بسم الله الرحمن الرحيم

ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

ބީލަން ފޮމް

ޕްރޮޖެކްޓް ނަން	އެސްޑީ ވޯން (SD-WAN) ސޮލިއުޝަން ޑިޕްލޮއި ކޮށްދޭނެ ފަރާތެއް ހޯދުން
ޕްރޮޖެކްޓް ނަންބަރު	PROC-2023-01
އިޢުލާން ނަންބަރު	(IUL) 164-PRO/1/2023/94
ތާރީޚް	*24 އޯގަސްޓް 2023*

ސެކްޝަން 1.	ބީލަމާއި ގުޅޭ އާންމު މައުލޫމާތު	
1.1. ތައާރަފު	މިއީ މިއިދާރާއަށް ގެންނަން ބޭނުންވާ/ ހިދުމަތެއް ހޯދުމަށް ކުރެވޭ އާންމު އިއުލާނެކެވެ.	
1.2. އިއުލާން	ނަންބަރު	(IUL) 164-PRO/1/2023/94
	އިއުލާން ތާރީޚް	24 އޮގަސްޓު 2023
	ބީލަމުގެ ނަން	ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީއަށް ބޭނުންވާ އެސްޑީ ވޭން (SD-WAN) ސަބްސްކްރިޕްޝަން ޑެލިވަރީ ކޮންޓްރެކްޓް ފަރާތެއް ހޯދުން
1.3. ބީލަން ހުށަހެޅުން	ތަން	ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ
	އެޑްރެސް	NCIT ބިލްޑިންގ، 64 ނރ ކޯރި، ކަލާފާނު ހިނގުން
	ތާރީޚާއި ގަޑި	2023 ސެޕްޓެމްބަރ 12 ވާ އަންގާރަ ދުވަހުގެ 10:00 ގެ ކުރިން NCITގެ ރިސެޕްޝަނަށް. ގަޑިޖެހުމަށްފަހު ހުށަހަޅާ ބީލަންތައް ބަލައެއް ނުގަނެވޭނެއެވެ. އަދި އެޑްވާންސް ސަބަބަކާހުރެ މިދުވަސް (2023 ސެޕްޓެމްބަރ 12 ވާ އަންގާރަ) ބަންދުނަމަ، ޖެހިގެން އަންނަ ރަސްމީ ދުވަހު 10:00ގެ ކުރިން NCIT ގެ ރިސެޕްޝަނަށް ބީލަން ހުށަހަޅަންވާނެއެވެ. އަދި ގަޑިޖެހުމަށްފަހު ހުށަހަޅާ ބީލަންތައް ބަލައެއް ނުގަނެވޭނެއެވެ.
1.4. ބީލަން ހުޅުވުން	ތަން	ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ
	އެޑްރެސް	NCIT ބިލްޑިންގ، 64 ނރ ކޯރި، ކަލާފާނު ހިނގުން
	ތާރީޚާއި ގަޑި	2023 ސެޕްޓެމްބަރ 12 ވާ އަންގާރަ ދުވަހު 10:10 ގައި، މި މަސައްކަތަށް އަންދާސީ ހިސާބު ހުށަހަޅުއްވާ ފަރާތްތަކުގެ ތެރެއިން އެވަގުތުގައި ހާޒިރުވެ ތިބި ބީލަންވެރިން ނުވަތަ ބީލަންވެރިންގެ ބަދަލުގައި އެ ފަރާތަކުން ކަނޑައަޅާ ފަރާތްތަކުގެ ހާޒިރުގައެވެ. އަދި އެޑްވާންސް ސަބަބަކާހުރެ މިދުވަސް (2023 ސެޕްޓެމްބަރ 12 ވާ އަންގާރަ) ބަންދުނަމަ، ޖެހިގެން އަންނަ ރަސްމީ ދުވަހު 10:10 ގައި، މި މަސައްކަތަށް އަންދާސީ ހިސާބު ހުށަހަޅުއްވާ ފަރާތްތަކުގެ ތެރެއިން އެވަގުތުގައި ހާޒިރުވެ ތިބި ބީލަންވެރިން ނުވަތަ ބީލަންވެރިންގެ ބަދަލުގައި އެ ފަރާތަކުން ކަނޑައަޅާ ފަރާތްތަކުގެ ހާޒިރުގައެވެ.

ސެކްޝަން 2.	ޕްރީބިޑްމީޓިންގ މަސައްކަތްކުރާތަނަށް ކުރިއަށްދާން ގޮތާއި އަމަލުކުރާނެ އުސޫލުތައް
2.1.	މި ބީލަމަށް ބޭނުންވާ ތަކެތި / މަސައްކަތުގެ ތަފްސީލު މި ބީލަންފޮތުގެ ސެކްޝަން 3 ގައި ތަފްސީލުކޮށް ހިމެނިފައިވާނެއެވެ.
2.2.	ބީލަމާއި ބެހޭގޮތުން އެއްވެސް ސުވާލެއްވާނަމަ، އީމެއިލް ކުރާނީ 2023 އޮގަސްޓު 29 ވާ އަންގާރަ ދުވަހު 11:00 ގެ ކުރިން tender@ncit.gov.mv އަށެވެ. އަދި އިސްތިފްސާރުތަކުގެ ސެންޓަރގެ ހަމަވުމުގެ ކުރިން ހުށަހެޅޭ ސުވާލުތަކުގެ ޖަވާބުތައް މިއިދާރާގެ ވެބްސައިޓް www.ncit.gov.mv ގައި 2023 ސެޕްޓެމްބަރ 03 އާދިއްތަ ދުވަހު 1:30 ގައި ޝާއިއު ކުރެވޭނެއެވެ. މި ބީލަމަށް

	ހުޅުވާނީ މިމަސައްކަތަށް އަންދާސީ ހިސާބު ހުށަހަޅުއްވާ ފަރާތްތަކުގެ ތެރެއިން އެވަގުތުގައި ހާޒިރުވެތިބި ބީލަން ވެރިން ނުވަތަ ބީލަންވެރިންގެ ބަދަލުގައި އެފަރާތްތަކުން ކަނޑައަޅާ ފަރާތްތަކުގެ ހާޒިރުގައެވެ.
.2·3	ބީލަމަށް ކުރިމަތިލެވޭނެ ފަރާތްތައް (ކޮލިފިކޭޝަން ކްރައިޓީރިއާ) ބީލަން ހުޅުވާލެވިފައިވަނީ، ވިޔަފާރި ރަޖިސްޓްރީ ކުރުމުގެ ގާނޫނު (ގާނޫނު ނަންބަރު: 18/2014) ގެ ދަށުން ވިޔަފާރި ރަޖިސްޓްރީ ކޮށްފައިވާ ހުރިހާ ވިޔަފާރިތަކަށެވެ. (ހ) ދިވެހިރާއްޖޭގެ ކުންފުންޏާބެހޭ ގާނޫނުގެ ދަށުން ރަޖިސްޓްރީ ކޮށްފައިވާ ކުންފުނިތައް. (ށ) ޕާޓްނަރ ޝިޕް ގާނޫނުގެ ދަށުން ރަޖިސްޓްރީ ކޮށްފައިވާ ޕާޓްނަރޝިޕްތައް. (ނ) ކޯޕަރޭޓިވް ސޮސައިޓީގެ ގާނޫނުގެ ދަށުން ރަޖިސްޓްރީ ކޮށްފައިވާ ކޯޕަރޭޓިވް ސޮސައިޓީތައް. (ބ) އަމިއްލަ ފަރުދުންގެ ވިޔަފާރީގެ ގާނޫނުގެ ދަށުން ރަޖިސްޓްރީކޮށްފައިވާ އަމިއްލަ ފަރުދުންގެ ވިޔަފާރިތައް.
.2·4	ބީލަން ހުށަހެޅުމަށްޓަކައި، ވިޔަފާރީގެ ފަރާތުން އިދާރާއަށް ހާޒިރުވާ ފަރާތަކީ ބީލަމާއި ގުޅޭ އެންމެހައި ލިޔެކިޔުންތަކުގައި ސޮއިކުރުމަށް، ބީލަން ހުށަހަޅާ ފަރާތުގެ ހުއްދަ ނުވަތަ ޕަވަރ އޮފް އެޓަރނީ ލިބިފައިވާ ފަރާތެއްކަމުގައި ބެލެވޭނެއެވެ.
.2·5	ކޮލިފިކޭޝަން ކްރައިޓީރިއާގައި ހިމަނާފައިވާ ކަންތައްތަކުން ފުރިހަމަ ނުވާ ބީލަންތައް ބާތިލުވާނެއެވެ. އަދި މި ބީލަންތައް އިވެލުއޭޝަން މަރުހަލާއަކަށް ނުގެންދެވޭނެއެވެ.
.2·6	ބީލަން ހުށަހެޅުމަށް ކަނޑައަޅާފައިވާ ސުންގަޑި ހަމަވުމަށްފަހު ހުށަހަޅާ ބީލަންތައް ބަލައެއް ނުގަންނާނެއެވެ.
.2·7	ބީލަންވެރިން ހުށަހަޅާ ޕްރޮޕޯޒަލް ހުންނަންވާނީ ތިރީގައި ބަޔާންކޮށްފައިވާ ގޮތަށެވެ. (ހ) ޕްރޮޕޯޒަލްގެ ކޮންމެ ސަފްހާއެއްގައި ނަންބަރު ޖަހާފައި ހުންނަން ވާނެއެވެ. (ށ) ޕްރޮޕޯޒަލް ހުންނަންވާނީ ބައިންޑްކޮށްފައެވެ. (ނ) މި ފޯމުގެ ސެކްޝަން 4 ގައި ބަޔާންކުރާ ހުރިހާ ތަކެތި ހަމަކުރަންވާނެއެވެ.
.2·8	ބީލަން ހުށަހަޅަންވާނީ ބަންދުކޮށްފައިވާ ސިޓީއުރައެއްގައެވެ. އަދި ސިޓީއުރައިގެ ބޭރުގައި މި ދަންނަވާ މަޢުލޫމާތު ހިމަނަންވާނެއެވެ. (ހ) ބީލަމުގެ ނަން (ށ) އިޢުލާން ނަންބަރު (ނ) ހުށަހަޅާ ފަރާތުގެ ނަން
.2·9	ޕްރޮޕޯޒަލްގައި ހިމެނޭ ކަންތަކާ ގުޅޭގޮތުން އިވެލުއޭޝަން މަރުހަލާގައި އިތުރު ސާފުކުރުންތަކެއް ބޭނުންނަމަ މަޢުލޫމާތާއި ލިޔެކިޔުން ހުށަހެޅުމުގެ އިޚްތިޔާރު އިދާރާއަށް ލިބިގެންވެއެވެ. އަދި އިދާރާއިން ބޭނުން މުއްދަތުގައި ލިޔުންތައް ހުށަނާޅައިފިނަމަ، ބީލަން ކެންސަލް ކުރުމުގެ އިޚްތިޔާރު އިދާރާއަށް ލިބިގެންވެއެވެ.
.2·10	ހުށަހަޅާ ބީލަމުގެ ބިޑް ވެލިޑިޓީ ޕީރިއަޑް ދުވަހުގެ މުއްދަތަކީ 90 (ނުވަދިހަ) ދުވަހެވެ.
.2·11	މިމަސައްކަތަށް ހަވާލުކުރުން ފަރާތެއް ހޮވުމުގައި ބޭނުންވާ އިވެލުއޭޝަން ކްރައިޓީރިއާ އާއި އެއްގޮތަށް މާކްސް ދިނުމުން، އެންމެ މަތިން މާކްސް ލިބޭފަރާތަކަށެވެ.
.2·12	ބީލަން ކެންސަލްކުރުމުގެ ހައްގު އިދާރާއިން ރިޒާވްކޮށް އަންނާނެއެވެ.
.2·13	ބީލަން ކެންސަލްކުރާނަމަ ފަރާތަށް ކޮންޓްރެކްޓް ހަވާލުކުރުމުގެ ކުރިން، ބީލަމުގައި ބައިވެރިވި ހުރިހާ ފަރާތްތަކަށް، އެބީލަން ކެންސަލްކުރި ކޮންފަރާތެއް ކަމާއި، ކެންސަލްކުރި ސަބަބު ފަރާތްތަކަށް ކޮބައިކަން

	އަންގާނެއެވެ. އަދި ބީލަން ކާމިޔާބު ނުވާފަރާތްތަކާ ބީލަމާ ގުޅިގެން ހުރިއެއްވެސް މައްސަލައެއް ވާނަމަ، އެމައްސަލަ ހުށަހެޅުމަށް 5 (ފަހެއް) ދުވަހުގެ މުހުލަތެއްދެވޭނެއެވެ.
2·14.	ބީލަން ކާމިޔާބު ކުރިފަރާތުން ހުށަހަޅާ ބީލުގެ އަގު -/500,000ރ (ފަސްލައްކަ) ރުފިޔާއަށް ވުރެ އަގުބޮޑުނަމަ ބިޑް އެވޯޑްވާ ފަރާތުން އެގްރީމެންޓްގައި ސޮއިކުރުމުގެ ކުރިން މާލިއްޔަތު ޤަވާއިދުގައިވާގޮތުގެމަތިން އެއްބަސްވުމުގައި ސޮއިކުރުމަށް ވަޑައިގަންނަވާއިރު ދިވެހިރާއްޖޭގައި ރަޖިސްޓްރީވެފައިވާ މާލީ ޚިދުމަތްދޭ ފަރާތަކުން ދޫކުރާ ޕާފޯމަންސް ގެރެންޓީއެއްގެ ގޮތުގައި ބީލަމުގެ ޖުމްލަ އަގުގެ 7% ހަތެއް އިންސައްތައަށްވާ -/56,000 ރ (ފަންސާސް ހަހާސް ރުފިޔާ) ހުށަހަޅަންވާނެއެވެ .
2·15.	މަސައްކަތުގެ މުއްދަތު ގުނަންފަށާނީ މަސައްކަތް ކުރުމަށް އެގްރިމެންޓްގައި ބަޔާންކޮށްފައިވާ ދުވަހުން ފެށިގެންނެވެ.
2·16.	އެއްބަސްވުމުގެ ޢާންމު މާއްދާތައް އަދި ހާއްސަ މާއްދާތައް މިފޯމުގެ ސެކްޝަން 6 ގައި ބަޔާންކޮށްފައި ވާނެއެވެ.
2·17.	މާލީ ޤާބިލުކަން ވަޒަންކުރާނެ ގޮތް މި ފޯމުގެ 6·4 ގައިވާ ގޮތުގައި ބަޔާންކޮށްފައިވާނެއެވެ.

ސެކްޝަން 3.	ހޯދަންބޭނުންވާ ތަކެތި ނުވަތަ ޚިދުމަތުގެ މަޢުލޫމާތު
3·1.	ހުށަހަޅާތަކެއްޗަކީ ބަޔާންކޮށްފައިވާ ސްޕެސިފިކޭޝަނަށްވުރެ ދަށް ސްޕެސިފިކޭޝަނަކަށް ވެގެން ނުވާނެއެވެ.
3·2.	ތަކެތި ޑެލިވަރ ކުރަންޖެހޭނީ، ހުށަހަޅާފައިވާ މުއްދަތުގެ ތެރޭގައި، ނޭޝަނަލް ސެންޓަރ ފޯރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ، ކަލާފާނު ހިނގުން، މާލެ އަށް ރަސްމީ ބަންދު ދުވަސްތައްފިޔަވައި، 14:00 ގެ ކުރިންނެވެ.
3·3.	ފައިސާ ދޫކުރެވޭނީ، އެތަކެތި ބަލާ ރިސީވްކުރުމަށްފަހު ތަކެތީގައި އެއްވެސް މައްސަލައެއް ނެތްކަމުގައިވާނަމައެވެ.
3·4.	ތަކެތީގެ ސްޕެސިފިކޭޝަން އަދި އެހެނިހެން މައުލޫމާތު މި ސެކްޝަންގައި ބަޔާންކުރެވިފައިވާނެއެވެ.

#	Requirements	Compliance (Yes / No)	Part No. and Reference
1	**01 Nos x Concentrator Appliance**		
	General Requirement		
	Make and Model of the proposed appliance should be clearly stated		
	The appliance should be a hardware appliance supporting next-generation firewall features and SD-WAN architecture without any additional module or hardware		
	OEM of the proposed appliance should be in “Leaders” or “Challengers” quadrant as per the last 2 years Gartner’s Magic Quadrant for “SD-WAN” or “Network Firewalls”.		
	Should be an appliance-based hardware platform which is optimized and purpose-built for high performance		

	The appliance should include redundant power supply units		
	Should be 19” rack mountable		
	Should support Active-Active as well as Active-Passive redundancy architecture for high availability		
	Bidder should submit the Original Manufacture’s Authorization Certificate along with the bid		
	Interface and Connectivity Requirements		
	Proposed device should have USB interfaces for connecting 3G/4G modems or alternatively should include pluggable LTE module		
	Proposed appliance should have the following interfaces • 8 x 10GE SFP+ ports • 1 x Dedicated Console/Management interface		
	Should include 8 x OM4 Duplex LC 5m Fiber Optic Patch Cord		
	Should include 8 x 10GE SFP+ Multi-Mode (SR) Original Cisco transceivers for existing equipment		
	Network and Routing Requirements		
	The appliance should support Static Routing, Policy-based Routing, Dynamic Routing (RIP, OSPF, BGP &IS-IS) and Application aware Routing		
	Should provide NAT functionality, including PAT		
	Should support Policy-based NAT		
	Should support NAT within IPsec VPN tunnels		
	The device should include perpetual license for the following features/function: Routing (RIP, OSPF, BGP), Essential Routing: NAT, DNS, NTP Essential Security: Firewall, IPS, IPsec VPN, Application visibility, Policy Based Routing		
	Administration & Management Requirements		
	Should support Graphical Interface (HTTP/HTTPS) and CLI (Telnet/ SSH) based management		
	Should have SNMPv2c and SNMPv3 support		
	Should support for role-based administration of the device		
	Encryption & VPN Requirements		
	Should support Hub and Spoke VPN topology		
	Should support encryption, authentication and integrity protocols: DES, 3DES, AES-128, AES-256, MD5, SHA, SHA-256		
	IPSec VPN should support XAuth over RADIUS		
	IPS and Application Control Requirements		
	The appliance should include all required license for IPS and Application Control		

	Should have built-in Signature and Anomaly based IPS engine on the same unit		
	Should identify and control applications		
	Should control popular IM/P2P, social media, malware, applications.		
	Should be able to control cloud-based applications and should be able to route the specific applications via different WAN links		
	Malware Protection		
	Should include all required license **advance malware protection.**		
	Should support real-time detection of viruses and malicious code for HTTP, HTTPS, SMTPS, POP3, IMAP		
	Should have options to prevent user downloads based on file extension as well as file type		
	Web Content Filtering Requirements		
	The appliance should include all required license for web content filtering		
	Web content filtering should work independently without the need to integrate with an external proxy server		
	Web content filtering should have the facility to block URLs.		
	Web content filtering should support HTTP and HTTPS traffic		
	Should prevent the download of specific file types via policy.		
	Should include DNS filtering feature to block DNS requests to known botnet C&C domains		
	Should have option to configure traffic shaping on policy basis, application basis and IP basis.		
	SD WAN Support		
	The appliance should support redundant links with active/active traffic load balancing		
	The SD WAN Solution should work seamlessly in typical NAT scenarios inclusive but not limited to • 1 to 1 NAT • Behind NAT / Traversal NAT		
	The appliance should support multiple WAN link types (4G LTE, MPLS, ILL, etc.)		
	Encryption of the WAN transport		
	Monitor the quality of the WAN links		
	Should provide a method for providing direct branch to branch WAN connectivity		
	Application based traffic steering should be available to be implemented for SD-WAN policies		
	SD-WAN policies should provide multiple WAN strategy options. Such as:		

	• Manually assign WAN link to an application/Internet service • Assign the best quality WAN link to an application/Internet service • Load balance traffic across all WAN links that meet the SLA targets		
	Warranty and Security Subscriptions		
	The proposed appliance should have OEM authorized warranty / support services (TAC) for 24x7 for One (01) year		
	The proposed appliance **should include 1-Year security subscription** with IPS, Advance Malware Protection, Cloud Sandboxing, and Application Control		
	The proposed appliance should include **1-Year subscription for SD-WAN license**		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
2	**16 Nos x SD-WAN BRANCH CPE**		
	General Requirements		
	Make and Model of the proposed appliance should be clearly stated		
	The appliance should be a physical appliance supporting next-generation firewall features and SD-WAN architecture without any additional module or hardware		
	OEM of the proposed appliance should be in “Leaders” or “Challengers” quadrant as per the last 2 years Gartner’s Magic Quadrant for “SD-WAN” or “Network Firewalls”.		
	Should be an appliance-based hardware platform which is optimized and purpose-built for high performance with a security-hardened, purpose-built operating system		
	Bidder should submit the Original Manufacture’s Authorization Certificate along with the bid		
	Interface and Connectivity Requirements		
	Proposed device should have USB interfaces for connecting 3G/4G modems or alternatively should include pluggable LTE module		
	Proposed device should have the following interfaces 4 x GE RJ45 ports 1 x USB interface 1 x console interface		
	Network & Routing Requirements		
	The appliance should support Static Routing, Policy-based Routing, Dynamic Routing (RIP, OSPF, BGP &IS-IS) and Application aware Routing		

	Proposed **SD-WAN BRANCH CPE** should support Policy-based Routing			
	Should provide NAT functionality, including PAT			
	Should support Policy-based NAT			
	Should support NAT within IPSec VPN tunnels			
	The device should include perpetual license for the following features/function: Routing (RIP, OSPF, BGP), Essential Routing: NAT, DNS, NTP Essential Security: Firewall, IPS, IPsec VPN, Application visibility, Policy Based Routing			
	Administration & Management Requirements			
	Should support Graphical Interface (HTTP/HTTPS) and CLI (Telnet/ SSH) based management			
	Should have SNMPv2c and SNMPv3 support			
	Should support for role-based administration of the device			
	Encryption & VPN Requirements			
	Should support Hub and Spoke VPN topology			
	Should support encryption, authentication and integrity protocols: DES, 3DES, AES-128, AES-256, MD5, SHA, SHA-256			
	IPSec VPN should support XAuth over RADIUS			
	IPS and Application Control Requirements			
	The appliance should include all required license for IPS and Application Control			
	Should have built-in Signature and Anomaly based IPS engine on the same unit			
	Should identify and control applications			
	Should control popular IM/P2P, social media, malware, applications regardless of port/protocol			
	Should be able to control cloud-based applications and should be able to route the specific applications via different WAN links			
	Malware Protection			
	Should include all required license **advance malware protection.**			
	Should support real-time detection of viruses and malicious code for HTTP, HTTPS, SMTPS, POP3, IMAP			
	Should have options to prevent user downloads based on file extension as well as file type			
	Web Content Filtering Requirements			
	The appliance should include all required license for web content filtering			

	Web content filtering should work independently without the need to integrate with an external proxy server		
	Web content filtering should have the facility to block URLs based on categories		
	Web content filtering should support HTTP and HTTPS traffic		
	Should prevent the download of specific file types via policy.		
	Should include DNS filtering feature to block DNS requests to known botnet C&C domains		
	Should have option to configure traffic shaping on policy basis, application basis and IP basis.		
	SD WAN Support		
	Redundant links with active/active traffic load balancing		
	The appliance should support for multiple WAN link types (4G LTE, MPLS, ILL, etc.)		
	The SD WAN Solution should work seamlessly in typical NAT scenarios inclusive but not limited to • 1 to 1 NAT • Behind NAT / Traversal NAT		
	Monitor the quality of the WAN links		
	Should provide a method for providing direct branch to branch WAN connectivity		
	Application based traffic steering should be available to be implemented for SD-WAN policies		
	SD-WAN policies should provide multiple WAN strategy options. Such as, - Manually assign WAN link to an application/Internet service - Assign the best quality WAN link to an application/Internet service - Load balance traffic across all WAN links that meet the SLA targets		
	Warranty & Subscriptions		
	The proposed device should include One (01) Year OEM authorized warranty, subscription and support services (TAC) for 24x7		
	The proposed appliance should include One (01) Year security subscription with IPS, Advance Malware Protection, Cloud Sandboxing, Application Control, and Web Filtering (URL, web content and DNS Filtering)		
	The proposed appliance should include One (01) Year **subscription for SD-WAN license**		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
3	**01 Nos x Management and Analytics Appliance**		
	The solution should have a centralized management appliance for managing a minimum 20 appliances of the same OEM from a single console and should be proposed as an on-premise Virtual appliance		
	The proposed virtual appliance should support VMware ESX/ESXi		
	The management appliance should provide the ability to collectively configure the device settings, objects and policies across all the devices from a single user interface		
	The management solution should support providing security updates to all managed devices		
	The management solution should support e-mail-based alerting of critical events		
	The management solution should have the capability to maintain audit trail (history) of configuration changes.		
	Failure of the Management solution should not impact the managed devices traffic flow		
	The management solution should include a central log retention capability to receive logs from all the managed devices.		
	The management solution should support Role Based Access Control (RBAC)		
	Logging and Reporting should be an out of the box solution and should be proposed as an on-premise virtual appliance		
	The complete traffic and system event logs of all devices of this solution should be retained in the appliance. The duration of the retention should be configurable for a period of 1 year.		
	The solution must support alerting notifications through SNMP traps, SMTP email, and remote syslog.		
	The solution should support out of the box predefined standard reports		
	The solution should support to generate customized reports for daily, weekly, monthly, yearly etc., and but not limited to link bandwidth utilization, device health monitors, security enforcements, system logins etc.		
	Warranty & Subscriptions		
	The proposed management and analytics solution should include One (01) Year OEM authorized warranty / support services (TAC) for 24x7		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
4	**Installation, Configuration, Migration and Training**		
	Hardware installation including mounting, management cabling and power up as per manufacturer guidelines		
	The vendor MUST have at minimum the following full time OEM Certified Professional/Engineer under its payroll to provide installation, configuration, integration, migration and training services. All relevant engineer(s) certificates and supporting documents should be included with the proposal.		
	A solution specific technical solution diagram that represents an overview of the solution (items proposed in this proposal) should be proposed.		
	The NCN core is currently based on technologies from Cisco Systems. The vendor should demonstrate capability to install the SDWAN to work with the NCN. We accept the following as demonstration: • Cisco Certified Employees • Proof Of Experience		
	Perform site readiness assessment ensuring hardware environment is ready for project commencement		
	Identify and assess existing environment including network security devices, core network switching and routing devices.		
	Ensure current deployment and configuration is setup such that the configuration and migration works can be conducted with minimal downtime.		
	The devices and appliances should be installed and configured as per manufacturer best practice guidelines and as per industry best practices. The installation plan (timeline) should be provided and agreed with NCIT before the commencement of installation. *Note : The proposed timeline should consider that all work should be done on official government, unless specified by NCIT.*		
	Configure secure management console for all devices and appliances.		
	Design appropriate LAN, WAN, and DMZ security policies.		
	Configure Malware Protection and Web filtering policies		
	Configure IPS and Application policies		
	Configure and migrate existing routing segments		
	Configure management and logging appliance		
	On the job training for minimally 02 technical personnel		
	Comprehensive testing and a detailed documentation inclusive of diagrams, flow charts and other industry standard documentation.		

5	**Service Level Expectations**		
	The support service vendor should provide the contact number of a single point of contact to facilitate immediate contact by client's representative and he or she should be responsible to liaise with all vendors for rectification of faults within the Next Business Day.		
	Defective equipment should be replaced by the bidder at their own cost including the cost of transport if any.		
	The support service vendor should provide all normal toolkit and test equipment needed for the maintenance of the hardware to NCIT.		
	System maintenance and support services should include the following activities. • 24 x 7 on-line Support. • Patch updating and major / minor software version upgrading support. • Phone/Email TAC support must be provided during support period. • Issue resolution / Onsite Visits within 1 day of hardware failures reported. • Local TAC support plan must be maintaining by the Bidder for the maintenance period.		
6	**Maintenance Support Services including on-site Technical Support**		
	On-site hardware repair/replace, and maintenance support service should be delivered by experienced OEM Certified Engineer		
	On-site diagnostics and repair service should be delivered by experienced OEM Certified Engineer and should diagnose, repair, and test the unit to ensure optimal performance.		
	Technical support experienced engineers should be available to answer questions.		
	Flexible on-site response times that best meets the business requirements		
	Service summary report should provide after each work performed including recommendations for service to ensure optimal performance.		
	Maintenance Support Engineer should check and ensuring the unit is operating with the most recent firmware version. Firmware upgrades should be provided at no extra charge.		
	During each maintenance visit, field service Engineers should run tests to verify that the system is functioning correctly in all operational modes, stopping problems before they start.		
	Maintenance Support Engineer should follow well-defined set of processes and procedures to be able to provide quality services, as per Industry standard.		
	The support service vendor should maintain critical parts locally in Male' to provide after sale support.		

ސެކްޝަން 4.	ބީލަން ހުށަހަޅާއިރު ތިރީގައިވާ މައުލޫމާތު އަދި ލިޔުންތައް ހުށަހަޅަންވާނެއެވެ.
.4.1	ހުށަހަޅާ މައުލޫމާތުގެ ޗެކްލިސްޓް
.4.2	ބީލަން ހުށަހަޅާފޯމު
.4.3	ފައިނޭންޝަލް ބެކްގްރައުންޑް ފޯމް / ނުވަތަ މި މައުލޫމާތު ހިމެނޭ ކޮޕީޝަން
.4.4	ހުށަހަޅާ ޕްރޮޖެކްޓަށް، ޕްރޮޖެކްޓް އުފެއްދި ފަރާތުން ބަޔާންކުރެވިފައިވާ މައުލޫމާތު، ޕްރޮޖެކްޓް ބެލެހެއްޓި

.4.5	ތަކެތި އުފައްދާ ފަރާތުން (މެނުފެކްޗަރަރ) ދޭ ހުއްދައާ ފަރާތަކުން ދޫކުރެވިފައިވާ އޮތޯރައިޒޭޝަން ފަރާތްތަކުން އަންގައިދޭ ލިޔުން
.4.6	ޓެކްނިކަލް ކޮމްޕްލަޔަންސް ފޯމު
.4.7	ދިވެހިރާއްޖޭގައި ރަޖިސްޓްރީ ކުރެވިފައިވާ ވިޔަފާރިއަކަށްވުން. (ކުންފުނި / ޕާޓްނަރޝިޕް / ކޯޕަރޭޓިވް ސޮސައިޓީ / އަމިއްލަ ފަރުދުންގެ ރަޖިސްޓްރީގެ ކޮޕީ)
.4.8	މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓް ދޫކޮށްފައިވާ ވިޔަފާރީގެ ޕްރޮފައިލް ޝީޓް.
.4.9	މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓްގައި ކުދި އަދި މެދު ފަންތީގެ ވިޔަފާރީގެ ގިންތިއެއްގައި ރަޖިސްޓްރީ ކުރެވިފައިވާ ދިވެހި ވިޔަފާރިއެއްކަން އަންގައިދޭ ސްޓޭޓަސްގެ ކޮޕީ (އެސް.އެމް.އީ ރަޖިސްޓްރޭޝަން) - ރަޖިސްޓަރ ވެފަ ވާ ފަރާތްތަކަށް
.4.10	މޯލްޑިވްސް އިންލަންޑް ރެވެނިއު އޮތޯރިޓީން ދޫކޮށްފައިވާ ޓެކްސް ޕޭޔަރ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓް ކޮޕީ
.4.11	މޯލްޑިވްސް އިންލަންޑް ރެވެނިއު އޮތޯރިޓީން ދޫކޮށްފައިވާ ޖީއެސްޓީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓް ކޮޕީ (ޖީ.އެސް.ޓީއަށް ރަޖިސްޓަރ ކޮށްފައިވާނަމަ)
.4.12	މޯލްޑިވްސް އިންލަންޑް ރެވެނިއު އޮތޯރިޓީން ދޫކުރާ ޓެކްސް ކްލިއަރަންސް ރިޕޯޓްގެ ކޮޕީ (ދޫކުރިތާފަހުން 03 މަސް ހަމަނުވާ)
.4.13	މަސައްކަތުގެ ތަޖުރިބާހުރިކަން ހާމަކޮށްދިނުމަށް މަސައްކަތް ކުރުވި ފަރާތުން ދޫކޮށްފައިވާ ލިޔުން
.4.14	މާލީ ޤާބިލްކަން ހުރި ފަރާތްތަކުން ސާބިތުކޮށްދިނުމަށްޓަކައި ބޭނުންވާ "ފައިނޭންޝަލް ސިޗުއޭޝަން ފޯމު" އަދި އޭގައިވާ މައުލޫމާތަށް ބަރޯސާވެވޭގޮތަށް ސަޕޯޓިންގް ޑޮކިއުމަންޓްސްގެ ގޮތުގައި، 2020، 2021 އަދި 2022 ވަނަ އަހަރުގެ ފައިނޭންޝަލް ސްޓޭޓްމަންޓްސް ނުވަތަ ދިވެހިރާއްޖޭ ޤަބޫލުކުރާ ފަރާތަކުން އޮޑިޓް ކުރެވިފަ ސިޓީ (ޖަދުވަލު 03 ގެ ފޯމް 03)
.4.15	ސަރުކާރު ޤަބޫލުކުރާ ބޭންކަކުން ނުވަތަ ފައިނޭންޝަލް އިންސްޓިޓިއުޝަނަކުން ދޫކޮށްފައިވާ ބިޑް ސެކިއުރިޓީ ނުވަތަ ގެރެންޓީ ގެ ގޮތުގައި ލަފާކުރާ އަގުގެ 1% (އެކެއް އިންސައްތަ) އަށްވާ -/8,000 ރ (އަށްހާސް ރުފިޔާ) ގެ ބިޑް ސެކިއުރިޓީ ނުވަތަ ގެރެންޓީ ހުށަހަޅަންވާނެއެވެ.

ސެކްޝަން 5. އިވެލުއޭޝަން ކްރައިޓީރިއާ		
މާރކްސް	ކްރައިޓީރިއާ	ތަފްސީލު
50%	އަގު (ޓޯޓަލް ކޮސްޓް އޮފް އޯނަރޝިޕް 5 އަހަރަށް)	ބެންޗްމާރކް (އެންމެ ދަށް އަގު) / ހުށަހެޅި އަގު × 50
30%	ޓެކްނިކަލް ކޮމްޕްލަޔަންސް	ފުރިހަމަ ކޮށްފައިވާ ކޮމްޕްލަޔަންސް ފޯމު
15%	ޑެލިވަރީ އަދި އިންސްޓޯލޭޝަން މުއްދަތު	ބިޑަރުންގެ ތެރެއިން ހުށަހެޅި އެންމެ ކުރުމުއްދަތު / ހުށަހެޅި މުއްދަތު × 15
5%	ތަޖުރިބާ	• ޕްރޮޖެކްޓް ދިނުމުގައި ބަލާނީ 2013 އިން ފެށިގެން މިއަދާއި ހަމައަށް -/800،000 ރ (އަށް ލައްކަ) ރުފިޔާއިން ފެށިގެން މަތިން ކޮށްފައިވާ މި ބާވަތުގެ މަސައްކަތްތަކުގައި ދެ ގޮތުން މަސައްކަތް ހަވާލު ކުރި ފަރާތުން ދީފައިވާ މަސައްކަތް ނިންމި ކަމުގެ ލިޔުމަކަށެވެ.

		● މި ބާވަތުގެ މަސައްކަތުގެ ގޮތުގައި ބެލެވޭނީ ނެޓްވޯކް ސެކިއުރިޓީ، ޑާޓާ ސެންޓަރ ނެޓްވޯކް އަދި އެސްޑީ ވޭން ފަދަ މަސައްކަތް ފޯރުކޮށްދީފައިވާ ކަމުގެ ހިދުމަތްތަކެވެ. ● ހުށަހަޅާ ލިޔުންތަކުގައި މަތީގައި ބަޔާންކޮށްފައިވާ މުއްދަތުގައި މަސައްކަތް ނިންމިކަން އެނގޭ ޕާޓީން އާއި މަސައްކަތުގެ އަގު އަދި މަސައްކަތް ފުރިހަމަ ކޮށްފައިވާ ފެންވަރު އެނގެން އޮންނަންވާނެއެވެ. ހުށަހަޅާ ރެފަރެންސް ލިޔުންތަކުގެ ތެރެއިން އިސްވެ ދެންނެވުނު ކަންކަން ފުރިހަމަވެފައިވާ ކޮންމެ ލިޔުމަކަށް 1 ޕޮއިންޓް ލިބޭނެއެވެ. މިބައިން އެންމެ ގިނަވެގެން ދެވޭނީ 05 ޕޮއިންޓެވެ.

އަގު ތަފްސީލު (ޓޯޓަލް ކޮސްޓް އޮފް އޯނަރޝިޕް 5 އަހަރަށް) ފުރިހަމަ ކުރުމަށް

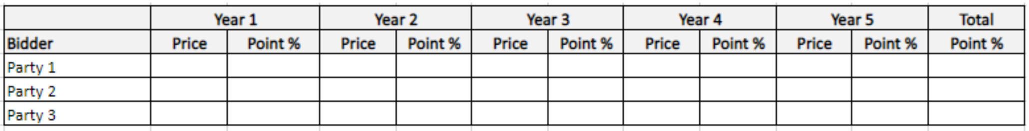
5 Year Total Cost of Ownership (TCO)	50%

5 Year Total Cost of Ownership (TCO)

Should provide detailed yearly cost breakdown for the following items for up to five years. However, the payments will be done for one year and the vendor will be fixed for the term of 5 years for renewals and further expansion.

Item	**Year 1**	**Year 2**	**Year 3**	**Year 4**	**Year 5**	**Total TCO**
01 Nos x Concentrator appliance security Subscriptions						
01 Nos x Concentrator Appliance OEM authorized warranty, subscription, and support services						
01 Nos x Concentrator Appliance subscription for SD-WAN license						
16 Nos x SD-WAN BRANCH CPE Security Subscriptions						
16 Nos x SD-WAN BRANCH CPE OEM authorized warranty, subscription, and support services						
16 Nos x SD-WAN BRANCH CPE subscription for SD-WAN license						
01 Nos x Management and Analytics Appliance OEM authorized warranty / support services						
Total						

Year	**Weightage**
Year 1	10.00
Year 2	10.00
Year 3	20.00
Year 4	20.00
Year 5	20.00
Total	**80.00**



	Year 1		Year 2		Year 3		Year 4		Year 5		Total
Bidder	Price	Point %	Price	Point %	Price	Point %	Price	Point %	Price	Point %	Point %
Party 1											
Party 2											
Party 3											

$$Price\ (Total\ TCO) = \frac{\text{Benchmark (lowest price)}}{Proposed\ Price\ By\ Bidder}\ x\ Weightage$$

ސެކްޝަން 6. ބީލަމާއި އެކު ހުށަހަޅަން ޖެހޭ ލިޔުންތައް

- މި ސެކްޝަނުގައި ބަޔާންކުރާ ލިޔުންތައް ޕްރޮޕޯސަލްގައި ހުށަހަޅަންވާނެއެވެ.
- މި ލިޔުމަކާއި އެކު ސަޕްލަޔަރގެ ޤާބިލުކަން ހުށަހަޅަން ބޭނުންވާނަމަ އެކަކެތި ފުރިހަމަކޮށް ހުށަހަޅަންވާނެއެވެ.
- މާލީ ބަޔާނުގެ ބައެއްގެ ގޮތުގައި، ވިޔަފާރިއެއްގެ ސޮލްވެންސީ ލެޓަރ އާއިއެކު 2020، 2021 އަދި 2022 ވަނަ އަހަރުގެ ފައިނޭންޝަލް ސްޓޭޓްމަންޓްސް ނުވަތަ ފައިން އޮޑިޓް ކުރެވިފައިވާ ބޭންކް ސްޓޭޓްމަންޓް އެއް ލިޔުމެއް ހުށަހަޅަންވާނެއެވެ.
- ފައިން އޮޑިޓް ކުރެވިފައި ނޫނީ، ބޭންކް ސްޓޭޓްމަންޓް އަދި ޕްރޮފިޓް އެންޑް ލޮސް ސްޓޭޓްމަންޓް ދ ނަމޫނާ ޤަބޫލުކުރެވިދާނެއެވެ. މިގޮތުން ހުށަހަޅާ ހިސާބު ތައްޔާރުކޮށްފައިވާ ފަރާތުގެ ފަރާތުން ސޮއިކޮށްފައިވާ ލިޔުމަކާ ޗާޓަޑް އެކައުންޓަންޓުގެ ތައްގަނޑު ޖަހާފައިވާ ލިޔުން ބަލައިގަނެވޭނެއެވެ.
- ބޭންކް ސްޓޭޓްމަންޓް، ޕްރޮފިޓް އެންޑް ލޮސް ސްޓޭޓްމަންޓް އަދި ފައިން އޮޑިޓް ކުރެވިފައިވާ ގޮތް ބަލައެއް ނުގަނެވޭނެއެވެ.

6.1 ހުށަހަޅާ މައުލޫމާތުގެ ޗެކްލިސްޓް

بسم الله الرحمن الرحيم

National Centre for Information Technology

ނޭޝަނަލް ސެންޓަރ ފޯރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

#	ހުށަހަޅާ ލިޔުންތައް	ސަފްހާ	ފާހަގަ
.1	ހުށަހަޅާ މައުލޫމާތުގެ ޗެކްލިސްޓް		
.2	ބީލަން ހުށަހަޅާފޯމު		
.3	ފައިނޭންޝަލް ބްރޭކްޑައުން ފޯމު / ނުވަތަ މި މައުލޫމާތު ހިމެނޭ ކޯޓޭޝަން		
.4	ހުށަހަޅާ ޕްރޮޑަކްޓް ކެޓަލޮގް، ޕްރޮޑަކްޓް އުފެއްދި ފަރާތުން ތައްޔާރުކުރައިވާ މައުލޫމާތު، ޕްރޮޑަކްޓް ބްރޯޝަރ		
.5	ވަކާލީ އުފައްދާ ފަރާތުން (މެނުފެކްޗަރަރ) ބިޑް ހުށަހަޅާ ފަރާތަށް ދޫކޮށްފައިވާ އޮތޮރައިޒްޑް ޑިސްޓްރިބިއުޓަރެއްކަމުގެ ލިޔުން		
.6	ބިޒްނަސް ކޮމްޕްލަޔަންސް ފޯމު		
.7	ދިވެހިރާއްޖޭގައި ރަޖިސްޓްރީ ކުރެވިފައިވާ ވިޔަފާރިއަކަށްވުން. (ކުންފުނި / ޕާޓްނަރޝިޕް / ކޯޕަރޭޓިވް ސޮސައިޓީ / އަމިއްލަ ފަރުދުންގެ ރަޖިސްޓްރީގެ ކޮޕީ)		
.8	މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓުން ދޫކޮށްފައިވާ ވިޔަފާރީގެ ޕްރޮފައިލް ޝީޓް.		
.9	މިނިސްޓްރީ އޮފް އިކޮނޮމިކް ޑިވެލޮޕްމަންޓްގައި ކުޑަ އަދި މެދު ފަންތީގެ ވިޔަފާރީގެ ޑިރެކްޓަރީން ޑިރެކްޓަރީގައި ރަޖިސްޓްރީ ކުރެވިފައިވާ ވިޔަފާރިއެއްކަން އަންގައިދޭ ސެޓްފިކެޓްގެ ކޮޕީ (އެސް.އެމް.އީ ރަޖިސްޓްރޭޝަން) - ރަޖިސްޓަރ ވެފަ ވާ ފަރާތެއްނަމަ		
.10	މޯލްޑިވްސް އިންލެންޑް ރެވެނިއު އޮތޯރިޓީން ދޫކޮށްފައިވާ ބިޒްނަސް ޓީއައިއެން ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓް ކޮޕީ		
.11	މޯލްޑިވްސް އިންލެންޑް ރެވެނިއު އޮތޯރިޓީން ދޫކޮށްފައިވާ ޖީ.އެސް.ޓީ ރަޖިސްޓްރޭޝަން ސެޓްފިކެޓް ކޮޕީ (ޖީ.އެސް.ޓީއަށް ރަޖިސްޓަރ ކޮށްފައިވާނަމަ)		
.12	މޯލްޑިވްސް އިންލެންޑް ރެވެނިއު އޮތޯރިޓީން ދޫކުރާ ބިޒްނަސް ކްލިއަރެންސް ރިޕޯޓްގެ ކޮޕީ (ދޫކުރިތާ ގިނަވެގެން 03 މަސް ހަމަނުވާ)		
.13	މަސައްކަތުގެ ތަޖުރިބާ ހުރިކަން ހާމަކޮށްދިނުމަށް މަސައްކަތް ކުރުވި ފަރާތުން ދޫކޮށްފައިވާ ލިޔުން		
.14	މާލީ ޤާބިލުކަން ހުރި ފަރާތެއްކަން ސާބިތުކޮށްދިނުމަށްޓަކައި ބޭނުންވާ "ފައިނޭންޝަލް ސްޓޭޓްމަންޓް ފޯމު" އަދި އޭގައިވާ މައުލޫމާތަށް ބާރުދޭނެ ސަޕޯޓިންގް ޑޮކިއުމަންޓްގެ ގޮތުގައި، 2020، 2021 އަދި 2022 ވަނަ އަހަރުގެ ފައިނޭންޝަލް ސްޓޭޓްމަންޓް ނުވަތަ ދިވެހިރާއްޖޭގެ ބޭންކް ސްޓޭޓްމަންޓް ވައިން އޮފް ކޮމަރސް ޝީޓް (ޖުމްލަ 03 ގެ ފޯމު 03)		
.15	ސަރުކާރުން ގަބޫލުކުރާ ބޭންކަކުން ނުވަތަ ފައިނޭންޝަލް އިންސްޓިޓިއުޝަނަކުން ދޫކޮށްފައިވާ ބިޑް ސެކިއުރިޓީ ނުވަތަ ގެރެންޓީ ގެ ގޮތުގައި ހުށަހަޅާ އަގުގެ 1% (އެކެއް އިންސައްތަ) އަދަދާ 8,000/- ރ (އަށްހާސް ރުފިޔާ) ގެ ބިޑް ސެކިއުރިޓީ ނުވަތަ ގެރެންޓީ ހުށަހަޅަންވާނެއެވެ.		

6.2 ބިޔަން ހުށަހަޅާ ފޯމު

National Centre for Information Technology

ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

އިދާރާ ނަންބަރު:		ތާރީޚް	

ބިލާއި ގުޅުންހުރި ކަންކަމުގައި މުއާމަލާތްކުރަން ސޮއި ކުރުމުގެ ހުއްދަ ދީފައިވާ ފަރާތުގެ

ނަން:	
އައިޑީކާޑު ނަންބަރު	
މަޤާމު:	
ގުޅޭނެ ނަންބަރު:	
އީމެއިލް:	
ތާރީޚް:	
ސޮއި:	

މި ބިލުގައި ހުށަހަޅާފައިވާ ސައްޙަ ތަފްޞީލުތައް ކަމަށް އިޤްރާރުވަމެވެ. އަދި މަތީގައި ބަޔާން ކުރެވިފައިވާ ފަރާތަކީ ބިލާއި ގުޅޭގޮތުން މި ވިޔަފާރި ޓްރާންސެކްޝަންކުރާ ފަރާތްކަމާއި، ވިޔަފާރީގެ ފަރާތުން ބިލާއި ގުޅުންހުރި ލިޔެކިޔުންތަކުގައި ސޮއިކުރުމުގެ ހުއްދަ ދީފައިވާ ފަރާތެކެވެ.

ބިޔަން ހުށަހަޅާ ފަރާތުން (އަމިއްލަ ފަރުދެއް ނަމަ ވިޔަފާރިވެރިޔާ، ކުންފުންޏެއް ނަމަ މެނޭޖިންގ ޑިރެކްޓަރ އަދި ޕާޓްނަރޝިޕްއެއް ނަމަ މެނޭޖިންގ ޕާޓްނަރ) ސޮއިކުރައްވާނީ

ނަން:		[illegible]
މަޤާމު:		
ގުޅޭނެ ނަންބަރު:		
އީމެއިލް:		
ތާރީޚް:		
ސޮއި:		

6.3. ފައިނޭންޝަލް ޕްރޮޕޯޒަލް ފޯމު (ޖިން ފޯމް-1) ނުވަތަ ފޯމުގައި ބައްޓަންކުރާ މައުލޫމާތު ހިމެނޭ ކޯޓޭޝަން. މި ފޯމު ނުވަތަ ކޯޓޭޝަނާއި އެކު، ތަކެތި އުފެއްދި ފަރާތުން ދޫކޮށްފައިވާ ޖެނުއިން ކަމުގެ މައުލޫމާތު ހިމެނޭ ފޮޓޯ، ބްރޯޝަރ ތަކެތި ހުށަހަޅަންވާނެއެވެ. މި ފޯމުގެ ހުރިހާ މައުލޫމާތެއް ފުރިހަމަކުރަންވާނެއެވެ. ނުވަތަ ކޯޓޭޝަނުގައި ހިމަނަންވާނެއެވެ.

بسم الله الرحمن الرحيم

National Centre for Information Technology ނޭޝަނަލް ސެންޓަރ ފޮރ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

Reference No: (generated by the proponent)
Quotation validity: (   ) days

#	Item / Equipment or work details	Qty	Price (MVR)	Total (MVR)
1	**01 Nos x Concentrator Appliance**			
	General Requirement			
	Make and Model of the proposed appliance should be clearly stated			
	The appliance should be a hardware appliance supporting next-generation firewall features and SD-WAN architecture without any additional module or hardware			
	OEM of the proposed appliance should be in “Leaders” or “Challengers” quadrant as per the last 2 years Gartner’s Magic Quadrant for “SD-WAN” or “Network Firewalls”.			
	Should be an appliance-based hardware platform which is optimized and purpose-built for high performance			
	The appliance should include redundant power supply units			
	Should be 19” rack mountable			
	Should support Active-Active as well as Active-Passive redundancy architecture for high availability			
	Bidder should submit the Original Manufacture’s Authorization Certificate along with the bid			
	Interface and Connectivity Requirements			
	Proposed device should have USB interfaces for connecting 3G/4G modems or alternatively should include pluggable LTE module			
	Proposed appliance should have the following interfaces ● 8 x 10GE SFP+ ports ● 1 x Dedicated Console/Management interface			
	Should include 8 x OM4 Duplex LC 5m Fiber Optic Patch Cord			
	Should include 8 x 10GE SFP+ Multi-Mode (SR) Original Cisco transceivers for existing equipment			
	Network and Routing Requirements			
	The appliance should support Static Routing, Policy-based Routing, Dynamic Routing (RIP, OSPF, BGP &IS-IS) and Application aware Routing			
	Should provide NAT functionality, including PAT			
	Should support Policy-based NAT			
	Should support NAT within IPsec VPN tunnels			
	The device should include perpetual license for the following features/function: Routing (RIP, OSPF, BGP), Essential Routing: NAT, DNS, NTP			

	Essential Security: Firewall, IPS, IPsec VPN, Application visibility, Policy Based Routing			
	Administration & Management Requirements			
	Should support Graphical Interface (HTTP/HTTPS) and CLI (Telnet/ SSH) based management			
	Should have SNMPv2c and SNMPv3 support			
	Should support for role-based administration of the device			
	Encryption & VPN Requirements			
	Should support Hub and Spoke VPN topology			
	Should support encryption, authentication and integrity protocols: DES, 3DES, AES-128, AES-256, MD5, SHA, SHA-256			
	IPSec VPN should support XAuth over RADIUS			
	IPS and Application Control Requirements			
	The appliance should include all required license for IPS and Application Control			
	Should have built-in Signature and Anomaly based IPS engine on the same unit			
	Should identify and control applications			
	Should control popular IM/P2P, social media, malware, applications.			
	Should be able to control cloud-based applications and should be able to route the specific applications via different WAN links			
	Malware Protection			
	Should include all required license **advance malware protection.**			
	Should support real-time detection of viruses and malicious code for HTTP, HTTPS, SMTPS, POP3, IMAP			
	Should have options to prevent user downloads based on file extension as well as file type			
	Web Content Filtering Requirements			
	The appliance should include all required license for web content filtering			
	Web content filtering should work independently without the need to integrate with an external proxy server			
	Web content filtering should have the facility to block URLs.			
	Web content filtering should support HTTP and HTTPS traffic			
	Should prevent the download of specific file types via policy.			
	Should include DNS filtering feature to block DNS requests to known botnet C&C domains			
	Should have option to configure traffic shaping on policy basis, application basis and IP basis.			
	SD WAN Support			
	The appliance should support redundant links with active/active traffic load balancing			
	The SD WAN Solution should work seamlessly in typical NAT scenarios inclusive but not limited to • 1 to 1 NAT • Behind NAT / Traversal NAT			
	The appliance should support multiple WAN link types (4G LTE, MPLS, ILL, etc.)			
	Encryption of the WAN transport			
	Monitor the quality of the WAN links			
	Should provide a method for providing direct branch to branch WAN connectivity			
	Application based traffic steering should be available to be implemented for SD-WAN policies			
	SD-WAN policies should provide multiple WAN strategy options. Such as:			

	• Manually assign WAN link to an application/Internet service • Assign the best quality WAN link to an application/Internet service • Load balance traffic across all WAN links that meet the SLA targets			
	Warranty and Security Subscriptions			
	The proposed appliance should have OEM authorized warranty / support services (TAC) for 24x7 for One (01) year			
	The proposed appliance **should include 1-Year security subscription** with IPS, Advance Malware Protection, Cloud Sandboxing, and Application Control			
	The proposed appliance should include **1-Year subscription for SD-WAN license**			
2	**16 Nos x SD-WAN BRANCH CPE**			
	General Requirements			
	Make and Model of the proposed appliance should be clearly stated			
	The appliance should be a physical appliance supporting next-generation firewall features and SD-WAN architecture without any additional module or hardware			
	OEM of the proposed appliance should be in “Leaders” or “Challengers” quadrant as per the last 2 years Gartner’s Magic Quadrant for “SD-WAN” or “Network Firewalls”.			
	Should be an appliance-based hardware platform which is optimized and purpose-built for high performance with a security-hardened, purpose-built operating system			
	Bidder should submit the Original Manufacture’s Authorization Certificate along with the bid			
	Interface and Connectivity Requirements			
	Proposed device should have USB interfaces for connecting 3G/4G modems or alternatively should include pluggable LTE module			
	Proposed device should have the following interfaces 4 x GE RJ45 ports 1 x USB interface 1 x console interface			
	Network & Routing Requirements			
	The appliance should support Static Routing, Policy-based Routing, Dynamic Routing (RIP, OSPF, BGP &IS-IS) and Application aware Routing			
	Proposed **SD-WAN BRANCH CPE** should support Policy-based Routing			
	Should provide NAT functionality, including PAT			
	Should support Policy-based NAT			
	Should support NAT within IPSec VPN tunnels			
	The device should include perpetual license for the following features/function: Routing (RIP, OSPF, BGP), Essential Routing: NAT, DNS, NTP Essential Security: Firewall, IPS, IPsec VPN, Application visibility, Policy Based Routing			
	Administration & Management Requirements			
	Should support Graphical Interface (HTTP/HTTPS) and CLI (Telnet/ SSH) based management			
	Should have SNMPv2c and SNMPv3 support			

	Should support for role-based administration of the device			
	Encryption & VPN Requirements			
	Should support Hub and Spoke VPN topology			
	Should support encryption, authentication and integrity protocols: DES, 3DES, AES-128, AES-256, MD5, SHA, SHA-256			
	IPSec VPN should support XAuth over RADIUS			
	IPS and Application Control Requirements			
	The appliance should include all required license for IPS and Application Control			
	Should have built-in Signature and Anomaly based IPS engine on the same unit			
	Should identify and control applications			
	Should control popular IM/P2P, social media, malware, applications regardless of port/protocol			
	Should be able to control cloud-based applications and should be able to route the specific applications via different WAN links			
	Malware Protection			
	Should include all required license **advance malware protection.**			
	Should support real-time detection of viruses and malicious code for HTTP, HTTPS, SMTPS, POP3, IMAP			
	Should have options to prevent user downloads based on file extension as well as file type			
	Web Content Filtering Requirements			
	The appliance should include all required license for web content filtering			
	Web content filtering should work independently without the need to integrate with an external proxy server			
	Web content filtering should have the facility to block URLs based on categories			
	Web content filtering should support HTTP and HTTPS traffic			
	Should prevent the download of specific file types via policy.			
	Should include DNS filtering feature to block DNS requests to known botnet C&C domains			
	Should have option to configure traffic shaping on policy basis, application basis and IP basis.			
	SD WAN Support			
	Redundant links with active/active traffic load balancing			
	The appliance should support for multiple WAN link types (4G LTE, MPLS, ILL, etc.)			
	The SD WAN Solution should work seamlessly in typical NAT scenarios inclusive but not limited to • 1 to 1 NAT • Behind NAT / Traversal NAT			
	Monitor the quality of the WAN links			
	Should provide a method for providing direct branch to branch WAN connectivity			
	Application based traffic steering should be available to be implemented for SD-WAN policies			
	SD-WAN policies should provide multiple WAN strategy options. Such as, - Manually assign WAN link to an application/Internet service - Assign the best quality WAN link to an application/Internet service - Load balance traffic across all WAN links that meet the SLA targets			
	Warranty & Subscriptions			
	The proposed device should include One (01) Year OEM authorized warranty, subscription and support services (TAC) for 24x7			

	The proposed appliance should include One (01) Year security subscription with IPS, Advance Malware Protection, Cloud Sandboxing, Application Control, and Web Filtering (URL, web content and DNS Filtering)			
	The proposed appliance should include One (01) Year **subscription for SD-WAN license**			
3	**01 Nos x Management and Analytics Appliance**			
	The solution should have a centralized management appliance for managing a minimum 20 appliances of the same OEM from a single console and should be proposed as an on-premise Virtual appliance			
	The proposed virtual appliance should support VMware ESX/ESXi			
	The management appliance should provide the ability to collectively configure the device settings, objects and policies across all the devices from a single user interface			
	The management solution should support providing security updates to all managed devices			
	The management solution should support e-mail-based alerting of critical events			
	The management solution should have the capability to maintain audit trail (history) of configuration changes.			
	Failure of the Management solution should not impact the managed devices traffic flow			
	The management solution should include a central log retention capability to receive logs from all the managed devices.			
	The management solution should support Role Based Access Control (RBAC)			
	Logging and Reporting should be an out of the box solution and should be proposed as an on-premise virtual appliance			
	The complete traffic and system event logs of all devices of this solution should be retained in the appliance. The duration of the retention should be configurable for a period of 1 year.			
	The solution must support alerting notifications through SNMP traps, SMTP email, and remote syslog.			
	The solution should support out of the box predefined standard reports			
	The solution should support to generate customized reports for daily, weekly, monthly, yearly etc., and but not limited to link bandwidth utilization, device health monitors, security enforcements, system logins etc.			
	Warranty & Subscriptions			
	The proposed management and analytics solution should include One (01) Year OEM authorized warranty / support services (TAC) for 24x7			
4	**Installation, Configuration, Migration and Training**			
	Hardware installation including mounting, management cabling and power up as per manufacturer guidelines			
	The vendor MUST have at minimum the following full time OEM Certified Professional/Engineer under its payroll to provide installation, configuration, integration, migration and training services. All relevant engineer(s) certificates and supporting documents should be included with the proposal.			
	A solution specific technical solution diagram that represents an overview of the solution (items proposed in this proposal) should be proposed.			
	The NCN core is currently based on technologies from Cisco Systems. The vendor should demonstrate capability to install the SDWAN to work with the NCN.			

	We accept the following as demonstration: - Cisco Certified Employees - Proof Of Experience			
	Perform site readiness assessment ensuring hardware environment is ready for project commencement			
	Identify and assess existing environment including network security devices, core network switching and routing devices.			
	Ensure current deployment and configuration is setup such that the configuration and migration works can be conducted with minimal downtime.			
	The devices and appliances should be installed and configured as per manufacturer best practice guidelines and as per industry best practices. The installation plan (timeline) should be provided and agreed with NCIT before the commencement of installation. *Note : The proposed timeline should consider that all work should be done on official government, unless specified by NCIT.*			
	Configure secure management console for all devices and appliances.			
	Design appropriate LAN, WAN, and DMZ security policies.			
	Configure Malware Protection and Web filtering policies			
	Configure IPS and Application policies			
	Configure and migrate existing routing segments			
	Configure management and logging appliance			
	On the job training for minimally 02 technical personnel			
	Comprehensive testing and a detailed documentation inclusive of diagrams, flow charts and other industry standard documentation.			
5	**Service Level Expectations**			
	The support service vendor should provide the contact number of a single point of contact to facilitate immediate contact by client’s representative and he or she should be responsible to liaise with all vendors for rectification of faults within the Next Business Day.			
	Defective equipment should be replaced by the bidder at their own cost including the cost of transport if any.			
	The support service vendor should provide all normal toolkit and test equipment needed for the maintenance of the hardware to NCIT.			
	System maintenance and support services should include the following activities. - 24 x 7 on-line Support. - Patch updating and major / minor software version upgrading support. - Phone/Email TAC support must be provided during support period - Issue resolution / Onsite Visits within 1 day of hardware failures reported - Local TAC support plan must be maintaining by the Bidder for the maintenance period.			
6	**Maintenance Support Services including on-site Technical Support**			
	On-site hardware repair/replace and maintenance support service should be delivered by experienced OEM Certified Engineer			
	On-site diagnostics and repair service should be delivered by experienced OEM Certified Engineer and should diagnose, repair, and test the unit to ensure optimal performance.			

	Technical support experienced engineers should be available to answer questions.			
	Flexible on-site response times that best meets the business requirements			
	Service summary report should provide after each work performed including recommendations for service to ensure optimal performance.			
	Maintenance Support Engineer should check and ensuring the unit is operating with the most recent firmware version. Firmware upgrades should be provided at no extra charge.			
	During each maintenance visit, field service Engineers should run tests to verify that the system is functioning correctly in all operational modes, stopping problems before they start.			
	Maintenance Support Engineer should follow well-defined set of processes and procedures to be able to provide quality services, as per Industry standard.			
	The support service vendor should maintain critical parts locally in Male' to provide after sale support.			
Total				
GST 8%				
Warranty				
Delivery and installation period				
Total with GST				

Bidder Stamp and Sign

____

بسم الله الرحمن الرحيم

National Centre for Information Technology ނޭޝަނަލް ސެންޓަރ ފޯ އިންފޮމޭޝަން ޓެކްނޮލޮޖީ

Financial Data for Previous 03 Years [MVR Equivalent]			
Financial Information of the Year	**2020**	**2021**	**2022**
Information from Balance Sheet			
Total Assets			
Total Liabilities			
Net Worth			
Current Assets			
Current Liabilities			
Working Capital			
Information from Income Statement			
Total Revenues			
Profits Before Taxes			
Profits After Taxes			

- Attached are copies of the financial statement (balance sheets including all related notes, and income statements), as indicated above, complying with the following conditions.
- All such documents reflect the financial situation of the Bidder.
- Historic financial statements must be complete, including all notes to the financial statements.
- Historic financial statements must correspond to accounting periods.

Evaluation criteria

Financial Situation evaluation

A. To be eligible the financial statements of the bidding party must show, average annual turnover of MVR 800,000.00 for the years 2020, 2021 and 2022.
(or)

B. To be eligible the financial statements of the bidding party must show, Minimum value of MVR 800,000.00 of the proposed price, for liquid asset, for the year 2020, 2021 and 2022.
(or)

C. If the bidding party is unable to meet any of the above requirement they shall submit “Line of Credit Letter” as per the template in Form FIN – 3. (Credit limit shall be no less than MVR 800,000.00 of the proposed price)

Bidder Stamp and Sign

____

#	Requirements	Complian ce (Yes / No)	Part No. and Reference
1	**01 Nos x Concentrator Appliance**		
	General Requirement		
	Make and Model of the proposed appliance should be clearly stated		
	The appliance should be a hardware appliance supporting next-generation firewall features and SD-WAN architecture without any additional module or hardware		
	OEM of the proposed appliance should be in “Leaders” or “Challengers” quadrant as per the last 2 years Gartner’s Magic Quadrant for “SD-WAN” or “Network Firewalls”.		
	Should be an appliance-based hardware platform which is optimized and purpose-built for high performance		
	The appliance should include redundant power supply units		
	Should be 19” rack mountable		
	Should support Active-Active as well as Active-Passive redundancy architecture for high availability		
	Bidder should submit the Original Manufacture’s Authorization Certificate along with the bid		
	Interface and Connectivity Requirements		
	Proposed device should have USB interfaces for connecting 3G/4G modems or alternatively should include pluggable LTE module		
	Proposed appliance should have the following interfaces ● 8 x 10GE SFP+ ports ● 1 x Dedicated Console/Management interface		
	Should include 8 x OM4 Duplex LC 5m Fiber Optic Patch Cord		
	Should include 8 x 10GE SFP+ Multi-Mode (SR) Original Cisco transceivers for existing equipment		
	Network and Routing Requirements		
	The appliance should support Static Routing, Policy-based Routing, Dynamic Routing (RIP, OSPF, BGP &IS-IS) and Application aware Routing		
	Should provide NAT functionality, including PAT		
	Should support Policy-based NAT		
	Should support NAT within IPsec VPN tunnels		
	The device should include perpetual license for the following features/function: Routing (RIP, OSPF, BGP), Essential Routing: NAT, DNS, NTP		

#	Requirements	Complian ce (Yes / No)	Part No. and Reference
	Essential Security: Firewall, IPS, IPsec VPN, Application visibility, Policy Based Routing		
	Administration & Management Requirements		
	Should support Graphical Interface (HTTP/HTTPS) and CLI (Telnet/ SSH) based management		
	Should have SNMPv2c and SNMPv3 support		
	Should support for role-based administration of the device		
	Encryption & VPN Requirements		
	Should support Hub and Spoke VPN topology		
	Should support encryption, authentication and integrity protocols: DES, 3DES, AES-128, AES-256, MD5, SHA, SHA-256		
	IPSec VPN should support XAuth over RADIUS		
	IPS and Application Control Requirements		
	The appliance should include all required license for IPS and Application Control		
	Should have built-in Signature and Anomaly based IPS engine on the same unit		
	Should identify and control applications		
	Should control popular IM/P2P, social media, malware, applications.		
	Should be able to control cloud-based applications and should be able to route the specific applications via different WAN links		
	Malware Protection		
	Should include all required license **advance malware protection.**		
	Should support real-time detection of viruses and malicious code for HTTP, HTTPS, SMTPS, POP3, IMAP		
	Should have options to prevent user downloads based on file extension as well as file type		
	Web Content Filtering Requirements		
	The appliance should include all required license for web content filtering		
	Web content filtering should work independently without the need to integrate with an external proxy server		
	Web content filtering should have the facility to block URLs.		
	Web content filtering should support HTTP and HTTPS traffic		
	Should prevent the download of specific file types via policy.		
	Should include DNS filtering feature to block DNS requests to known botnet C&C domains		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
	Should have option to configure traffic shaping on policy basis, application basis and IP basis.		
	SD WAN Support		
	The appliance should support redundant links with active/active traffic load balancing		
	The SD WAN Solution should work seamlessly in typical NAT scenarios inclusive but not limited to • 1 to 1 NAT • Behind NAT / Traversal NAT		
	The appliance should support multiple WAN link types (4G LTE, MPLS, ILL, etc.)		
	Encryption of the WAN transport		
	Monitor the quality of the WAN links		
	Should provide a method for providing direct branch to branch WAN connectivity		
	Application based traffic steering should be available to be implemented for SD-WAN policies		
	SD-WAN policies should provide multiple WAN strategy options. Such as: • Manually assign WAN link to an application/Internet service • Assign the best quality WAN link to an application/Internet service • Load balance traffic across all WAN links that meet the SLA targets		
	Warranty and Security Subscriptions		
	The proposed appliance should have OEM authorized warranty / support services (TAC) for 24x7 for One (01) year		
	The proposed appliance **should include 1-Year security subscription** with IPS, Advance Malware Protection, Cloud Sandboxing, and Application Control		
	The proposed appliance should include **1-Year subscription for SD-WAN license**		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
2	**16 Nos x SD-WAN BRANCH CPE**		
	General Requirements		
	Make and Model of the proposed appliance should be clearly stated		
	The appliance should be a physical appliance supporting next-generation firewall features and SD-WAN architecture without any additional module or hardware		
	OEM of the proposed appliance should be in “Leaders” or “Challengers” quadrant as per the last 2 years Gartner’s Magic Quadrant for “SD-WAN” or “Network Firewalls”.		

#	Requirements	Complian ce (Yes / No)	Part No. and Reference
	Should be an appliance-based hardware platform which is optimized and purpose-built for high performance with a security-hardened, purpose-built operating system		
	Bidder should submit the Original Manufacture's Authorization Certificate along with the bid		
	Interface and Connectivity Requirements		
	Proposed device should have USB interfaces for connecting 3G/4G modems or alternatively should include pluggable LTE module		
	Proposed device should have the following interfaces 4 x GE RJ45 ports 1 x USB interface 1 x console interface		
	Network & Routing Requirements		
	The appliance should support Static Routing, Policy-based Routing, Dynamic Routing (RIP, OSPF, BGP &IS-IS) and Application aware Routing		
	Proposed **SD-WAN BRANCH CPE** should support Policy-based Routing		
	Should provide NAT functionality, including PAT		
	Should support Policy-based NAT		
	Should support NAT within IPSec VPN tunnels		
	The device should include perpetual license for the following features/function: Routing (RIP, OSPF, BGP), Essential Routing: NAT, DNS, NTP Essential Security: Firewall, IPS, IPsec VPN, Application visibility, Policy Based Routing		
	Administration & Management Requirements		
	Should support Graphical Interface (HTTP/HTTPS) and CLI (Telnet/ SSH) based management		
	Should have SNMPv2c and SNMPv3 support		
	Should support for role-based administration of the device		
	Encryption & VPN Requirements		
	Should support Hub and Spoke VPN topology		
	Should support encryption, authentication and integrity protocols: DES, 3DES, AES-128, AES-256, MD5, SHA, SHA-256		
	IPSec VPN should support XAuth over RADIUS		
	IPS and Application Control Requirements		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
	The appliance should include all required license for IPS and Application Control		
	Should have built-in Signature and Anomaly based IPS engine on the same unit		
	Should identify and control applications		
	Should control popular IM/P2P, social media, malware, applications regardless of port/protocol		
	Should be able to control cloud-based applications and should be able to route the specific applications via different WAN links		
	Malware Protection		
	Should include all required license **advance malware protection.**		
	Should support real-time detection of viruses and malicious code for HTTP, HTTPS, SMTPS, POP3, IMAP		
	Should have options to prevent user downloads based on file extension as well as file type		
	Web Content Filtering Requirements		
	The appliance should include all required license for web content filtering		
	Web content filtering should work independently without the need to integrate with an external proxy server		
	Web content filtering should have the facility to block URLs based on categories		
	Web content filtering should support HTTP and HTTPS traffic		
	Should prevent the download of specific file types via policy.		
	Should include DNS filtering feature to block DNS requests to known botnet C&C domains		
	Should have option to configure traffic shaping on policy basis, application basis and IP basis.		
	SD WAN Support		
	Redundant links with active/active traffic load balancing		
	The appliance should support for multiple WAN link types (4G LTE, MPLS, ILL, etc.)		
	The SD WAN Solution should work seamlessly in typical NAT scenarios inclusive but not limited to • 1 to 1 NAT • Behind NAT / Traversal NAT		
	Monitor the quality of the WAN links		
	Should provide a method for providing direct branch to branch WAN connectivity		
	Application based traffic steering should be available to be implemented for SD-WAN policies		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
	SD-WAN policies should provide multiple WAN strategy options. Such as, - Manually assign WAN link to an application/Internet service - Assign the best quality WAN link to an application/Internet service - Load balance traffic across all WAN links that meet the SLA targets		
	Warranty & Subscriptions		
	The proposed device should include One (01) Year OEM authorized warranty, subscription and support services (TAC) for 24x7		
	The proposed appliance should include One (01) Year security subscription with IPS, Advance Malware Protection, Cloud Sandboxing, Application Control, and Web Filtering (URL, web content and DNS Filtering)		
	The proposed appliance should include One (01) Year **subscription for SD-WAN license**		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
3	**01 Nos x Management and Analytics Appliance**		
	The solution should have a centralized management appliance for managing a minimum 20 appliances of the same OEM from a single console and should be proposed as an on-premise Virtual appliance		
	The proposed virtual appliance should support VMware ESX/ESXi		
	The management appliance should provide the ability to collectively configure the device settings, objects and policies across all the devices from a single user interface		
	The management solution should support providing security updates to all managed devices		
	The management solution should support e-mail-based alerting of critical events		
	The management solution should have the capability to maintain audit trail (history) of configuration changes.		
	Failure of the Management solution should not impact the managed devices traffic flow		
	The management solution should include a central log retention capability to receive logs from all the managed devices.		
	The management solution should support Role Based Access Control (RBAC)		
	Logging and Reporting should be an out of the box solution and should be proposed as an on-premise virtual appliance		

	The complete traffic and system event logs of all devices of this solution should be retained in the appliance. The duration of the retention should be configurable for a period of 1 year.		
	The solution must support alerting notifications through SNMP traps, SMTP email, and remote syslog.		
	The solution should support out of the box predefined standard reports		
	The solution should support to generate customized reports for daily, weekly, monthly, yearly etc., and but not limited to link bandwidth utilization, device health monitors, security enforcements, system logins etc.		
	Warranty & Subscriptions		
	The proposed management and analytics solution should include One (01) Year OEM authorized warranty / support services (TAC) for 24x7		

#	Requirements	Compliance (Yes / No)	Part No. and Reference
4	**Installation, Configuration, Migration and Training**		
	Hardware installation including mounting, management cabling and power up as per manufacturer guidelines		
	The vendor MUST have at minimum the following full time OEM Certified Professional/Engineer under its payroll to provide installation, configuration, integration, migration and training services. All relevant engineer(s) certificates and supporting documents should be included with the proposal.		
	A solution specific technical solution diagram that represents an overview of the solution (items proposed in this proposal) should be proposed.		
	The NCN core is currently based on technologies from Cisco Systems. The vendor should demonstrate capability to install the SDWAN to work with the NCN. We accept the following as demonstration: • Cisco Certified Employees • Proof Of Experience		
	Perform site readiness assessment ensuring hardware environment is ready for project commencement		
	Identify and assess existing environment including network security devices, core network switching and routing devices.		
	Ensure current deployment and configuration is setup such that the configuration and migration works can be conducted with minimal downtime.		
	The devices and appliances should be installed and configured as per manufacturer best practice guidelines and as per industry best practices. The installation plan (timeline) should be provided and agreed with NCIT before the commencement of installation. *Note : The proposed timeline should consider that all work should be done on official government, unless specified by NCIT.*		
	Configure secure management console for all devices and appliances.		

	Design appropriate LAN, WAN, and DMZ security policies.		
	Configure Malware Protection and Web filtering policies		
	Configure IPS and Application policies		
	Configure and migrate existing routing segments		
	Configure management and logging appliance		
	On the job training for minimally 02 technical personnel		
	Comprehensive testing and a detailed documentation inclusive of diagrams, flow charts and other industry standard documentation.		
5	**Service Level Expectations**		
	The support service vendor should provide the contact number of a single point of contact to facilitate immediate contact by client's representative and he or she should be responsible to liaise with all vendors for rectification of faults within the Next Business Day.		
	Defective equipment should be replaced by the bidder at their own cost including the cost of transport if any.		
	The support service vendor should provide all normal toolkit and test equipment needed for the maintenance of the hardware to NCIT.		
	System maintenance and support services should include the following activities. • 24 x 7 on-line Support. • Patch updating and major / minor software version upgrading support. • Phone/Email TAC support must be provided during support period • Issue resolution / Onsite Visits within 1 day of hardware failures reported • Local TAC support plan must be maintaining by the Bidder for the maintenance period.		
6	**Maintenance Support Services including on-site Technical Support**		
	On-site hardware repair/replace and maintenance support service should be delivered by experienced OEM Certified Engineer		
	On-site diagnostics and repair service should be delivered by experienced OEM Certified Engineer and should diagnose, repair, and test the unit to ensure optimal performance.		
	Technical support experienced engineers should be available to answer questions.		
	Flexible on-site response times that best meets the business requirements		
	Service summary report should provide after each work performed including recommendations for service to ensure optimal performance.		
	Maintenance Support Engineer should check and ensuring the unit is operating with the most recent firmware version. Firmware upgrades should be provided at no extra charge.		
	During each maintenance visit, field service Engineers should run tests to verify that the system is functioning correctly in all operational modes, stopping problems before they start.		
	Maintenance Support Engineer should follow well-defined set of processes and procedures to be able to provide quality services, as per Industry standard.		
	The support service vendor should maintain critical parts locally in Male' to provide after sale support.		

6.6. ލައިން އޮފް ކްރެޑިޓް ސިޓީގެ ނަމޫނާ.

[letterhead of the Bank/Financing Institution/Supplier]

[date]

To: *[Name and address of the Contractor]*

Dear,

You have requested {name of the bank/financing institution/supplier issuing the letter) to establish a line of credit for the purpose of executing {insert Name and identification of Project}.

We hereby undertake to establish a line of credit for the aforementioned purpose, in the amount of {insert amount}, effective upon receipt of evidence that you have been selected as successful bidder.

This line of credit will be valid through the duration of the contract awarded to you.

Authorized Signature:
Name and Title of Signatory:
Name of Agency:

6.7. ބިޑް ސެކިއުރިޓީގެ ނަމޫނާ

Form of Bid Security (Bank Guarantee)

WHEREAS, ……………………………………………….[name of Bidder] (hereinafter called "the Bidder") has submitted his Bid for the Project no……….issued by National Centre for Information Technology ………………………………… …………..for construction of …………………………… …….[name of Contract] (hereinafter called "the Bid").

KNOW ALL PEOPLE by these presents that We ……………………………………. [name of Bank] of ……… …………………… [name of country] having our registered office at ……………………………………………………………………………….. (hereinafter called "the Bank") are bound unto …………………………….[name of Purchaser] (hereinafter called "the Purchaser") in the sum of *……………………………………….. for which payment well and truly to be made to the said Purchaser, the Bank binds itself, its successors, and assigns by these presents.

SEALED with the Common Seal of the said Bank this ……..day of …………….20……………..

THE CONDITIONS of this obligation are:

(1) If, after Bid opening, the Bidder withdraws his Bid during the period of Bid validity specified in the Form of Bid;

or

(2) If the Bidder having been notified of the acceptance of his Bid by the Purchaser during the period of Bid validity:

(a) fails or refuses to execute the Form of Agreement in accordance with the Instructions to Bidders, if required; or

(b) fails or refuses to furnish the Performance Security, in accordance with the Instruction to Bidders; or

(c) does not accept the correction of the Bid Price pursuant to Clause 27,

we undertake to pay to the Purchaser up to the above amount upon receipt of his first written demand, without the Purchaser's having to substantiate his demand, provided that in his demand the Purchaser will note that the amount claimed by him is due to him owing to the occurrence of one or any of the three conditions, specifying the occurred condition or conditions.

* The Bidder should insert the amount of the Guarantee in words and figures denominated in Maldivian Rufiyaa. This figure should be the same as shown in Clause 16.1 of the Instructions to Bidders.

This Guarantee will remain in force up to and including the date ………………………. days after the deadline for submission of bids as such deadline is stated in the Instructions to Bidders or as it may be extended by the Purchaser, notice of which extension(s) to the Bank is hereby waived. Any demand in respect of this Guarantee should reach the Bank not later than the above date.

DATE…………………………… SIGNATURE OF THE BANK

WITNESS ……………………… SEAL

[signature, name, and address]

6.8 ޕަރފޯމަންސް ގެރެންޓީގެ ނަމޫނާ ސާމްޕަލް

Form of Performance Bank Guarantee (Unconditional)

To: ……………………………………………………………………………………………….
[name &address of Purchaser]
……………………………………………………………………………………………….
……………………………………………………………………………………………….

WHEREAS ……………………. *[name and address of Supplier]* (hereinafter called "the Supplier") has undertaken, in pursuance of Contract No. …… dated ……………………… to execute …………………………… *[name of Contract and brief description of Works]* (hereinafter called "the Contract");

AND WHEREAS it has been stipulated by you in the said Contract that the Supplier shall furnish you with a Bank Guarantee by a recognized bank for the sum specified therein as security for compliance with his obligations in accordance with the Contract;

AND WHEREAS we have agreed to give the Supplier such a Bank Guarantee;

NOW THEREFORE we hereby affirm that we are the Guarantor and responsible to you, on behalf of the Supplier, up to a total of *…………….. *[amount of Guarantee]* ……………………… *[amount in words]*, such sum being payable in the types and proportions of currencies in which the Contract Price is payable, and we undertake to pay you, upon your first written demand and without cavil or argument, any sum or sums within the limits of ……………… *[amount of Guarantee]* as aforesaid without your needing to prove or to show grounds or reasons for your demand for the sum specified therein.

*An amount is to be inserted by the Guarantor, representing the percentage of the Contract Price specified in the Contract, in Maldivian Rufiyaa.

We hereby waive the necessity of your demanding the said debt from the Supplier before presenting us with the demand.

We further agree that no change or addition to or other modification of the terms of the Contract or of the Works to be performed there under or of any of the Contract documents which may be made between you and the Supplier shall in any way release us from any liability under this Guarantee, and we hereby waive notice of any such change, addition, or modification.

This Guarantee shall be valid until the date of issue of the Defects Correction Certificate.

SIGNATURE AND SEAL OF THE GUARANTOR ………………………..
Name of Bank ……………………………………..
Address ……………………………………..
……………………………………..
……………………………………..
Date ………………………………………

6.9. އެއްބަސްވުމުގެ ނަމޫނާ

އެއްބަސްވުން

ނަންބަރު:

1. ތަޢާރަފު.

1.1. މިއީ (މަސައްކަތުގެ ތަފްސީލު) ގެނުމަށް މަސައްކަތް ހަވާލުވާ ފަރާތާއި އެކު ވެވޭ އެއްބަސްވުމެކެވެ.

2. އެއްބަސްވުމުގެ ބައިވެރިން.

2.1. މި އެއްބަސްވުމުގައި މަސައްކަތް ހަވާލުކުރި ފަރާތްކަމުގައި ބަޔާންކުރެވިފައިވަނީ، ނޭޝަނަލް ސެންޓަރ ފޯ އިންފޮމޭޝަން ޓެކްނޮލޮޖީއެވެ.

2.2. މަސައްކަތާއި ހަވާލުވާ ފަރާތް ކަމަށް ބަޔާންކުރެވިފައިވަނީ (ކުންފުނި ނުވަތަ ވިޔަފާރީގެ ނަން)

3. އެއްބަސްވުމުގައި ހިމެނޭ ތަކެއްޗާއި މަސައްކަތްތައް

3.1. މަސައްކަތް ހަވާލުކުރި ފަރާތުން (ތާރީޚް) ވަނަދުވަހު ކުރި އިއުލާން (ނަންބަރު) އާއި ގުޅިގެން މަސައްކަތާއި ހަވާލުވިފަރާތުން ހުށަހަޅާފައިވާ، (މި އެއްބަސްވުމުގެ ޖަދުވަލު 1 ގައި އެއްކަރުދާސްކުރެވިފައިވާ) ޕްރޮޕޯޒަލްގައިވާ ތަކެތި/މަސައްކަތް ހަވާލުކުރިފަރާތަށް ސަޕްލައިކޮށްދިނުން.

4. މަސައްކަތުގެ އަގު.

4.1. ޖަދުވަލު 1 ގައިވާ މަސައްކަތްކުރުމަށް މަސައްކަތުގެ އަގު ގޮތުގައި ކަނޑައަޅާފައިވަނީ (އަގު) އެވެ.

5. މަސައްކަތުގެ މުއްދަތު.

5.1. ޖަދުވަލު 1 ގައި ބަޔާންކޮށްފައިވާ މަސައްކަތް (މުއްދަތު) ދުވަހުގެ ތެރޭގައި (ރަސްމީ ބަންދު ދުވަސްތައް ހިމަނައިގެން) ނިންމުމަށް މަސައްކަތް ހަވާލުވި ފަރާތުން އެއްބަސްވަމެވެ.

(ހ) އެއްބަސްވުމުގައި ސޮއި ކުރާ (ތާރީޚް) އެވެ.

(ށ) އެއްބަސްވުމުގައިވާ މަސައްކަތް ނިންމަންޖެހޭ (ތާރީޚް) އެވެ.

6. މަސައްކަތަށް ފައިސާދެއްކުން

6.1. މަސައްކަތް އެއްބަސްވުމުގައިވާ ފެންވަރަށް ނިންމުނުކަމަށް މަސައްކަތް ހަވާލުކުރިފަރާތުން ނިންމުމުން، މަސައްކަތް ހަވާލުވިފަރާތުން މަސައްކަތުގެ ބިލުގެ އަސްލު، މަސައްކަތް ހަވާލުކުރި އޮފީހުގެ ރަސްމީ އީމެއިލް ނުވަތަ ރިސެޕްޝަނަށް ހުށަހަޅަންވާނެއެވެ. އަދި މި ބިލަށްވާ ފައިސާ 30 (ތިރީސް) ދުވަހުގެ ތެރޭގައި ޚަލާސްކޮށް ނިންމަންވާނެއެވެ.

7. ނިންމަންވީ ގޮތާއި ފެންވަރު

7.1. ކުރަންޖެހޭ މަސައްކަތްތަކުގެ ތަފްސީލު، މި އެއްބަސްވުމުގެ ޖަދުވަލު 1 ގައި ބަޔާން ކުރެވިފައިވާނެއެވެ. އަދި މި މަސައްކަތް ޖަދުވަލު 1 ގައި ބަޔާންކޮށްފައިވާ ފެންވަރާއި ވަގުތަށް ނިންމަންވާނެއެވެ.

7.2. ކަނޑައަޅާފައިވާ މުއްދަތުގެ ތެރޭގައި މަސައްކަތް ހަވާލުކުރި ފަރާތަށް ޤަބޫލު ކުރެވޭފަދަ ރަނގަޅު ފެންވަރެއްގައި މަސައްކަތް ނިންމުމަށްފަހު މަސައްކަތް ޙަވާލުކުރި ފަރާތާ ޙަވާލު ކުރަންވާނެއެވެ.

8. މަސައްކަތަށް ބަދަލުދިނުން.

8.1. މި އެއްބަސްވުމުގައި ކުރުމަށް ޖަދުވަލު 1 ގައި ބަޔާންކުރެވިފައިވާ މަސައްކަތްތަކަށް އެއްވެސް ބަދަލެއް (އަގު، މުއްދަތު ނުވަތަ މަސައްކަތަށް) ގެންނަން ޖެހިއްޖެ ނަމަ ހިދުމަތް ދޭ ފަރާތުން ނުވަތަ ހިދުމަތް ލިބިގަންނަ ފަރާތުން ލިޔުމަކުން އެގްރިމަންޓްގެ މުއްދަތުގައި އަންގައި ހުއްދަ ހޯދަން ވާނެއެވެ.

(ހ) މި އެއްބަސްވުމުގެ ޖަދުވަލު 1 ގައި ބަޔާންކޮށްފައިވާ މަސައްކަތްތަކުގެ އިތުރުން މަސައްކަތެއް ކުރަން ޖެހިއްޖެނަމަ މަސައްކަތް ހަވާލުކުރާފަރާތުން މަސައްކަތުގެ ސްކޯޕް ލިޔުމުން ފޮނުވައިދޭންވާނެއެވެ.

(ށ) ސްކޯޕް ކުރުމުގައިވާ ކަންކަމަށް، މަސައްކަތް ކުރާ ފަރާތުން އެކަމަށް ހިނގާނެ ހަރަދު ބަޔާންކޮށް ލިޔުމުން މަސައްކަތް ހަވާލުކުރި ފަރާތަށް ހުށަހަޅަންވާނެއެވެ.

(ނ) މިގޮތުން އިތުރުކުރާ މަސައްކަތެއް ފަށަންވާނީ ދެފަރާތުން އެއްބަސްވުމެއް ހަދައި އެއްބަސްވުމުގައި ސޮއިކުރުމަށްފަހުއެވެ.

(ރ) އަގަށް އެއްބަސް ނުވެވޭ ހާލަތެއްގައި އެހެން ފަރާތަކާއި އެކު މަސައްކަތުގެ އެއްބަސްވުން ހަދުމުގެ އިޚްތިޔާރު، މަސައްކަތް ހަވާލުކުރާ ފަރާތަށް ލިބިގެންވެއެވެ.

(ބ) ކަނޑައެޅިފައިވާ މުއްދަތަށް މަސައްކަތް ނިންމުމަށް މަސައްކަތް ހަވާލުވިފަރާތަށް ދަތިވާނަމަ ސަބަބު ބަޔާންކޮށް މަސައްކަތް ހަވާލުކުރިފަރާތަށް ބަޔާންކުރާ ހެއްކާއިއެކު ދުރާލައި ލިޔުމުން އަންގަންވާނެއެވެ.

8.2. މިގޮތުން ގެންނަ ބަދަލެއް ގެންނަންވާނީ ކަމާގުޅޭގޮތުން ދެފަރާތުން އެއްބަސްވާ ގޮތެއްގެ މައްޗަށް ލިޔުން ސޮއިކުރުމަށްފަހު މާލިއްޔަތު ޤަވާއިދުގެ 10.55 ވާއި އެއްގޮތްވާގޮތުގެ މަތިންނެވެ.

8.3. މި ލިޔުން ހިމެނޭނީ މި އެއްބަސްވުމުގެ ބައެއްގެ ގޮތުގައެވެ.

9. ކަނޑައެޅިފައިވާ މުއްދަތަށް މަސައްކަތް ނިންމުން.

9.1. މިގޮތުން މަސައްކަތް ހަވާލުވިފަރާތުގެ އިހުމާލެއްނެތި ބާރުނުފޯރާ ކަމެއްކަމުގައި ވާނަމަ މުއްދަތު އިތުރުކޮށްދިނުމުގެ އިޚްތިޔާރު މާލިއްޔަތު ވުޒާރާއި އެއްގޮތްވާގޮތުގެ މަތިން މަސައްކަތް ހަވާލުކުރިފަރާތަށް ލިބިގެންވާނެއެވެ.

9.2. މަޝްރޫޢު އުޖޫރައިން ކަނޑައަޅާފައިވާ މުއްދަތުތެރޭގައި މަސައްކަތް ނުނިމިއްޖެނަމަ ނަމަ، މާލިއްޔަތު ގަވާއިދުގެ 10.71 ވަނަ މާއްދާ ގައިވާ ގޮތުން އިތުރުވާ ކޮންމެ ދުވަހަކަށް ތިރީގައިވާ ގޮތުގެ މަތިން އެއްބަސްވުމުގެ އަގުން އުނިކުރެވިގެން ދާނެއެވެ.

9.3. ޖުމުލަ އަގު -/5،000،000 ރުފިޔާއަށްވުރެ ދަށުގެ ބިޑްތަކްނަމަ ފައިސާ ކަނޑާނީ، ޖުމުލަ އަގު 0.005 (ޕޮއިންޓް ސުފުރު ސުފުރު ފަހެއް) އާ ގުނަކުރުމުން ޖެހޭ އަދަދާ މުއްދަތަށްވުރެ އިތުރުވާ ދުވަސްތަކުގެ އަދަދާ ގުނަކުރުމުން ޖެހޭ އަދަދެކެވެ.

ލިކުއިޑޭޓެޑް ޑެމޭޖަސް = CP*0.005*LD

އަދި ޖުމުލަ އަގު -/5،000،000 ރުފިޔާއަށްވުރެ މަތީގެ ބިޑްތަކްނަމަ ފައިސާ ކަނޑާނީ، ޖުމުލަ އަގު 0.0025 (ޕޮއިންޓް ސުފުރު ދޭއް ފަހެއް) އާ ގުނަކުރުމުން ޖެހޭ އަދަދާ މުއްދަތަށްވުރެ އިތުރުވާ ދުވަސްތަކުގެ އަދަދާ ގުނަކުރުމުން ޖެހޭ އަދަދެކެވެ.

ލިކުއިޑޭޓެޑް ޑެމޭޖަސް = CP*0.0025*LD

CP (ކޮންޓްރެކްޓް ޕްރައިސް): ކޮންޓްރެކްޓްގެ ޖުމުލަ އަގު

LD (ލޭޓް ޑިއުރޭޝަން): ކޮންޓްރެކްޓްގެ މުއްދަތަށްވުރެ އިތުރުވާ ދުވަސްތައް

9.4.
- މި ގޮތުން މި އެއްބަސްވުމުގެ އަގަށް ބަލާއިރު ލަސްވާ ކޮންމެ ދުވަހެއްގެ ލިކުއިޑޭޓެޑް ޑެމޭޖަސްގެ ގޮތުގައި (ފައިސާގެ އަދަދު) ކޮންޓްރެކްޓުން އުނިކުރެވޭނެއެވެ.

9.5. މަތީގައިވާ ގޮތުގެ މަތިން ލަސްވުމުގެ އަގަށް ދޭންޖެހޭ ވަރު މުޅި ކޮންޓްރެކްޓުގެ 15% (ފަނަރަ އިންސައްތަ) އަށްވުރެ ބޮޑުވެގެން ނުވާނެއެވެ.

9.6. އެއްވެސް ހާލަތެއްގައި މުޅި ކޮންޓްރެކްޓުގެ އަގުގެ 15% (ފަނަރަ އިންސައްތަ) އަށްވުރެ ލިކުއިޑޭޓެޑް ޑެމޭޖަސް އިތުރުވެއްޖެނަމަ، ކޮންޓްރެކްޓުގެ ހުސްކުރުވި އޮތްބައި ކޮންޓްރެކްޓަރުގެ އަތުން ވަކިކުރެވިދާނެއެވެ. އަދި ކޮންޓްރެކްޓަރ ހިލާފުވި ފަރާތުގެ ޕަރފޯމަންސް ސެކިއުރިޓީ ނުވަތަ އެހެން ސެކިއުރިޓީއެއް ވާނަމަ ދޫނުކޮށް ހިފެހެއްޓޭނެއެވެ. މީގެ ތެރޭގައި ކޮންޓްރެކްޓަރ ދައްކަންޖެހޭ ލިކުއިޑޭޓެޑް ޑެމޭޖަސް ހިމެނޭނެއެވެ.

9.7. މި އެއްބަސްވުމުގައިވާ ކަންކަން ހާސިލުވަންދެން ނުވަތަ އެއްބަސްވުން ނިމުމަކަށް ގެންނަން ދެން މި އެއްބަސްވުން ދެމި ހުންނާނެއެވެ.

10. އެއްބަސްވުމުގެ މުއްދަތު

10.1. މިއެއްބަސްވުމުގެ މުއްދަތުގައި މިއެއްބަސްވުމުގެ ސަބަބުން ނުވަތަ މިއެއްބަސްވުމާއި ގުޅިގެން ނުވަތަ މިއެއްބަސްވުމުގައި ބަޔާންކޮށްފައިވާ ކަންތައްތައް ހައްލުކުރާނީ ދެފަރާތުން ސުލްހަވެރިކަމާއެކު ވާހަކަ ދައްކައިގެންނެވެ. އެފަދައިން ވާހަކަދެއްކުމުގައި އަދި ގޮތެއް ނިންމުމުގައި ދެފަރާތުން ޤަބޫލުކުރާ ފަރާތެއް ނުވަތަ ފަރާތްތަކެއް ބައިވެރިކުރުވިދާނެއެވެ.

11. ދިމާވާ މައްސަލަ ހައްލުކުރާނެ ގޮތް

11.1. ސުލްހަވެރި ނިމުމެއް މައްސަލައަށް ނުހޯދިއްޖެނަމަ، ދިވެހިރާއްޖޭގެ ކަމާބެހޭ ކޯޓަށް މައްސަލަ ހުށަހަޅައި ޝަރުޢީ ނިޔާމުގެގޮތުގައިން މައްސަލަ ނިންމުމަކުން މި އެއްބަސްވުން ހުރަހެއް ނާޅާނެއެވެ.

12. މުޢާމަލާތުކުރުން.

12.1. މި އެއްބަސްވުމުގައި ޝާމިލުވާ ފަރާތްތަކުން މިއެއްބަސްވުމާއި ގުޅިގެން އެއް ފަރާތުން އަނެއް ފަރާތަށް އަންގަންޖެހޭ އެންގުމަކީ އެންގުންތައް އާއްމުގޮތެއްގައި އަންގާނީ ލިޔުމުންނެވެ.

މަތީގައިވާ އެންމެހައި ކަންތައްތަކުގެ މައްޗަށް އެއްބަސްވެ މި އެއްބަސްވުމުގައި (ތާރީޚް) ވީ (ދުވަސް) ދުވަހު ދެފަރާތުން ސޮއިކުރީމެވެ.

މަސައްކަތު ހަވާލުކުރި ފަރާތް	މަސައްކަތާއި ހަވާލުވި ފަރާތް
(މަސައްކަތު ހަވާލުކުރި ފަރާތުގެ ނަން)	(މަސައްކަތާ ހަވާލުވި ފަރާތުގެ ނަން)
ނަން :	ނަން :
މަގާމު :	މަގާމު :
ހެކިން:	މަސައްކަތާއި ހަވާލުވި ފަރާތް
ސޮއި:	ސޮއި:
ނަން:	ނަން :
އައިޑީ ކާޑު :	އައިޑީ ކާޑު :