, ppsx,***		Refer to corrigendum

293	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The Proposed solution should be able to generate out of box reports to highlight Infections, C&C behavior, Lateral Moment, Asset and data discovery and Exfiltration	In a sophisticated attack the advanced attackers may or may not use malware, but they definitely use 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 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 inspection, Packet flows, Signature matching and statistics i) Supports extensive metadata		Refer to corrigendum
294	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed APT must able to operate in Asymmetric traffic environment with Vulnerability / Exploit filters for protection	Analyzing asymmetric traffic results in ton's of false positive's and adds unnecessary workload on validation of such all the alerts resulting in Alert Fatigue on SOC team, hence we request removal of such clause which adds overheads to security team and miss on legitimate threats.		Refer to corrigendum
295	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	The proposed APT solution must support Adaptive Filter Configuration(AFC) which will alert or disable ineffective filter in case of noisy filters	OEM Specific IPS Solution, Request removal of this clause.		Refer to corrigendum
296	Section 9 - Technical Specifications	38	Annexure J - Technical Compliance	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	Duplicate Clause, Point 17 covers the requirement hence we request removal of this clause. Also it is important for Anti-APT solution to Block callback to C&C and malicious communications in inline mode.		Refer to corrigendum

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	Annexure J - Technical Compliance	The proposed APT must be able to control the known bad host such as spyware, botnet C2 server, spam and so on based on country of origin, exploit type and the reputation score	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	Must have the ability to correlate the monitored attacks to the APT filters number and recommended action	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	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 Solution for faster report generation."***		Refer to corrigendum
310	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	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. **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	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

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

316	Section 9 - 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".
317	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.	Advanced attackers leverage various types of files to infiltrate in the target environment especially Webshell attacks on Web Servers and manipulate the server and redirect to malicious content. 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, in the benefit of NPCI we request 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 detection support for JSP, PHP, and WAR (Web archive) file types etc."***		Refer to corrigendum

318	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	Sandbox appliance should have redundant power supply, 2 TB or more storage capacity with dedicated management port	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
319	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The Proposed Solution should be able to detect known bad URL before sandboxing	Does NPCI only wants to detect known bad URL's only?		Refer to corrigendum
320	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The proposed solution should detect file-less malware tools used for extracting plain text passwords, hash, PIN codes and Kerberos tickets.	Attackers use encoded algorithms like XOR to hide password instead of plain text, do NPCI would like to detect and extract passwords which are encoded algorithm XOR instead of just plain text? If yes, We request you to modify the clause to: ***"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...."***		Refer to corrigendum
321	Section 9 - Technical Specifications	40	Annexure J - Technical Compliance	The Proposed solution should allow Admin be able to inquire how many detections come from malicious password-protected files	Please provide clarification on the requirement.		Refer to corrigendum

322	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The Proposed Sandboxing solution must support of analysis of Windows & Linux Operating System files	In Advanced Threat Landscape the attacks are not limited to Windows & 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 C&C servers. 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."***		Refer to corrigendum
323	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The proposed solution should support X-Dst-Forwarded-For header, so that Network Security alerts displays the correct destination IP address			Need more clarity
324	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The proposed solution should provide alert details with mapping to the MITRE ATT&CK Framework to give more context for attack investigation and allow easier triaging			Need more clarity
325	Section 9 - Technical Specifications			**SSL Capabilities**	Does NPCI wants dedicated SSL solution for Network Anti-APT or are looking for built-in SSL decryption capabilities in Network Anti-APT? as the requirement point/clause mentioned below are typically available in dedicated SSL decryption solution.		Refer to corrigendum

326	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	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	Advanced attackers uses Webshell inject attacks to compromise Web Servers, would NPCI like to also have Webshell Attack detections capabilities? If yes please confirm and amend/modify the same to the requirement mentioned. For Example the clause can be modified as: ***"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 attempted data exfiltration & SSL/TLS handshake fingerprinting at the minimum"***		Refer to corrigendum
327	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Integrate with any existing Proxy solution of NPCI.	Please provide clarification on proxy and expectation on Integration with Proxy.		Should able to be deployed inline with proxy solution.
328	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	SSL functionality should be available on the proposed inline APT appliance	Duplicate to Point 93 which clearly states that the Anti-APT should have built-in SSL intercept capability which itself makes SSL inline to Network Anti-APT, unless NPCI is looking for dedicated SSL solution if yes, we would than propose dedicated SSL decryption appliance inline to Anti-APT.		Refer to corrigendum
329	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	The solution must support TLS fingerprint detection detects malicious communication by TLS fingerprinting with JA3 between the client and server.	Very important point where Anti-APT solution should be able to detect malicious communication by TLS Fingerprinting with JA3 inbetween Client and Server. If it is good to have in that case NPCI may miss this capability provided by some of the Anti-APT solutions.		No change in RFP
330	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to automatically intercept all SSL/TLS based flows, also on other ports and protocols (not only HTTPS)	Please Clarify on the clause, as TCP ports have to be defined manually to automatically intercept SSL/TLS or HTTPS.		Refer to corrigendum
331	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Support multiple active-inline devices simultaneously	Please provide more clarification		Refer to corrigendum

332	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on source/destination ip/port	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
333	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on host/URL categorization	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
334	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on threat intelligence	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
335	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on CA status	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls? Also provide use case for the same		Refer to corrigendum
336	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on Subject / Domain Name	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
337	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Ability to configure encryption/decryption policy (incl. block/pass-through) based on Cipher Suite and Key Strength	These requirements can only be supported with dedicated SSL interception solution, We request NPCI to confirm if they need dedicated SSL interception solution to provide granular controls?		Refer to corrigendum
338	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	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?	Requirement depends on the port capability or external Active Failover Kit is required, Please confirm of NPCI needs external Bypass Kit to support the same?		Refer to corrigendum

339	Section 9 - Technical Specifications	41	Annexure J - Technical Compliance	Support TLS 1.0, TLS 1.1, TLS 1.2, TLS 1.3, SSL3, and SSL2 encryption protocols?	SSL stands for Secure Socket Layer while TLS stands for Transport Layer 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), Hashed Message Authentication Code protocol is used.** **3) SSL (Secure Socket Layer) is less**		Refer to corrigendum
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. Hence we request removal of point 112 as duplicated.		Refer to corrigendum
341	Section 9 - Technical 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 would compromise security.		Refer to corrigendum

343	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