Ministry of Home Affairs

Cayman Islands Government

Supply and installation of Core Network

ID Number: CTC/13-14/MHA/017

TABLE OF CONTENTS

LIST OF TABLES

RFP Instructions

Executive Summary

The Government of the Cayman Islands through the Computer Services Department is seeking a firm price tender for a core network upgrade/replacement.

INVITATION TO TENDER

The Computer Services Department through the Ministry of Home Affairs invite suitably qualified vendors to submit a firm price proposal for the upgrade of the core network for the Government. The tender includes equipment and installation. For queries regarding this invitation contact the undersigned at MoHA@gov.ky . Responses will emailed to all who express an intention to tender.

The Cayman Islands Government does not bind itself to accept the lowest nor any tender. Late bids will not be accepted, CIG will not defray any cost incurred by bidders. The Cayman Islands Government shall not be bound to assign any reason for not accepting any tender and may accept a Tender in whole or in part.

The bidder must provide a brief summary of the proposal, highlighting the solution description and outlining the specific benefits to the Government of the Cayman Islands.

Business Objectives

The Computer Services Department of the Government of the Cayman Islands is a services based department within the Ministry of Home Affairs. It is the main supplier of shared IT and communications facilities and services across the government and includes a number of statutory organisations among its customers. Services include, hosting solutions, development, communications and operational maintenance.

CSD services approximately 2500 users across 60 departments and organisations. While it is not envisaged that the number of users will significantly grow over the next five years, it is anticipated that there will be significant increase in the demand for services as new technologies, connectivity and the growing trend of mobile technologies, data mining, electronic content and server virtualization.

CSD's mandate is to provide flexible, modern, secure, resilient and reliable services to its customers.

Overview of Data Center Core Network

Current Core Network

The Cayman Islands Government has a total of 5 Cisco Chassis Switches (4 x 6509's and 1 x 6506 being used to provide the core network for two main datacentres in two different buildings with 1 being at a third site. These two datacentres act as the main hub for central government, all remote switches link back to them by various means. The two data centres are linked together via 10 GB fibre and are geographically about 1 mile.

New network design principles

1) Network Design agnostic – Top of Rack, end-of-row, chassis based etc
2) Cloud Ready
3) Leveraging of existing technology in relation to existing edge and wan switches
4) High availability. If the network is down the business is down. The winning solution should be able to provide redundancy in hardware and load-sharing
5) resilient switching and routing technologies
6) High-performance - leverage a non-blocking crossbar fabric and multi-layer QoS prioritisation for VoIP and advance multicast routing and switching for video. That solution should ensure wire-speed delivery of IPv4 and IPv6 traffic.
7) Highly manageable – SNMP - Security can also be extended to the network management level with functions such as SSH v2 and SNMP v3 that authenticates and encrypts management traffic.
8) Total Cost of Ownership – Capital and 5 Year support/Maintenance costs are competitive
9) Ability to converge the core and aggregation layers into a single layer, creating a two-tiered model
10) Ability to use existing/generic GBICs on core switches
11) Ability to minimize the number of network switches in the datacentre while ensure maximum redundancy

New Network Must Have Requirements

1) IPv4
2) IPV6 support
3) Support for IPsec
4) Ipsec VPN support
5) Replace or interoperate with the current EIGRP routing protocol now in place at the core
6) redundancy at the core
7) redundant links between buildings
8) Increased bandwidth between buildings (40G) - Redundant 40 GB Single mode Fibre link between two datacentres - 0.75 Miles apart
9) Consolidated bandwidth to blade enclosures and dense virtualisation server (10g)
10) Out of band support for iSCSI between buildings, core and racks
11) QoS controls to allow for expansion of VOIP capabilities
12) support for full video-streaming and video-distribution over the LAN
13) stricter inter-VLAN access rule
14) Ability to support roughly 300 plus Linux and Windows servers with storage presented from 3PA, and P2000
15) Restrict Broadcast Domains
16) Spanning Tree Protocol (STP) security
17) VLAN Best Common Practices
18) Switching Infrastructure – Total Visibility
19) Switching Infrastructure – Complete Control

Optional Pricing Options

20) Wire speed – Fire wall at core and uplink ports
21) Virtual network configuration with VMware and Windows IP
22) SSL VPN
23) Future Proof - Wireless network capability – Out of band and for core network access
24) Load Balancing – across core – between racks

SAN Network Requirements

25) Out of band support for Fibre Channel between buildings, core and racks.
26) Legacy SAN switches need to be replaced. FC (Fiber Channel) count of at least 100 over two SAN fabrics with ability to expand.
27) Initially adopting FC to ensure continuity and FCOE/iSCSI in the medium to long term future.
28) Ability to support 3PAR F200 series, EVA 9000, P2000 enclosures, DAS, IP storage and, NAS solutions.

Objectives/Scope of Work

The scope includes supplying and installing all the necessary components to upgrade the network to a modern one capable of handling the needs of the Government including the near future. Subsequent to the upgrade of the core network, it is the Ministry's intention to upgrade or replace the components on the fringe of the network to improve performance. It is envisaged that the type of traffic will continue to change to include more streaming and as more government systems are brought online to the public there will be additional traffic. The network should be expandable to meet those future needs.

Environment the Data Center Network Will Support

Location and Resiliency

The Cayman Islands Government has a total of 5 Cisco Chassis Switches (4 x 6509's and 1 x 6506 being used to provide the core network for two main datacentres in two different buildings with 1 being at a third site. These two datacentres act as the main hub for central government, all remote switches link back to them by various means. The two datacentres are linked together via 10 GB fibre and are geographically about 1 mile.

Network site 1 (GAB)

1) Six server racks
2) Six HP c7000 Blade enclosures – Connected with stacked 4 x 10G uplinks (per 3 Enclosures) and 6 x 1G management ports per enclosure
3) Rack servers

Network site 2 (Citrus Grove)

1) Five server racks
2) Four HP c7000 Blade enclosures – Connected with stacked 4 x 10G uplinks (per 3 Enclosures) and 6 x 1G management ports per enclosure
3) 50 Rack Servers

Network Site 3 (Fire)

1) No server racks
2) Distribution to edge via 1gb

- The proposed data center resiliency strategy is active/active and the primary technologies to enable the strategy include DNS, replication, virtualization, and automatic fail over.
- Both the GAB and Citrus Grove locations are modern category 5 hurricane resistant buildings with backup power supply.

Applications and Users

- The primary Government applications housed in the data centers are real time mission critical transactional based applications supporting all government departments. It also includes the voice communication systems electronic content management and certain video streaming systems.
- The Government has applications with particularly stringent network performance or availability requirements including voice, video, big data and call center.
- The Government carries a number of virtualized servers and is seeking to capitalize on optimization platforms, including load-balancing, WAN Optimization and Web application firewall.

Devices, Compute and Virtualization

- It is anticipated that there will be continued growth of approximately 20% per year.
- Includes VMware, Oracle VM and hyperV.

Storage

- The storage includes a combination of fiber channels, NAS and direct attached. Future needs includes ISCSI.

Information Security

- Describe the security platforms, including firewall, VPN, SIEM, SWG, IDS/IPS, SWG and DLP solutions.

Liability and Reserved Rights

This RFP does not commit the government to pay any cost incurred in the preparation or submission of any proposal or to procure or contract for any services. The government will, at its discretion, award the contract to the bidder submitting the best proposal that complies with the RFP. The government may, at its sole discretion, reject any or all proposals received or waive minor defects, irregularities or informalities therein.

Bids considered being either abnormally high, or abnormally low, will be scored accordingly. Where there is an inconsistency in a bid, particularly in relation to the price tendered, the Cayman Islands Government reserves the right to clarify that price with the tenderer. There is no obligation to accept the lowest bid. All tenders are conducted in accordance with the procurement policy of the Ministry of Home affairs.

The Ministry of Home Affairs reserves the right to amend this RFP by an addendum issued up to five business days prior to the date set for receipt of proposals. Addenda or amendments will be emailed to all bidders that have copies of the RFP. If revisions are of such a magnitude as to warrant the postponement of the date for receipt of proposals, then an addendum will be issued announcing the new date.

Instructions to Bidder

This section outlines specific instructions for proposal submission. Bidder that does not adhere to these instructions may be subject to disqualification without further consideration.

Your Tender when completed is to be delivered, together with all other relevant documents to:

To:

The Central Tender Committee

c/o the Ministry of Finance

Government Administration Building,

#133 Elgin Avenue, George Town

Grand Cayman, KY1-9000 CAYMAN ISLANDS

Re: CTC/13- 14/MHA/017—Core Network Upgrade

The deadline for Tender submissions is Thursday, March 6, 2014, 12:00 noon.

The Tender and any other supporting documents stated when completed and signed are to be received not later than **Thursday, March 6, 2014, 12:00 noon** in a package which must not bear any indication of the bidder's identity. Tenders must be submitted in clearly marked envelopes; one for each proposal containing company information, Evidence of manufacture's authorization to sell and support equipment tendered, evidence of Trade and Business license, technical specifications of proposed equipment, warranty information, time period for delivery and the price proposed for the Tender.

The following documents are to be included with the proposal:

1. Company Information
2. Evidence of manufacture authorization to sell and support equipment tendered
3. Evidence of Trade and Business License to operate in the Cayman Islands or to operate a business in another country.
4. Technical Specifications of proposed equipment
5. Warranty Information
6. Time Period for Delivery
7. Time for validity of pricing
8. Completed Form of Tender
9. Equipment specification details
10. Pricing Matrix

General Procedures

Issuing Authority

This RFP is issued by The Ministry of Home Affairs:

- Contact Name: Tristaca Ebanks
- Department: Ministry of Home Affairs
- Street Address: 133 Elgin Ave, Georgetown, KY1-9000
- Telephone Number: 345 949 7900
- Email Address: MoHA@gov.ky

Price Guarantee

Bidder must guarantee its prices for a period of six months, beginning on the date of submission of the response to this RFP. In addition, the bidder must honor price and discounting structure for the duration of the project implementation, up to two years.

Preproposal Questions

Bidder must submit questions by emailing to:

- Contact Name: Tristaca Ebanks
- Department: Ministry of Home Affairs
- Street Address: 133 Elgin Ave, Georgetown, KY1-9000
- Telephone Number: 345 949 7900
- Email Address: MoHA@gov.ky

All questions must be received by February 27th, 2014 to allow for The Ministry of Home Affairs' response. Responses to these questions will be distributed by The Ministry of Home Affairs' to all bidders.

RFP Response Terminology

It is important for bidder to respond in a concise manner to each section of the RFP document.

Indicate the level of compliance with required specifications by replying with the following language:

- "Acknowledge" — The bidder has read and understands the information provided; however, no action is required by the bidder.
- "Comply" — The bidder meets the specifications.
- "Partially comply" — The bidder meets part of the specification; bidder should always explain how, or the deviation from the specification.
- "Comply with clarification" — The bidder meets the specification; however, the manner in which the bidder accomplishes this may be different from that specified in the RFP. The bidder should provide clarifying information.
- "Exception" — The bidder does not meet the specification. Please provide an alternative solution when possible.

Preparation of Proposals

Proposal Format

The complete proposal must include the proposal document with a point-by-point response to the RFP and all other materials requested. Bidder may include any additional materials it feels could assist in the evaluation of its proposed systems. However, bidder must provide complete solutions. References to other documents will not be accepted. Each vendor may supply up to three alternative bids. Where alternatives are supplied, each will be evaluated separately on its own merit.

Proposals that do not follow the RFP's format and content requirements will be subject to rejection without appeal. Bidders must supply three hard copies of each proposal in addition to one soft copy.

Proposal Due Date

All proposals must be received by 12:00 noon on March 6, 2014 and will be labeled: "Response to CTC/13-14/MHA/017 RFP for The Ministry of Home Affairs — Proposal No. [specify number, if appropriate]."

Proposal Delivery

Bidder is requested to submit a complete copy of the proposal to the contact presented above.

Proposal Inclusions

All equipment, accessories, training, software, hardware, licensing, maintenance, labour and materials must be furnished for the installation in a bill-of-material format. Any additional material or equipment necessary for installation, operation and maintenance of the system(s) not specified or described herein will be deemed to be part of the bidder's proposal.

Standard Agreements

The bidder must provide a copy of its standard product agreements that The Ministry of Home Affairs will sign if it awards the contract to that bidder. The Ministry of Home affairs requires five years full warranty and software and hardware support on all equipment supplied.

Proposal Modification and Withdrawal

Once the proposal is submitted, the bidder may modify or withdraw it only by appropriate notice to The Central Tenders Committee. Such notice will be in writing over the signature of the bidder. A bidder may resubmit a withdrawn proposal up to the time designated for the receipt of proposals, provided it then fully conforms to the general terms and conditions of the RFP.

Confidentiality

All information in this RFP is confidential and will not be disclosed to anyone other than those responding to this RFP.

All information regarding the terms and conditions, financial or technical aspects of the bidder's proposal that it considers to be of a proprietary or confidential nature shall be clearly marked "proprietary" or "confidential" at each relevant item or page or be marked in such a way in a statement covering the entire proposal.

Proposals submitted to The Ministry of Home Affairs for consideration will be held in confidence and not made available to other bidders for review or comparison. In all cases, bid responses will only be distributed to those directly involved with the bid evaluation — whether employees or contracted resources of The Ministry of Home Affairs. Proposals submitted and terms and conditions specified in each bidder's response will remain the property of The Ministry of Home Affairs.

The Ministry of Home Affairs reserves the right to publish the winning bid. For security reasons, the winning bidder will not publish, share or make public the architecture or details of the bid without permission from the Ministry of Home Affairs.

Calendar of Events

Table 1 reflects the project schedule.

Table 1. Project Schedule

Activity	Primary Responsibility	Date (Date Month Year)
RFP released to bidders	The Ministry of Home Affairs	February 19, 2014
Bidder's acknowledgment of intention to bid	Bidder	February 27, 2014

Activity	Primary Responsibility	Date (Date Month Year)
Provide preproposal questions by deadline	Bidder	February 27, 2014
Provide final questions by deadline	Bidder	February 27, 2014
Proposal Delivery	Bidder	March 6, 2014
Proposal opening	The Ministry of Home Affairs	March 7, 2014
Evaluation	The Ministry of Home Affairs	March 12, 2014
CTC Award	CTC	March 19, 2014
Contract negotiations completed	Bidder/The Ministry of Home Affairs	April 2, 2014
Final contract signed	Bidder/The Ministry of Home Affairs	April, 7 2014
Delivery of Equipment	Bidder	April 30, 2014
System installation and testing	Bidder with The Ministry of Home Affairs oversight	May 28, 2014
System cutover (no later than)	Bidder with The Ministry of Home Affairs oversight	June 16, 2014

Source: The Ministry of Home Affairs (February 2014)

Solution Architecture Overview

Bidder should provide an architectural solution overview, including

- A high-level network architecture/design description.
- A reference architecture on which the design is based. This should include references to documentation that is publicly available on the vendors' website.
- Description of the network topology being proposed. This includes the topology type (i.e., Spine/Leaf CLOS, ring, full-mesh or hierarchical) and number of physical and virtual tiers.
- Identify whether the solution uses a top-of-rack (ToR), end-of-row (EoR) or alternative design.
- Identify the primary elements of the solution and whether they are physical, virtual or software-based (e.g., physical switches, virtual switches, controllers and software).
- Description of the logical topology of the network being proposed. Vendor should clearly indicate where Layer 3 routing/switching is delineated from Layer 2 switching, as well as the protocols that are used at both Layer 3 and Layer 2.
- Description of the primary forwarding approach proposed and/or supported for the proposal (Spanning-Tree, TRILL, SPB, Layer 3 ECMP, SDN or a proprietary approach, etc.).
- A high-level overview of the management capability of the proposed solution.
- A high-level summary of the key differentiating aspects of the vendors' solution versus other leading vendors. Ideally, these differentiating characteristics should map to specific requirements for the The Ministry of Home Affairs environment.

Data Center Interconnect

- Provide a high-level diagram identifying how DCI will be accomplished in the proposed solution.
- Provide an overview of hardware/software options to meet The Ministry of Home Affairs's DCI requirements (e.g., physical interfaces and protocols to provide fault tolerance).

Hardware Requirements

This section identifies the hardware included in the bidder's solutions. It should only include products that are generally available and shipping. Any products not generally available (i.e., Beta or not yet shipping) at the time of this RFP should be explicitly noted. Bidder should specify:

- The number, type and speed of physical interfaces included in the proposal. Specify whether the interfaces support multiple speeds (e.g., hybrid 1G/10G) and whether the interfaces support Ethernet, Fibre Channel, Fibre Channel over Ethernet (FCoE) or Infiniband.

Note: This does not include interfaces that are required to interconnect the data center network itself. The number of interfaces specified here are available to plug devices such as servers into the network.

- Specify physical form-factor of devices required (chassis, stackable, appliances, etc.). Identify which (if any) of these network devices can optionally be delivered via software or virtual machine versus proprietary hardware (e.g., NFV). Identify the hypervisors that are supported.
- Describe how growth is accounted for and identify additional access interface capacity included in the proposal (e.g., for devices such as servers to plug in).
- Describe how growth is accounted for in the overall system design (e.g., scale-out versus scale-up) and how many network nodes can be added before new devices or modules must be added.
- Include data specification sheets for each class of hardware included in the proposal (as an appendix).
- Specify the degree of redundancy for the individual device components (power supplies, fans, supervisors, etc.).
- Specify the switching fabric capacity and the forwarding capacity of the individual network devices proposed (e.g., whether they are line-rate or oversubscribed) and of the overall topology proposed in the solution.
- Specify whether the devices proposed use a centralized, decentralized or hybrid forwarding plane. Identify which major functions and operations are performed in hardware versus software.
- Specify the interface packet buffers and the degree to which they are shared or dedicated.
- Specify the key physical operating characteristics of the device models proposed, including size, height, weight, airflow, power consumption, operating temperature and overall mean time between failure (MTBF) of the entire device.
- Specify the expandability of the devices — are they modular or upgradable from an interface and/or fabric perspective.
- Describe the cabling supported and required for the devices (e.g., copper, Fiber) and any transceivers required.
- Identify port-to-port latency between for individual devices (intraswitch latency) and within the physical data center solution proposed (i.e., best- and worst-case server to server latency within the proposed solution).
- Describe the CPU and memory of the devices, if not provided in the specifications literature.
- Describe any "green" initiatives or solutions included in the proposal.

- Describe any differentiating or highly innovative hardware capabilities compared with leading competitors.
- Refer to Appendix A and identify any protocols/standards that are **not** supported in the proposal.

Facilities Requirements

Physical Requirements

Bidder should specify:

- Floor space to support the proposed solution
- Floor-loading and elevation requirements
- Raised-floor requirements
- Minimum ceiling height
- Location of network interfaces (e.g., front, rear)
- Options for mass termination of cables
- FRUs that require removal of cables before replacement

(A diagram is optional.)

Environmental Requirements

Bidder should specify:

- System power circuit breaker panel location
- Lighting requirements
- Long- and short-term environmental ranges that the system can tolerate, including the:
  - Desirable temperature range
  - Desirable humidity range
  - Heat dissipation of the system at maximum configuration in British thermal units (BTUs) per hour
  - Required airflow (front to back, left to right, etc.)
  - Specialized rack requirements

Power Requirements

Bidder should specify:

- Voltage and phase parameters of the main components, such as switches and appliances.
- Circuit breaker panel requirements relative to the number of circuits and amperage ratings.
- Recommendations for reserve power requirements in stand-by hours and battery capacity (ampere-hours), if an uninterruptible power supply (UPS) is proposed.
- Centralized and local power and cooling requirements.

Software and Feature Requirements

This section identifies the software and features included in the bidders' solution as quoted. It should only include products that are generally available and shipping. Any products not generally available (e.g., beta or not yet shipping) at the time of this RFP should be explicitly noted. Bidder should identify:

General Software Requirements

- Describe the mechanism and/or options for the primary forwarding approach within the solution (examples include Spanning-Tree, TRILL/SPB, ECMP, SDN, Proprietary, etc.). Vendor should specify if any facets of the implementation are proprietary.
- Describe any differentiating or highly innovative features compared to leading competitors. Include whether these features are proprietary or not.
- Bidder must provide specific software versions recommended for each class of equipment, including release notes.
- Bidder should include documentation regarding open bugs or issues in the software proposed, ordered by priority (likely as an appendix).

Data Link and Network Layer Requirements

- Solution supports Layer 2 discovery protocols (i.e., LLDP) and should specify if they are proprietary or not.
- The number of MAC addresses and VLANs supported on the switching hardware.
- Support for IPv4 and IPv6 routing/forwarding. Vendor should specify the number of route entries supported and if forwarding occurs in hardware versus software.
- Solution supports Layer 3 unicast dynamic routing protocols, including OSPF and BGP. Vendor can list other protocols supported and should specify if any are proprietary..
- Solution supports multicast protocols, including PIM, DVMRP, IGMP, Snooping and MSDP. Vendor can list other protocols supported and should specify if any are proprietary.
- Solution supports first-hop gateway routing protocols, including VRRP. Vendor can list other protocols supported and should specify if any are proprietary.

- Solution supports Software-Defined Networking and overlay tunneling capabilities including OpenFlow, NVGRE and VXLAN. Bidder should also identify existing SDN controller(s) and available SDN applications.
- Solution supports VLAN tagging, VLAN trunking, Link Aggregation (LACP) and multi-chassis link aggregation.

Additional Software Features

- Describe which storage technologies are supported (e.g., FCoE along with the full data center bridging [DCB] suite, ISCSI, Fibre Channel and NAS).
- Identify quality of service capabilities, including the number of classes supported, rate-limiting and flow control. Identify whether these features are ingress/egress and if they are supported in hardware or software.
- Solution supports IP services including proxy ARP, DNS (client/server), DHCP (client, server, relay, snooping and Option 82, etc.).
- Solution supports protocols that provide metadata traffic flows (IPFIX, sFlow, Netflow, etc.), including specific versions.
- Solution supports traffic mirroring capability, commonly referred to as "port mirrors," "tap" or "span" ports. Identify the mirroring capacity (number of ports per device, capability for VLAN mirroring, etc.).
- List any additional stacking or virtual device clustering capability.
- Solution supports integration with virtualization software (VMware, Hyper-V, XEN, etc.). Describe the specifics of the integration.
- Refer to Appendix A and identify any protocols/standards that are not supported in the proposal.

Network Management Requirements

The purpose of this section is to ensure that the proposed solution meets The Ministry of Home Affairs's fault monitoring, network performance monitoring (NPM) and network configuration and change management (NCCM) requirements. This includes identifying how the hardware/software solution proposed integrates into The Ministry of Home Affairs's existing network management solutions, as well as any specialized management software that is included or embedded with the hardware/software solution proposed.

Vendor-Specific, Stand-Alone Network Management System

- Does the bidder have a dedicated stand-alone management system(s) or is the primary approach for the individual elements to feed existing management system(s)?
- Describe the capabilities of the dedicated, stand-alone management system, including the major functions provided.

- The management solution must support strong security features including, but not limited to, password attribute customization, authentication logging, role-based access, audit logs and multilevel authorization access.
- The bidder should describe any optional management tools it recommends to specifically enhance operations and the ability to manage the proposed solution.
- Describe any differentiating or highly innovative management features of the dedicated stand-alone management system.

Integration With Existing Management Solution

Note: In addition to integration with existing solutions, if any of the capabilities below are partially or fully met with the bidder's stand-alone network management system described above, that should be noted:

- List the basic element management protocols supported (Refer to Appendix A and identify any protocols/standards that are not supported).
- Describe the supported methods for integration with existing fault monitoring solution(s). This includes detection of troubles and component failures in the proposed system, as well as alarm monitoring and diagnostic tools.
- Describe the supported methods for integration with existing NPM solution(s).
- Describe the supported methods for integration with existing NCCM solution(s), including
  - Supported scripting tools (Perl, Python, Expect, Puppet, Chef, etc.).
  - Supported methods for configuration changes to hardware/software included in the proposal (identify if they are out-of-the-box connectors).
  - Supported methods for configuration backup and restoration and how to detect and alert on configuration changes.
  - Supported methods to perform a differential audit between configuration versions and establish and enforce compliance with network device configuration policies.
  - Methods supporting backup, recovery and update activities.
  - Methods to support software release version control, as well as to support the ability to undo a configuration change if it becomes necessary to determine the cause of a problem.
  - Methods to record and update the inventory in place/consumed across the organization, covering the following inventory items: hardware, software, licensing, services and maintenance.
- Describe the supported methods for integrating with virtualization software and cloud management platforms (standardized protocols, scripting tools and/or APIs, etc.).

Network Security Requirements

Security features of the solution must include, at a minimum, password requirements with configurable parameters, access authorization levels, authentication, secure access, logging activities, backup/restore and patching/update capabilities. Bidder should confirm compliance and describe security features of the proposed solution as requested below. Bidder should describe the following capabilities of the solution:

- IP and MAC access control lists — describe if they're applied on L3/L2 ports.
- Describe what features exist to support device partitioning (e.g., VRF) and multitenancy.
- Support for private VLANs.
- Ability to restrict network access on the interface level, either via DHCP or ARP interrogation, 802.1X or other mechanisms.
- Administrative user access levels to restrict administration access and flexible password configuration parameters (e.g., password length, aging, complexity).
- Support for strong (two-factor) authentication, authentication logging, auditing/accounting and RBAC. This applies to all components (physical/logical devices, controllers, etc.).
- Protection from unauthorized access.
- Protection from denial-of-service attacks.
- Ability to integrate with The Ministry of Home Affairs proposed security solutions in the data center, including Firewall, SWG and IDS/IPS.
- Bidders may propose an alternative firewall solution as an option.

Warranty, Maintenance and Training

Warranty

Bidder should specify the warranty periods for all solution hardware, as well as the software associated with running the proposed systems and applications. The Government requires at least five years full warranty and maintenance including software support. Any subsequent cost of support will be paid annually after year one.

Maintenance

The bidder must quote maintenance on a contractual basis — indicating the annual fixed maintenance rate after warranty expiration, including the rate for the next three years with an optional two years. The quotes for system maintenance options should include

- Hardware support including part replacement and RMAs

- Software support that entails new releases (including new features and/or bugs/vulnerability remediation)
- General technical support/assistance with operational and maintenance activities

The bidder should provide multiple levels of maintenance to choose from, including an emergency response time of no more than four hours, 24/7. However, The Ministry of Home Affairs will be able to choose different service levels for different devices. For instance, core and access switches may need different service levels. Bidders must detail on island availability of skill set to support the solutions proposed.

Bidder should:

- Define the number of factory-trained service technicians available through the local service depot (per physical data center location), and identify the centers from which technicians will be dispatched after hours, on holidays and during weekends.
- Provide a copy of the standard maintenance contract and details of optional extras.
- Describe committed response times and mean time to repair (MTTR) by type of service disruption.
- Provide a copy of normal maintenance escalation procedures, and include communications with affected parties — with names and contact details of all parties affected.
- Provide emergency contact number if normal channels of fault-reporting communications fail. Describe how that emergency contact number will be answered and by whom:

  (1) Are there any times or restrictions by day, week or month on this service?

  (2) What information will those answering a call have available?

  (3) Will they have specific information on the system being proposed for the organization?
- Describe the procedures for software updates and upgrades; detail what, if any, costs would be associated with upgrades.
- Define major and minor alarm conditions and how the system responds to each circumstance.
- Describe the capabilities for remotely monitoring the system.
- Describe the capabilities for automatically reporting fault conditions, both to organizational and supplier personnel.
- Indicate where the local and regional parts depots are located.
- Provide an inventory of all spare parts, including pricing that will need to be maintained in on-site inventory.

Training

Providers should describe what training of The Ministry of Home Affairs staff is required or recommended to use the provider's solution and services. The successful bidder will be required to provide online or on-site training and train-the-trainer sessions to users and system management communities. Trainers should have English as a first language. If training costs are not included as part of the system pricing response, then the bidder must provide those costs along with a detailed training schedule. The schedule should denote class sizes and length of a typical training session. The bidder shall also provide pricing for alternative modes of training delivery, if available.

Implementation

This section should include a detailed explanation of any professional services that are provided as part of the RFP response. Bidder should describe how it will manage the transition from current state to target state, including migration/implementation plans and handoff, clearly identifying who will provide the necessary resources and who will pay for them.

Bidder must provide an implementation plan that includes:

- Project stages and milestones
- Resources required
- Responsibilities of each of the parties
- Sources and skills required of the program and/or project manager(s)
- Sources and skills required of other resources and who will pay for them
- Communication processes for reporting the project's progress
- Recommendations for briefing the project manager, and possibly the organization's working party or steering committee members
- Implementation should include out of hours work to maintain availability of the system to users within normal working hours.

System Pricing and Licensing

Bidder should describe the pricing structure of the proposed solution and provide a bill of materials (BOM). The bidder shall offer methods of payment and all relevant payment terms. The BOM is a table or spreadsheet in editable electronic format with all pricing information showing line-item detail for any item that has a separate price, even if the item is sold as part of a bundle. ***All prices are to be duty free***.

Column headings should reflect:

- Part number
- Item description
- List price

- Discount amount
- Net unit price
- Quantity
- Total net price

Bidder should provide pricing for the following components:

- Hardware
- Software
- Licensing
- Maintenance
- Training
- Professional services (includes design)
- Implementation services
- Project management costs
- Documentation
- Delivery/Shipping costs
- Applicable taxes
- Optional capabilities

Finance

Provide a purchase agreement, with the terms and conditions. When there are currency exchange rate considerations in the prices quoted, define them and spell out policies to allow for fluctuations in exchange rates. The Ministry of Home affairs will pay no more than 25% on delivery of the equipment on site and the balance after hand over of a fully functioning system winning the specifications of the winning bid. More generous credit terms will be evaluated favourably.

Bidder Qualifications

Company History

The bidder must provide:

- A brief description of its company.
- A description of its experience in providing communication systems.
- Evidence of financial stability with an annual report, or audited financial statement.

- Name of the manufacturer of the proposed system.
- Name/location of a technical support center that provides remote maintenance.
- A list of other types of customer support available from the technical support center.
- At least three reference customers with similar requirements to the one proposed. Customer reference information must include company name and location, contact person, telephone number, email and the system name with model number.
- Customer references should include at least one from (1) the same market vertical of The Ministry of Home Affairs, (2) the same geographic region of The Ministry of Home Affairs and (3) a recent deployment (within the past 12 months).
- The quantity and location of qualified personnel available to support the proposed solution.
- All Qualification Statements submitted by the Tenderers must address each of the following mandatory requirements below:
    - A narrative description that the supplier is either an Original Equipment Manufacturer (OEM) or an authorized distributor of an OEM for the equipment
    - An assertion and evidence that supplier can and will provide after sales support. This should be evidenced by an inventory of trained personnel in the particular solution and commitment to carry the necessary parts and spares and facilities.
    - The Tenderer should provide assurance that the equipment can be delivered within one months of being awarded the contract. Should the proposed timeframe be in excess of above, this must be stipulated. Should there be a delay beyond the specified time for acts of god the request for additional time must be made in writing to the Ministry of Home Affairs. The Ministry is under no obligation to consider any such extension and may cancel the order upon such communication at its discretion.
    - A tender form completed in full by stating the price of the equipment delivered to the Cayman Islands. Note that this price should be duty free as this procurement has been given duty exemption status.

Responsibility for Proposed System Implementation

The bidder must include a statement describing the terms of the agreement with the manufacturer(s) of the proposed solutions. The statement must define the distributor's authorized territory; note the current contract expiration date; and include a statement from the manufacturer agreeing to support the product, the distributor and the buyer for a minimum of seven years.

If the bid is from more than one party, such as a combined proposal from a manufacturer and a distributor or system integrator, then the accountabilities of each party must be spelled out clearly. The prime contractor and the account management structure proposed must be acceptable to the customer.

Bidder's Support and Structure

The bidder should describe the structure of its organization, with organization charts showing the executive, engineering, sales and field support (installation, service and training) entities within the company.

The bidder should state how many people it employs in each of the following job categories and whether they are employees or contractors:

- Project management
- Engineering support
- Customer service
- Network device installation
- Training

A bidder should:

- Provide a copy of its most recent annual report, or at least a financial status statement including annual revenue, profit, net worth and other data.
- Have a technical support center that provides remote maintenance.
- Explain what other types of customer support are available from the technical support center.
- Describe its standards and processes for providing emergency service.

Bidder should provide references for at least three customers with comparable systems in terms of size, geography and features that The Ministry of Home Affairs is seeking. Customer references should be germane to The Ministry of Home Affairs' vertical market, such as finance, government, healthcare, hospitality or retail. References should include the company name, contact name, telephone number, email, and the system names or model numbers installed and used.

Evaluation Criteria

All tenders will be evaluated by the Tender Review Committee in accordance with the following criteria and weightings:

1. **Performance of the system**
   - Weighting: 15%
     - *Best performance bidder meeting or exceeding the specifications will receive 15%. In the event that two bidders in the opinion of the committee materially have the same level of performance, they will both be awarded 15%*
     - *Subsequent bids will be weighted by subtracting 5 percentage points from the amount awarded to the superior bid in this segment. The minimum attainable is(minus) -15%*

2. **Availability**
   - Weighting: 15%
     - *Highest availability achieving in excess of 95% meeting the specifications will receive 15%*
     - *Subsequent bids will be weighted based on relative price to the lowest bid meeting the specifications*
     - *Not meeting the minimum specifications or availability will be rejected*

3. **Support**
   - Weighting: 10%
     - *On Island qualified support with 24 hours response 10%*
     - *24 hour online and phone support with same day local support 8%*
     - *24 hour online and phone support with one day onsite response for production down 5%*
     - *24 hour online and phone support 0*
     - *Limited support or no assessed skilled team available rejected*

4. **Management**
   - Weighting: 10%
     - *Superior management capabilities of the system including ease of use 10%*
     - *Regular management capabilities or complex usage 5%*
     - *Regular management capabilities or easy usage 5%*
     - *Poor management capabilities rejected*
5. **Value for Money (VFM)**
   - Weighting: 30%
     - Lowest price of qualifying options meeting or exceeding the specifications evaluated for total cost of ownership over five years 30%
     - *Subsequent bids will be weighted based on relative total cost of ownership over five years to the lowest bid meeting the specifications*

6. **Payment Terms**
   - Weighting: 5%
     - *30 day or greater credit after installation 5%*
     - *Payment after hand over 3%*
     - *25% on delivery of equipment at site and payment after hand over 0*
     - *Prepayment will be rejected*

7. **Security**
   - Weighting: 15%
     - *Superiority in hardware and software security capabilities 15%*
     - *Better than minimum requirements plus ease of use 10%*
     - *Meet the minimum requirements plus ease of use 5%*
     - *Meeting the minimum security requirements in the tender requirement 0*
     - *Not meeting the minimum requirements rejected*

Ministry of Home Affairs

Cayman Islands Government

Government Administration Building,

133 Elgin Avenue, Georgetown, Grand Cayman, KY1-9000

Cayman Islands

FORM OF TENDER

To be returned by **Thursday, March 6, 2014, 12:00 noon**.

To: **The Central Tender Committee**

c/o the Ministry of Finance

Government Administration Building,

#133 Elgin Avenue, George Town

Grand Cayman, KY1-9000 CAYMAN ISLANDS

Re: CTC/13-14/MHA/017—Core Network Upgrade

To the Government of the Cayman Islands

I. We have perused the following documents:
   1. Invitation to Tenderers
   2. Instructions to Tenderers including the evaluation criteria that will be used to assess tenders
   3. Confidentiality provisions
   4. Form of Tender
   5. Equipment specification details
   6. Project Schedule
   7. Price matrix

II. We agree that the proper law of this Contract shall be Cayman Islands Law.

III. We agree that the essence of selective tendering is that the client shall receive bona fide competitive tenders from all those tendering. In recognition of this principle, we certify that this is a bona fide tender intended to be competitive, and that we have not fixed or

adjusted the amount of the tender by or under or in accordance with any agreement or arrangement with any other person. We also certify that we have not done and we undertake that we will not do at any time before the hour and date specified for the return of this tender any of the following acts:

a) communicate to a person other than the person calling for those tenders the amount or approximate amount of the proposed tender, except where the disclosure, in confidence, of the approximate amount of the tender is necessary to obtain insurance premium quotations required for the preparation of the tender;
b) enter into any agreement or arrangement with any other person that he shall refrain from tendering or as to the amount of any tender to be submitted;
c) offer or pay or give or agree to pay or give any sum of money or valuable consideration directly or indirectly to any person for doing or having done or causing or having caused to be done in relation to any other tender or proposed tender for the said work any act or thing of the sort described above. In this paragraph, the word "person" includes any persons and anybody or association, corporate or unincorporated; and "any agreement or arrangement" includes any such transaction, formal or informal, and whether legally binding or not.

IV. We undertake to satisfy the Government that the prices of the several items in the copy of the original Scope of Requested Equipment which we furnish with this tender are those on which our tender is based and that they bear reasonable relation to each other.

V. We agree that, should obvious error in arithmetic be discovered in any priced Scope of Works submitted by us during consideration of this offer, these errors will be corrected by giving us an opportunity of confirming our offer or of amending it to correct such errors. However, this provision cannot be used as an opportunity for bidders to change their price.

VI. Qualifying Criteria (Mark {X} all that apply)

A	Trade and Business Licence	☐
B	Authorised OEM distributor	☐
C	Technical Support Capabilities	☐
D	Able to execute Warranty	☐

VII. Subject to and in accordance with paragraphs II,III,IV and V above and the terms and conditions contained or referred to in the documents listed in paragraph I, we offer to supply the equipment referred to in the said documents in consideration of payment by the Cayman Islands Government of the sum shown in the Price Matrix.

Duly authorized to sign tenders for and on behalf of (in BLOCK CAPITALS) _____

_____

Postal Address _____

_____

Telephone No: _____ Date: _____ 19 _____

Email address: _____

NOTE: Bidders are reminded that tenders should be returned as follows:

Tenders must be submitted in clearly marked envelopes; one for each proposal containing company information, evidence of manufacturers authorization to sell and support equipment tendered, evidence of Trade and Business license, technical specifications of proposed equipment, warranty information, time period for delivery, and the price proposed for the Tender.

FORM OF TENDER (continued)

Envelope contents: (one envelope per solution)

1. Company Information
2. Evidence of manufacture authorization to sell and support equipment tendered
3. Evidence of Trade and Business License to operate in the Cayman Islands or to operate a business in another country.
4. Technical Specifications of proposed equipment
5. Warranty Information
6. Details of system performance
7. Details of system availability
8. Proposed management solution
9. Time Period for Delivery
10. Time for validity of pricing
11. Completed and signed Form of Tender
12. Equipment specification details
13. Completed Pricing Matrix (one per solution)
14. Document check list

Document Check list

Document	Included
Company Information	
Evidence of manufacture authorization to sell and support equipment tendered	
Technical Specifications of proposed equipment	
Warranty Information	
Details of system performance	
Proposed management solution	
Time Period for Delivery	
Time for validity of pricing	
Completed and signed Form of Tender	
Equipment specification details	
Completed Pricing Matrix (one per solution)	

Appendix A: Standards

Standard	Description
DCB/DCBx	Data Center Bridging
IEEE 802.1ab	LLDP
IEEE 802.1AE	MAC Security
IEEE 802.1d	MAC Bridging
IEEE 802.1p	L2 Prioritization
IEEE 802.1q	VL Tagging
IEEE 802.1qau	DCB-CN
IEEE 802.1qaz	DCB-ETS
IEEE 802.1qbb	DCB-PFC
IEEE 802.1s	MSTP
IEEE 802.1w	RSTP
IEEE 802.1x	NAC
IEEE 802.3ab	1000bT
IEEE 802.3ad	LACP
IEEE 802.3ae	10G Ethernet
IEEE 802.3ba	40G Ethernet
IEEE 802.3u	Fast Ethernet
IEEE 802.3x	Flwow Control
IEEE 802.3z	Gigabit Ethernet
iSCSI	
QSFP+	
RFC 768	UDP
RFC 783	TFTP
RFC 786	UDP
RFC 791	IPv4
RFC 792	ICMP
RFC 793	TCP
RFC 826	ARP
RFC 854	Telnet

Standard	Description
RFC 959	FTP
RFC 1027	Proxy ARP
RFC 1195	IS-IS
RFC 1215	SNMP Traps
RFC 1305	NTPv3
RFC 1350	TFTPv2
RFC 1519	CIDR
RFC 1542	BootP Relay
RFC 1591	DNS Client
RFC 1812	IPv4 Routers
RFC 1850	OSPFv2 MIB
RFC 1858	IP Fragmentation
RFC 1997	BGP Comm Attr
RFC 2096	IP Forwarding MIB
RFC 2131	DHCP Helper
RFC 2236	IGMPv2
RFC 2328	OSPFv2
RFC 2365	IP Multicast
RFC 2385	BGP MD5
RFC 2453	RIPv2
RFC 2460	IPv6
RFC 2474	DS Field
RFC 2545	BGPv4 Ext IPv6 IDR
RFC 2740	OSPFv3
RFC 2784	GRE
RFC 2858	Multiproto Ext BGP4
RFC 2865	RADIUS
RFC 2866	RADIUS Accounting
RFC 3021	31-Bit Subnet Masks
RFC 3036	LDP Specification

Standard	Description
RFC 3046	DHCP Relay Agent
RFC 3065	Confederations for BGP
RFC 3376	IGMPv3
RFC 3416	SNMPv2
RFC 3418	MIB for SNMP
RFC 3446	Anycast RP PIM/MSDP
RFC 3618	MSDP
RFC 3623	Graceful OSPF Restart
RFC 3630	TE Extensions OSPFv2
RFC 3768	VRRP
RFC 3810	MLDPv2 for IPv6
RFC 4254	SSH
RFC 4271	BGPv4
RFC 4382	MPLS or BGP Layer 3 VPN MIB
RFC 4456	BGP Route Reflection
RFC 4601	PIM-SM
RFC 4607	SSM
RFC 4610	Anycast-RP Using PIM
RFC 4724	Graceful Res BGP
RFC 4750	OSPF Version 2 MIB
RFC 4760	Multiproto Ext BGP4
RFC 4781	Graceful Res BGP/MPLS
RFC 4798	IPv6 Islands Over IPv4 MPLS
RFC 4893	BGP Four-Octet Number Space
SFP+	
SR4	