Corrigendum to the RFP for "Cloud Based Web Proxy Solution" (*RFP No. NB.HO.DIT/1470/DIT-012-26/201-20) dated 10 January 2020*

S. No.	RFP Page No.	Clause No. / Clause Pertaining to	RFP Clause	Revised Clause
1	18	18	The Bidder shall provide training ……	The bidder shall provide a minimum of 3 days training at NABARD Head Office, to 6 personnel identified by the bank on functional, operational and reporting aspects of the Cloud Based web proxy solution. The training material covering various aspects of the solution and the different reports available will also have to be provided in English. The cost may be indicated in the Commercial Bid Form.
2	19	28	The solution should be capable of …	The solution should be capable of managing Cross-origin resource sharing (CORS) requests.
3	19	36	Solution to provide forensic evidence….	Solution should provide forensic evidence on the infections activity from the network
4	26	3 (iv)	The Bidder shall also submit a "On-Demand" ……	The bidder shall obtain an "On-Demand" Vulnerability Testing Report of the solution from the OEM at least once in six months along with the mitigation measures implemented for the same.
5	56	7	The format for certificate, to be …….	The format for certificate, to be submitted, is provided in Annexure-I. Necessary documents (Like PO) should be attached. Email confirmation from the customer, directly sent to dit@nabard.org, confirming the implementation, may also be arranged. Contact details of the customer will also have to be shared with NABARD.
6	91	SLA	"M/s_____, a company incorporated under the provisions of the Companies Act,…….	M/s_____, a company incorporated under the provisions of the Companies Act, 1956 and having its registered office at _____, together with its Affiliates and represented herein by its Authorised Signatory, _____hereinafter referred to as "M/s_____", (which expression shall mean and unless repugnant to the context, includes its successors in business, legal

				representatives and administrators or permitted assigns) of OTHER PART."	
7	93	2.1.3	The SI onsite engineer, along with the TAM of the OEM shall do…….	The SI onsite engineer, along with the TAM of the OEM shall do a "knowledge transfer" to the identified officers of NABARD and engineers of our IT services management vendor during the last month of support to ensure smooth takeover of the operations and management of the **cloud based web-proxy solution.**	
<u>Modifications in Annexure – L (Technical Bid Form).</u>					
8	64	10	Solution should provide caching functionality.	This point is removed.	Please see the Annexure on Revised Technical Bid Form on next page.
9	65	16	The solution should have a large number of websites in its URL filtering……	This point is removed from "Must Have" category and marks have been stipulated in 2 heads viz. 90+ and 100+ predefined categories.	
10	69	40,43,44	The solution should have the capability to manage….	These points have been merged.	

ANNEXURE

Annexure - L
Technical Bid Form

S.No.	Compliance to Technical Specifications	Compliance (Y/N)	Remark if any	Total Marks Allotted by NABARD	Marks Scored by the Bidder (To be calculated by NABARD)	Must Have (Yes / No)
Part A	**General Specifications**			**9.5(Total of the section)**		
1	Solution should provide quickly enforcing of policies for network access and use.			1		
2	Solution should instantly report on web threats and user activities.			1.5		
3	The solution should have a simple control mechanism to deny all traffic control to deactivate all internet services to be used in case of an outbreak, hacking attempt, etc.			1		
4	The agent on the roaming user machines should be tamperproof, for example, the agent cannot be uninstalled by the user even with admin rights to the system or the user cannot stop the services.			5		Yes
5	The Solution should be able to work with: i) Microsoft › Windows 7,8,10 (32-bit and 64-bit) (NABARD has some systems on other OS as well and supporting the endpoints on the same will be an added advantage) ii) Apple Macintosh › OS X 10.6 to 10.14			1		

	Agent installed should be browser independent to support frequent browsers version updates					
Part B	**Deployment Mode**			**10.5(Total of the section)**		
6	User authentication should happen using AD mechanism which helps single sign on. Solution should be capable to provide email based binding to end machine for users who are not part of AD			1		
7	The proposed solution should support to monitor traffic from multiple segments like WAN, DMZ, Wi-Fi network, MPLS links etc. simultaneously.			1.5		
8	The solution should have complete license for web security, Antivirus, SSL, and content inspection. The Solution should intercept user requests for web destinations (HTTP, HTTPs) for web security and in-line AV scanning.			5		Yes
9	The solution should provide real-time Analysis for Advanced Threat Protection via defence assessment areas, using a composite scoring and predictive analysis. Multiple real-time content engines analyze full web page content, active scripts, web links, contextual profiles, files and executables			1.5		
10	The solution should have support for two factor Authentication for login to console			1.5		

Part C	URL Filtering and Content Analysis			15 (Total of this Section)		
11	Solution should have strong Content filtering database. Solution should provide real time threats updates, new signatures and URL database like blacklisted Phishing, Malicious sites, Porn sites, terrorist sites, Religion based sites, Gambling sites, hacking sites, anonym zing websites, anonymizing tools, anonymizing proxies, advanced malware command and control, advanced malware payloads, C& C, Bot networks, Compromised websites, key loggers, Ransomware detection and other frauds etc. Also in-addition solution should have ability to configure custom categories for the organization.			5		Yes
12	Solution should have web protection mechanism to identify and block web pages having malicious java script, VB script, executable, malicious or unauthorized ActiveX applications, potentially harmful programs or software`s download and shareware including cross sub site access.			1		
13	Solution should be able to provide safe search, application blocking, URL re- categorization option.			1.5		
14	The solution should be capable of dynamically blocking a legitimate website which has become infected and unblock the site in real time when the threat has been removed for below mentioned			1		

	security categories and vulnerabilities.					
15	The solution should have a large number of websites in its URL filtering database and' should have pre-defined URL categories and application protocols along with YouTube, Facebook and linked-in controls. Solution vendor should ensure that 90+ predefined categories & 100+ pre-defined protocols/application control categories should be available on product from day-1. Also in-addition solution should have ability to configure custom categories for organization.			5 (Up to 100 predefined categories: **3** More than 100 predefined categories: **5)**		
16	The solution in addition to category based filtering should support reputation based technology. It should have the capability to provide reputation based analysis on the security risk posed, enabling administrators to apply very granular rules about what to permit or deny.			1.5		
Part D	**SSL Capabilities**			**2(Total of this section)**		
17	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.			2		

Part E	**Anti-Virus and Anti-Malware**			**11.5(Total of this section)**		
18	Solution to provide Network-level Anti-Virus and Anti-Malware inspection and prevention			5		Yes
19	Solution to provide forensic evidence on the infections activity within the network as follow: Event time stamp, network events in sequence, packet capture of suspicious communication, malware behaviors, malware type, severity, source and destination of attack.			1.5		
20	The solution must support different types of compression algorithms and scan nested compressed files.			1		
21	The solution should have efficient anti-malware engines			1		
22	The solution should have capabilities to inspect malware embedded in PDF, word, PPT files.			1		
23	Solution must offer the customized White-List/Black-List, capabilities and file reputation analysis to block the Advance Threat.			2		
Part F	**Access logs and Reporting**			**15.5(Total of the section)**		
24	The solution should log all the events and be configurable to generate report.			1		
25	Solution should provide advanced threat dashboard to track the infection or threat history for User/IP, with the ability to access all forensic evidence for past			2		

	infections. (at least 6 months)					
26	Solution should have built in various reports and should be able to create custom reports like Executive report, Investigative report, Top 10 reports for various category and Health reports etc.			5		Yes
27	Solution should be able to schedule reports and also provide the flexibility to generate on-demand reports in daily/weekly/monthly/yearly or specific range (by day and time).			2		
28	The solution must support granular access control and authorization to facilitate gathering of logs of users access			1		
29	The solution should create custom reports on a granular and/or enterprise level such a s (but not limited to): - Usage Report of Specific User/IP/Group based on Time/Date - Report for all users who have been accessed the specific URL - Usages report based on Time & Date - Top service user - Most requested service			1.5		
30	The solution should have capabilities to automatically deliver reports based on schedule to selected recipients. The solution should support custom report creation in Excel and PDF.			2		
31	The solution should report incident with URL category information along with user, IP, web content violating policy etc.			1		

Part G	**General Features and Policies**			**8.5 (Total of the section)**		
32	Multiple accesses provisioning for same user using single policy instead of creating multiple policies or multiple access control lists for same user and IP			1		
33	Solution should be able to apply same policies / restrictions even when the user is connecting to Internet through dongle, wifi, hotspot, etc.			1		
34	Solution provider should have at least 2 data centres with at least 1 primary data centre being in India.			5		Yes
35	Solution should support visibility and control on data movement via compliance(PII,PCI)/key word based policy			1.5		
Part H	**User Control and Management**			**10.5(Total of this section)**		
36	The solution should have granular control over popular social web applications like Facebook, LinkedIn, Twitter, YouTube, and others. The solution should have social control Video UPLOADS to Facebook and YouTube applications.			1		
37	The solution should have the ability to create user defined URL Category.			1.5		
38	The solution should enable roaming user to browse content originating from a specific geolocation, regardless of the user's location.			1		

39	The solution should have the capability to manage internet access for specific user/ users/ group/ groups/ client/ clients to access internet on specific / Day/ Date/ Weekly/ Monthly etc. The solution should provide authenticated session control to configure how long users can browse once authenticated and it should be able to restrict User to access internet, during specified hours.			2		
40	The solution should allow internet access only after user authentication and authorization			1		
41	The solution should provide customizable (but not limited to) - default error pages, - Messages to users, - Alerts.			1		
42	The solution should support real time graphical and chart based dashboard for the summary of activities over Web.			1		
43	Solution should be able to restrict Users to download certain file types based on extension.			1		
44	Solution should have capabilities to configure User, IPs, URLs and Domains to Black list or white list/ exceptions for detections			1		
Part I	**Integrations with other solutions**			**17.5 (Total of this section)**		
45	The solution provide cloud application visibility and control as the part of the solution .			1.5		
46	CASB solution integration should be possible in future from the same / other OEM.			1		

47	Cloud based proxy solution should co-exist with Next Generation Firewalls, SDWAN solutions (At present Checkpoint and Fortinet Firewalls deployed in the Bank. In future SDWANs will also be deployed, therefore the solution must seamlessly co-exist with SDWAN as well).			5		Yes
48	The solution should work with the local breakout of internet i.e. centralization of internet must not be a prerequisite.			5		Yes
49	Solution should be integrated with SIEM tools like RSA.			5		Yes
Part J	**Cloud Web Security Administrator and Management**			**7(Total of this section)**		
50	The solution should have the capability of blocking the malicious cloud app (if such requirement arises).			2		
51	Solution should have centralized architecture with web or GUI based dashboard console to monitor, reporting, notification, maintaining and policy push for the registered users centrally.			1		
52	Solution shall support role-based administration such as Administrator and Read-only access user.			1		
53	The solution must detect and protect against anonymizing websites and anonymizing tools.			1		
54	The solution should provide multiple methods for deploying the solution via the Proxy dependent Endpoint ,Direct Access Endpoint, IPSEC and also GRE.			2		

Part K	**Support by Bidder and OEM**			**2.5(Total of this section)**		
55	Solution should have own or tie up with Global Threat Intelligent Network to protect from Zero day attack, blended threats, Botnet, Trojan, Malwares communication, Spywares, Pharming attack (traffic includes compressed files.)			1		
56	The bidder should have a 24x7 365 days support contact center in order to log the calls. The contact center numbers should be provided to the Bank along with the escalation matrix mentioning the contact person's name, number and designation in the company			1.5		
Part L	**Certification and License**			**3(Total of this section)**		
57	The solution should have CSA STAR , ISO 27000 series and SOC 1,2,3 certifications for NOC , development and production environment.			3		

----------End of Document----------