

Design, development, integration, implementation, operation and maintenance of National Logistics Portal (Marine)

Indian Ports Association (IPA)

Design, development, integration, implementation, operation and maintenance of National Logistics Portal (Marine)

RFP No.: IPA/PGAV/NLP-Marine/2020

Dated 28-09-2020

Corrigendum No.: IPA/PGAV/NLP-Marine/2020/Corrigendum-X

Dated 17-12-2020

Design, development, integration, implementation, operation and maintenance of National Logistics Portal (Marine)

Contents

Modification/ Clarification in RFP/ Corrigendum	3
--	----------

Modification/ Clarification in RFP/ Corrigendum

S. No.	RFP/Corrigendum reference	Changes requested by the bidder	Response (Modification/ Clarification)
1.	<p>3.4.2.1 Single Window Certification System (NLPRFPVol2.pdf)</p> <p>This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application</p>	<p>Remarks:</p> <p>1. Our understanding is that this is the requirements for Listing module in NLP Marine portal (not mobile application). Please confirm</p> <p>2. Is there any mobile requirement for Listing module?</p>	<p>Modification</p> <p>National Logistics Portal (NLP MARINE) mobile application may be read as National Logistics Portal (NLP MARINE) mobile application/ Portal</p>
2.	<p>3.4.2.2 Common Application Form (CAF) module (NLPRFPVol2.pdf)</p> <p>This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application</p>	<p>Remarks:</p> <p>1. Our understanding is that this is the requirements for Listing module in NLP Marine portal (not mobile application). Please confirm</p> <p>2. Is there any mobile requirement for CAF module?</p>	<p>Modification</p> <p>Pls refer to S.No.1</p>
3.	<p>3.4.2.3 Payments Module (NLPRFPVol2.pdf)</p> <p>This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application</p>	<p>Remarks:</p> <p>1. Our understanding is that this is the requirements for Payments module in NLP Marine portal (not mobile application). Please confirm</p> <p>2. Is there any mobile requirement for Payments module?</p>	<p>Modification</p> <p>Pls refer to S.No.1</p>
4.	<p>3.4.2.3 Payments Module (NLPRFPVol2.pdf)</p> <p>This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application</p>	<p>Remarks:</p> <p>1. Our understanding is that this is the requirements for EPC/PGA Interface module in NLP Marine portal (not mobile application). Please confirm</p> <p>2. Is there any mobile requirement for EPC/PGA Interface module?</p>	<p>Modification</p> <p>Pls refer to S.No.1</p>

S. No.	RFP/Corrigendum reference	Changes requested by the bidder	Response (Modification/ Clarification)
5.	<p>3.4.2.3 Payments Module (NLPRFPVol2.pdf)</p> <p>This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application</p>	<p>Remarks:</p> <p>1. Our understanding is that this is the requirements for Generated Certificates Module in NLP Marine portal (not mobile application). Please confirm</p> <p>2. Is there any mobile requirement for Generated Certificates Module?</p>	<p>Modification</p> <p>Pls refer to S.No.1</p>
6.	<p>3.4.3.1 Trade Finance Platform (NLPRFPVol2.pdf)</p> <p>This section presents the key and minimum functional requirements specifications for the National Logistics Portal (NLP MARINE) Mobile Application</p>	<p>Remarks:</p> <p>1. Our understanding is that this is the requirements for Trade Finance Module in NLP Marine portal (not mobile application). Please confirm</p> <p>2. Is there any mobile requirement for Trade Finance Module?</p>	<p>Modification</p> <p>Pls refer to S.No.1</p>
7.	<p>Corrigendum-V, page 77 Anti-APT (File, Network, Email, Endpoints)</p> <p>a. The Solution shall have ability to detect malicious traffic in Network, Email, Web and Endpoints</p> <p>b. The solution shall be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, targeted Advanced Persistent Threat etc without relying on just Signature database</p> <p>c. The solution shall perform dynamic real-time analysis of advanced malware on the solution itself to confirm true zero-day and targeted attacks</p> <p>d. The solution shall automatically detect and confirm multistage zero-day malware and targeted attacks without prior knowledge of the malware</p> <p>e. The solution shall utilize a state-full attack</p>	<p>Following points may be deleted:</p> <p>h. The solution must be able to perform a pre-assessment scan of the file server</p> <p>j. The solution shall provide ability to create a quarantine share/folder and move malicious files to that share/folder as well as the ability to create a good share/folder and the ability to move clean files to that share/folder</p> <p>l. The solution must support typo-squatting attack detection for all sender domain & URL domain in email body.</p>	<p>Modification</p> <p>a. The Solution shall have ability to detect malicious traffic in Network, Email, Web and Endpoints</p> <p>b. The solution shall be able to detect and prevent advanced Malware, Zero-day attack, spear phishing attack, targeted Advanced Persistent Threat, Malicious attachments and/or attacks on URL domain, etc. without relying on just Signature database</p> <p>c. The solution shall perform dynamic real-time analysis of advanced malware on the solution itself to confirm true zero-day and targeted attacks</p> <p>d. The solution shall automatically detect and confirm multistage zero-day malware and targeted attacks without prior</p>

S. No.	RFP/Corrigendum reference	Changes requested by the bidder	Response (Modification/ Clarification)
	<p>analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack</p> <p>f. The solution shall capture, and store packet captures of traffic relevant to the analysis of detected threats</p> <p>g. The solution shall have the ability to be on-demand scanning and continuous scanning</p> <p>h. The solution must be able to perform a pre-assessment scan of the file server</p> <p>i. The solution shall have the ability to scan and analyse emails to identify malicious attachments or URLs in real-time and quarantine emails with malicious attachments or URLs</p> <p>j. The solution shall provide ability to create a quarantine share/folder and move malicious files to that share/folder as well as the ability to create a good share/folder and the ability to move clean files to that share/folder</p> <p>k. The solution shall provide visibility into scan histories of each file scanned that are aborted, completed, or in progress</p> <p>l. The solution must support typo- squatting attack detection for all sender domain & URL domain in email body.</p> <p>m. The solution may have capability to identify the payload information of APT including the origination and code information</p>		<p>knowledge of the malware</p> <p>e. The solution shall utilize a state-full attack analysis to detect the entire infection lifecycle, and trace the stage-by-stage analysis of an advanced attack.</p> <p>f. The solution shall capture, and store packet captures of traffic relevant to the analysis of detected threats</p> <p>g. The solution shall have the ability to be on-demand scanning and continuous scanning</p> <p>h. The solution must be able to perform a pre-assessment scan of the file.</p> <p>i. The solution shall have the ability to scan and analyse emails to identify malicious attachments or URLs in real-time and quarantine emails with malicious attachments or URLs</p> <p>j. The solution shall provide ability to create a quarantine share/folder and move malicious files to that share/folder as well as the ability to create a good share/folder and the ability to move clean files to that share/folder</p> <p>k. The solution shall provide visibility into scan histories of each file scanned that are aborted, completed, or in progress</p> <p>l. The solution may have capability to identify the payload information of APT</p>

S. No.	RFP/Corrigendum reference	Changes requested by the bidder	Response (Modification/ Clarification)
			including the origination and code information
8.	<p>Corrigendum-V, page 79 Web Gateway</p> <p>a. The solution shall have ability to share most types of Internet connections effortlessly, allowing multiple users to simultaneously surf the web, retrieve their email, or chat with online messaging, as if they were directly connected to the Internet</p> <p>b. The solution shall have ability to handle requests from a wide variety of Web applications and Internet protocols, such as Web browsers, Messaging software, FTP and SSL and shall also support Real Time Streaming Audio/ Video</p> <p>c. The solution shall have ability to enforce advanced and flexible access-control and acceptable user policies for IPA</p> <p>d. The solution shall have ability to monitor usage in real time, and maintain per-user and per-service audit logs</p> <p>e. The solution shall have ability to stop viruses, spam and inappropriate content from entering the network</p> <p>f. The solution shall have ability to protect servers from internal or external threats</p> <p>g. The solution shall have ability to support user database and policies so that the administrators alike can limit and control users' access to the web</p> <p>h. The solution shall have ability for logging, auditing, and a real-time activity and history viewer - detailed records of user activities</p> <p>i. The solution shall have ability to provide for ways to block/ control access to all executable</p>	<p>Following points may be modified as below:</p> <p>l. The solution shall have ability to support scheduling priority i.e. Allow to make certain services respond more quickly than others by giving a higher priority to the forwarding of packets related to that service. bandwidth limits for particular URL categories</p> <p>m. The solution shall be capable on compression of static as well as perform on-demand compression of dynamically generated responses before sending them over the network</p> <p>n. The solution shall support caching and inspection of traffic which is compressed. It shall do so by decompressing the content, followed by inspection and caching (if required) and shall allow flexibility of sending the decompressed content to the end user. The solution shall also support send the compressed content to the end user.</p>	<p>Modification</p> <p>a. The solution shall have ability to share most types of Internet connections effortlessly, allowing multiple users to simultaneously surf the web, retrieve their email, or chat with online messaging, as if they were directly connected to the Internet</p> <p>b. The solution shall have ability to handle requests from a wide variety of Web applications and Internet protocols, such as Web browsers, Messaging software, FTP and SSL and shall also support Real Time Streaming Audio/ Video</p> <p>c. The solution shall have ability to enforce advanced and flexible access-control and acceptable user policies for IPA</p> <p>d. The solution shall have ability to monitor usage in real time, and maintain per-user and per-service audit logs</p> <p>e. The solution shall have ability to stop viruses, spam and inappropriate content from entering the network</p> <p>f. The solution shall have ability to protect servers from internal or external threats</p> <p>g. The solution shall have ability to support user database and policies so that the administrators alike can limit and control users' access to the web</p>

S. No.	RFP/Corrigendum reference	Changes requested by the bidder	Response (Modification/ Clarification)
	<p>content</p> <p>j. The solution shall have ability to provide granular access control to file downloads through file extension</p> <p>k. The solution shall have ability to provide inbound and outbound access control on User-based or group-based access policy</p> <p>l. The solution shall have ability to support scheduling priority i.e. Allow to make certain services respond more quickly than others by giving a higher priority to the forwarding of packets related to that service. bandwidth limits for particular URL categories</p> <p>m. The solution shall be capable on compression of static as well as perform on-demand compression of dynamically generated responses before sending them over the network</p> <p>n. The solution shall support caching and inspection of traffic which is compressed. It shall do so by decompressing the content, followed by inspection and caching (if required) and shall allow flexibility of sending the decompressed content to the end user. The solution shall also support send the compressed content to the end user</p>		<p>h. The solution shall have ability for logging, auditing, and a real-time activity and history viewer - detailed records of user activities</p> <p>i. The solution shall have ability to provide for ways to block/ control access to all executable content</p> <p>j. The solution shall have ability to provide granular access control to file downloads through file extension</p> <p>k. The solution shall have ability to provide inbound and outbound access control on User-based or group-based access policy</p> <p>l. The solution shall have the ability to support scheduling priority and bandwidth limits for particular URL categories.</p> <p>m. The solution shall be capable on compression of static as well as perform on-demand compression of dynamically generated responses before sending them over the network</p> <p>n. The solution shall support caching and inspection of traffic which is compressed</p>
9.	Corrigendum-V, page 87 Two Factor Authentication	Two factor access control shall be provided for the initial registration and update of the IPA accounts.	<p>Modification</p> <p>Two factor access control shall be provided for the initial registration and update of the IPA Accounts. Minimum of Two Factor Authentication (2FA) with scalability to</p>

S. No.	RFP/Corrigendum reference	Changes requested by the bidder	Response (Modification/ Clarification)
			provision Multifactor Authentication (MFA) shall be provided.
10.	RFP Volume 2 page 144 8.2.1 Functional Requirement of Cloud	Database and Allied Services: Cloud services provider shall provide services like Database as a service (both RDBMS and No SQL), SMTP and SMS, DNS, Data warehouse, Storage, Analytics, Message queuing etc.	Modification Database and Allied Services: Cloud services provider shall provide services like Database as a service (both RDBMS and No SQL), SMTP and SMS, DNS, Recursive DNS Security , Data warehouse, Storage, Analytics, Message queuing, etc for its scope.
11.	Corrigendum-VIII, S. No. 3, Page 4 Bidder shall be awarded marks as long as the ranking is under the NIRF ranking category as per the relevant degree mentioned, irrespective of the year of obtaining the degree. It may be further clarified; bidder shall be awarded marks as long as it is under NIRF rankings. The link for NIRF ranking is: https://www.nirfindia.org/2020/Ranking2020.html	Changes suggested in Corrigendum-V across all resource profiles B1 – B10; in Annexure 1.2 technical bid evaluation; Clause 4.6 vol 1, Page no 39 – 53, are clear and the same should be followed.	Clarification For sake of absolute clarity, marking system as formulated in Corrigendum-V, shall prevail.