Public Works and Government Services Canada | Travaux publics et Services gouvernementaux Canada

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Récption des soumissions - TPSGC
11 Laurier St./11, rue Laurier
Place du Portage, Phase III
Core 0A1 / Noyau 0A1
Gatineau, Québec K1A 0S5
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

Revision to a Request for a Standing Offer
Révision à une demande d'offre à commandes

National Master Standing Offer (NMSO)

Offre à commandes principale et nationale (OCPN)

The referenced document is hereby revised; unless otherwise indicated, all other terms and conditions of the Offer remain the same.

Ce document est par la présente révisé; sauf indication contraire, les modalités de l'offre demeurent les mêmes.

Comments - Commentaires

Vendor/Firm Name and Address
Raison sociale et adresse du fournisseur/de l'entrepreneur

Issuing Office - Bureau de distribution
Network equipment and services/Equipment de réseau et services
Portage III 5C2
11 Laurier Street/11 rue Laurier
Gatineau, Québec K1A 0S5
Gatineau
Québec
K1A 0S5

Title - Sujet INTERNETWORKING EQUIPMENT	
Solicitation No. - N° de l'invitation EN578-030742/J	**Date** 2012-06-08
Client Reference No. - N° de référence du client EN578-030742	**Amendment No. - N° modif.** 008
File No. - N° de dossier 001nes.EN578-030742	**CCC No./N° CCC - FMS No./N° VME**
GETS Reference No. - N° de référence de SEAG PW-$NES-001-22322	
Date of Original Request for Standing Offer **Date de la demande de l'offre à commandes originale**	2011-02-22
Solicitation Closes - L'invitation prend fin **at - à** 02:00 PM **on - le** 2012-10-31	**Time Zone** **Fuseau horaire** Eastern Daylight Saving Time EDT
Address Enquiries to: - Adresser toutes questions à: St-Jean Valois(NES), Joanne	**Buyer Id - Id de l'acheteur** 001nes
Telephone No. - N° de téléphone (819) 956-1189 ( )	**FAX No. - N° de FAX** (819) 934-1411
Delivery Required - Livraison exigée	
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	
Security - Sécurité This revision does not change the security requirements of the Offer. Cette révision ne change pas les besoins en matière de sécurité de la présente offre.	

Instructions: See Herein

Instructions: Voir aux présentes

Acknowledgement copy required **Accusé de réception requis**	**Yes - Oui** □	**No - Non** □
The Offeror hereby acknowledges this revision to its Offer. **Le proposant constate, par la présente, cette révision à son offre.** **Signature**	**Date**	
Name and title of person authorized to sign on behalf of offeror. (type or print) Nom et titre de la personne autorisée à signer au nom du proposant. (taper ou écrire en caractères d'imprimerie)		
For the Minister - Pour le Ministre		

Canada

Modification 008 à la demande d'offres à commandes (DOC) relative à l'offre à commandes principale et nationale (OCPN) du Services de Soutien de L'Équipement de Réseau (SSER).

L'objectif de la présente est de modifier la DOC comme cela est décrit à l'appendice REV-10

===

APPENDICE "REV-10"

A cause d'un problème technique l'attachement Annexe A Appendice A Spécification Technique (réviser 1 juin 2012) est transmise via cette modification.

NESS – Equipment NMSO

Classes and Categories of Equipment

Technical Specifications

Annex A – Appendix A

2012 06 01

This page left intentionally blank

Table of Contents

This page left intentionally blank

Volume I, Part 3 - Technical Offer Instructions to Offerors

1. All technical specifications and requirements in this document are Mandatory, unless specifically identified with the words “Optional”.
2. To be eligible for a NMSO award in a given Network Equipment Category, a Technical Offer must be compliant with all Mandatory technical specifications in that category.
3. Compliance with Optional requirements is not a prerequisite of eligibility for a NMSO award.
4. Technical specifications are only relevant for the purpose of evaluating an Offer, and must be fully met as a pre-condition of being awarded a NMSO. Once a NMSO is awarded, the technical specifications in this Appendix are not relevant for the purpose of adding products, pursuant to Section 5 of Annex A.
5. Section 12 towards the end of this document defines common mandatory environmental requirements applicable to all of the Categories of equipment included within this Annex. Exceptions are defined within the list of technical specifications for a Category. Any compliant offer must include demonstrated compliance with the required environmental requirements.
6. In responding to the technical specifications and requirements in this Annex, the Offeror must propose a single product, or family of products, that are compliant with the:
    a. Class definition
    b. Category definition
    c. Technical specifications and requirements in that Category.

    The Offeror must provide for each Offer:
    a. The product/model number(s) being offered
    b. Compliance (Yes or No) for each mandatory technical specification and requirement
    c. *Substantiation documentation for each mandatory technical specification and requirement
    d. How compliancy is substantiated, by providing in table format a list of supporting reference material links.
7. The Offeror must use the same numbering scheme as in Annex A - Appendix A for each Class and Category for which an Offer is being submitted.

*Note: Substantiation documentation must be a publicly available technical brochure, manual, data sheet, or technical test reports certified by an independent third party. Substantiation documentation, or a written statement of compliance, cannot be created by the Offeror solely for the purpose of responding to this RFSO. A statement of non-compliance or missing substantiation documentation will result in the Offer being declared non-compliant.

1. Class – LAN Switches

Main Functionality: Network device to provide Ethernet local area network switching.

1.1. Category – L2 LAN Switches

Technical Definition:

Layer 2 Ethernet Switch that does not include Layer 3 routing functionality except in the management features.

Technical specifications for RFSO qualification only:

Propose one L2 switch model or family of models supporting the following requirements, features and protocols:

1) Architecture:
    a. Standalone or stackable

2) Port Density:
    a. Min 2 Small Form-Factor Pluggable (SFP) or GBICs, expandable to min of 16
    b. Min 24 RJ-45 ports, expandable to min of 192 RJ-45 and/or SC ports
    c. Support for min of 192 10/100Base-TX ports
    d. Support for min of 24 standard 1000Base-T (for full configuration)

3) Access Speeds & Interfaces:
    a. 10Base - TX / 100 Base-TX speed and duplex auto-sensing on each RJ-45 port
    b. 1000Base-T- RJ-45 SFP or GBIC
    c. 1000Base-SX SFP or GBIC
    d. 1000Base-LX SFP or GBIC

4) Performance (for full configuration 192 ports):
    a. Switching Fabric: no less than 30 Gbps
    b. Forwarding (64 byte packets): no less than 14 Mpps
    c. Number of MAC addresses supported: min 4096
    d. Number of VLAN configured: min 192
    e. Number of VLAN ID supported: min 192

5) Standards:
    a. Link aggregation as per IEEE 802.3-2002
    b. 10Base-T as per IEEE 802.3-2002
    c. 100Base-TX as per IEEE 802.3-2002
    d. Gigabit Ethernet 1000Base-T or SX or LX as per IEEE 802.3-2002

e. Auto-negotiation of speed and duplex mode for all data rates - IEEE 802.3-2002
f. Manual setting for speed and duplex mode for 10/100data rates - IEEE 802.3-2002
g. Full duplex mode, flow control as per IEEE 802.3-2002
h. Ethernet prioritization and CoS as per IEEE 802.1Q - 2003, IEEE 802.1p
i. VLAN tagging as per IEEE 802.1Q - 2003
j. STP, RSTP as per IEEE 802.1D, IEEE 802.1w
k. MSTP as per IEEE 802.1Q -2003 (Optional)
l. Security: IEEE 802.1x
m. IP multicast flooding prevention feature - IGMP snooping or equivalent

6) Management Features:
  a. CLI (command line interface) support
  b. SNMPv1 as per RFCs 1157, 1155, 1212, 1215 and SNMPv2c as per RFCs 1901, 2578–2580, 3416-3418
  c. SNMPv3 as per RFCs 3410 – 3415, 3584 (Optional)
  d. RMON I as per RFC 2819
  e. RMON II as per RFC 2021 (Optional)
  f. Telnet (RFC 854)
  g. TFTP (RFC 1350)
  h. DNS support (Optional)
  i. SNTP as per RFC 2030 or NTP as per RFC 1305
  j. Port mirroring
  k. A port must be provided for management and diagnostics
  l. Switch configuration must be stored in NVRAM, or an equivalent method of storing the configuration information during power down
  m. Requirement deleted
  n. Visual indication of the status of the device and components is required

7) Security Features:
  a. Support user authentication as per IEEE 802.1X
  b. Support user authentication via Radius or TACACS+
  c. MAC address filtering, MAC learning and locking
  d. Password encryption, Secured Shell

8) Informational: PoE support on all access ports – as per IEEE 802.af, Class 3

1.2. Category – L2-3 LAN Switches

Technical Definition:

Layer 2/3 Ethernet Switch / IP routing. The device may include hardware and software modules with specialized functionality that must be integrated within the device.

Technical specifications for RFSO qualification only:

Propose a Layer 2-3 LAN switch supporting the following requirements, features and protocols:

1) Physical specifications:
   a. 19" rack mountable unit

2) Redundancy:
   a. Add on modules for hot swappable redundant CPU and Power supply (Optional)

3) Port Density:
   a. Min 48 10/100/1000 Base-T Ethernet interfaces
   b. Min 48 1000 Base-SX MMF interfaces
   c. Min 2 10Gigabit ports

4) Access Speeds & Interfaces:
   a. 10Base-T / 100Base -TX - Speed and duplex auto-sensing
   b. 10Base-T / 100Base - TX or 1000Base - T - speed and duplex auto-sensing
   c. 1000Base-T
   d. 1000Base-LX or SX
   e. 10GBase-SR or LR
   f. 10Gbase-LX4 (Optional)

5) Performance:
   a. Switching fabric: min 80 Gbps.
   b. Forwarding: min 60Mpps
   c. Number of MAC addresses supported: min 16000
   d. Number of VLAN configured: min 1024
   e. Number of VLAN ID supported: min 4094
   f. Support for Jumbo Frames better than: 4000 bytes

6) Standards:
   a. Link aggregation as per IEEE 802.3 – 2002
   b. 10Base-T as per IEEE 802.3 - 2002
   c. 100Base-TX as per IEEE 802.3 – 2002
   d. Gigabit Ethernet 1000Base-T or SX or LX as per IEEE 802.3 – 2002
   e. Ten Gigabit Ethernet 10GBase-SR/LR as per IEEE 802.3ae

f. 10GBase-LX4 as per IEEE802.ae (Optional)
g. Auto-negotiation of speed and duplex mode for all data rates - IEEE 802.3-2002 (except 10GE data rate)
h. Manual setting for speed and duplex mode for 10/100data rates - IEEE 802.3 -2002
i. Full duplex mode, flow control as per IEEE 802.3 -2002
j. Ethernet prioritization and CoS as per IEEE 802.1Q -2003, IEEE 802.1p
k. VLAN tagging as per IEEE 802.1Q - 2003
l. STP, RSTP, as per IEEE 802.1D, IEEE 802.1w
m. MSTP as per IEEE 802.1Q- 2003 (Optional)
n. Security: IEEE 802.1x

7) IP routing:
   a. Inter VLAN IP routing
   b. Static routes, RIPv1, RIPv2, as per RFC1058, RFC 2453
   c. OSPFv2 as per RFC 2328
   d. BGPv4 as per RFC 1771 (Optional)
   e. IGMP RFC 1112, RFC 2236
   f. DHCP Relay –RFC 1541, RFC1542
   g. Protocol Independent Multicasting (PIM) –RFC 2362

8) QoS Features:
   a. 802.1Q-2003 CoS classification/ reclassification based on:
      i. Incoming physical port
      ii. Source / destination IP address
      iii. Source / destination MAC address (Optional)
      iv. TCP/UDP port number
   b. DSCP marking:
      i. Incoming physical port
      ii. Source / destination IP address
      iii. TCP / UDP port number
   c. ACL based per input port rate limiting

9) Management Features:
   a. CLI (command line interface) support
   b. SNMPv1 as per RFCs 1157, 1155, 1212, 1215 and SNMPv2c as per RFCs 1901, 2578–2580, 3416-3418
   c. SNMPv3 as per RFCs 3410 – 3415, 3584 (Optional)
   d. RMON I as per RC 2819;
   e. RMON II as per RFC 2021 (Optional)
   f. Telnet (RFC 854)
   g. Tools for managing software images and configuration files (can be web based, TFTP as per RFC 1350, FTP as per RFC 959, etc)
   h. DNS support (Optional)
   i. SNTP as per RFC 2030 or NTP as per RFC 1305
   j. Port mirroring

k. A port must be provided for management and diagnostics
l. Switch configuration must be stored in NVRAM
m. Requirement deleted
n. Visual indication of the status of the device and components is required

10) Security Features:
a. Support user authentication as per IEEE 802.1X
b. Support user authentication via Radius or TACACS+
c. MAC address filtering, MAC learning and locking
d. Password encryption, Secured Shell
e. Cryptographic modules must be FIPS 140-2 certified (Optional)

11) PoE support on all access ports – as per IEEE 802.af, Class 3 (Optional)

2. Class – Routers

<u>Main Functionality:</u> Network device for routing IP protocols, with the ability to interconnect multiple different networks that use the same or different routing protocols.

2.1. Category – Branch Routers

<u>Technical Definition:</u>

Small to medium capacity routers (less than 20 Mpps forwarding rate). The device may include hardware and software modules with specialized functionality that must be integrated within the device.

<u>Technical specifications for RFSO qualification only:</u>

Propose one small to medium capacity router model supporting the following requirements, features and protocols:

(Table Removed)

1) Access Speeds & Interfaces:
    a. 10BaseTX / 100BaseTX - speed and duplex auto-sensing

2) Performance (for full configuration 6 ports):
    a. Forwarding (64 byte packets): less than 20 Mpps
    b. Number of VLAN configured: min 8
    c. Number of VLAN ID supported: min 256

3) Standards (as applicable based on supported interface configuration):
    a. 10BaseT, 100Base-TX as per IEEE 802.3 - 2002
    b. Ethernet full duplex, flow control as per IEEE 802.3 -2002
    c. Ethernet prioritization and CoS as per IEEE 802.1Q -2003, IEEE 802.1p
    d. VLAN tagging as per IEEE 802.1Q - 2003
    e. Ipv4 - RFC 1812**.**
    f. IPv6 —Ipv6 Ready Logo certification (Optional)
    g. IPSec tunnelling with 3DES, AES support (Optional)
    h. Point-to-point and point-to-multipoint VPNs (Optional)
    i. Quality of Service (QoS) features
    j. Frame Relay support - RFC 2427 (Optional)
    k. ADSL - G.992.1 Annex A; RFC 2364, RFC 2684 (Optional)
    l. X.25 (Optional)

4) IP and Routing:
    a. Inter VLAN IP routing
    b. Static routes, RIPv1 and RIPv2 support - RFC1058, RFC 2453
    c. IGMP RFC 1112, RFC 2236, RFC 3376
    d. OSPFv2 as per RFC 2328

- e. BGPv4 as per RFC 1771
- f. Protocol Independent Multicast (PIM)
- g. Distance Vector Multicast Routing Protocol (DVMRP) (Optional)
- h. Policy Base Routing (PBR)
- i. Bootstrap Protocol, DHCP Relay–RFC 951, RFC1542, RFC2131
- j. Port Address Translation (PAT) (Optional)
- k. Network Address Translation (NAT) (Optional)
- l. IPX support (Optional)
- m. DLSw – RFC 1795 (Optional)

5) Security Features:

- a. Firewall capability (Optional)
- b. IEEE 802.1X (Optional)
- c. Access control Lists
- d. Password encryption, Secured shell
- e. RADIUS or TACACS+ support
- f. Cryptographic modules must be FIPS 140-2 certified (Optional)

6) Management Support:

- a. CLI
- b. SNMPv1 (RFCs 1157, 1155, 1212, 1215) and SNMPv2c (RFCs 1901, 2578–2580, 3416-3418)
- c. SNMPv3 (RFCs 3410 – 3415, 3584) (Optional)
- d. RMON I as per RC 2819;
- e. RMON II as per RFC 2021 (Optional)
- f. Telnet (RFC 854)
- g. TFTP (RFC 1350) (Optional)
- h. DNS support (Optional)
- i. SNTP as per RFC 2030 or NTP as per RFC 1305
- j. A port must be provided for management and diagnostics
- k. Requirement deleted

2.2. Category – Enterprise Router

Technical Definition:

Large capacity routers (greater than 20 Mpps forwarding rate). The device may include hardware and software modules with specialized functionality that must be integrated within the device.

Technical specifications for RFSO qualification only:

Propose one large capacity router model supporting the following requirements, features and protocols:

1) Access Speeds & Interfaces:
    a. 10 Base-TX / 100 Base-TX speed and duplex auto-sensing on each RJ-45 ports
    b. 100 Base-FX
    c. 1000 Base-SX SFP or GBIC
    d. 1000 Base-LX SFP or GBIC
    e. 10 Gig Ethernet-LX4, 10 GE-LR (Module Support) (Optional)
    f. T1 / DS1 (Optional)
    g. T3 / DS3 (Optional)
    h. ATM or POS over OC3, OC12, OC48 (Optional)

2) Performance (for full configuration):
    a. Switching fabric - no less than 700 Gbps (Optional)
    b. Maximum forwarding rate (64 byte packets): no less than 25 Mpps
    c. Number of MAC addresses supported: min 12000
    d. Number of VLAN configured: min 1024
    e. Number of VLAN ID supported: min 4094
    f. Support for Jumbo Frames better than: 4096 bytes

3) Standards:
    a. 10Base-T as per IEEE 802.3 - 2002
    b. 100Base-TX as per IEEE 802.3 – 2002
    c. Gigabit Ethernet 1000Base-T or SX or LX as per IEEE 802.3 – 2002
    d. Ten Gigabit Ethernet 10GBase-SR or LX4 or LR as per IEEE 802.3ae (Optional)
    e. Auto-negotiation of speed and duplex mode for all data rates - IEEE 802.3-2002
    f. Manual setting for speed and duplex mode for 10/100 data rates - IEEE 802.3 -2002
    g. Full duplex mode, flow control as per IEEE 802.3 -2002
    h. Ethernet prioritization and CoS as per IEEE 802.1Q -2003, IEEE 802.1p
    i. VLAN tagging as per IEEE 802.1Q - 2003

j. L2 switching present: STP, RSTP, MSTP as per IEEE 802.1D, IEEE 802.1w, IEEE 802.1Q- 2003 (Optional)
k. IPSec tunnelling with 3DES, AES support (Optional)
l. L2 Ethernet switching modules/ blades present: Port based network access control as per IEEE 802.1x (Optional)
m. Frame Relay –RFC 2427 (Optional)
n. Multiprotocol traffic over ATM AAL5 - RFC 2684 (Optional)
o. IP over ATM (Optional)
p. MPLS – RFCs: 2547, 2702, 2961, 3031, 3032

4) IP Routing:
a. Inter-VLAN IP routing
b. Static Routes, RIPv1, RIPv2, as per RFC1058, RFC 2453
c. OSPFv2 as per RFC 2328
d. VRRP RFC 3768 or an equivalent standby router/ redundancy protocol
e. IGMP RFC 1112, RFC 2236, RFC 3376
f. BGPv4 as per RFC 1771
g. Protocol Independent Multicast (PIM) – RFC 2362
h. Distance Vector Multicast Routing Protocol (DVMRP) – RFC 1075 (Optional)
i. Policy Base Routing (PBR)
j. DHCP relay
k. IPX support (Optional)
l. DLSw – RFC 1795 (Optional)
m. SDLC Support (Optional)
n. DHCP Relay–RFC 1541, RFC1542
o. IPv6 – Ipv6 Ready Logo certification.
p. IPv4 – RFC 1812
q. Network Address Translation (NAT) (Optional)
r. Port Address Translation (PAT) (Optional)
s. Multi-protocol routing support (Optional)

5) Advanced Features:
a. Multi Protocol Label Switching (MPLS)
b. Multi Protocol Label Switching Virtual Private Network (MPLS VPN) Layer 2 and 3
c. Multi Protocol Label Switching Quality of Service (MPLS QoS)
d. MPLS label imposition, disposition, and switching functionality
e. Virtual Routing Forwarding Customer Edge (Multi-VRF CE)
f. IEEE 802.1Q tunnelling
g. VLAN translation
h. Layer 2 (Ethernet, Frame Relay and ATM) transport over MPLS
i. Layer 2 Protocol Tunnelling (L2TP) (Optional)
j. Traffic shaping and priority queuing

6) Management Features:
    a. CLI support (command line interface)
    b. SNMPv1 (RFCs 1157, 1155, 1212, 1215) and SNMPv2c (RFCs 1901, 2578–2580, 3416-3418)
    c. SNMPv3 (RFCs 3410 – 3415, 3584) (Optional)
    d. RMON I as per RC 2819;
    e. RMON II as per RFC 2021 (Optional)
    f. Telnet (RFC 854)
    g. TFTP (RFC 1350) (Optional)
    h. DNS support (Optional)
    i. SNTP as per RFC 2030 or NTP as per RFC 1305
    j. Port mirroring
    k. A port must be provided for management and diagnostics
    l. Switch configuration must be stored in NVRAM
    m. Requirement deleted
    n. Visual indication of the status of the device and components is required
    o. Console port with dial-in support (Optional)

7) Security Features:
    a. Standard security with access control lists
    b. Support user authentication via Radius or TACACS+
    c. MAC address filtering, MAC learning and locking
    d. Password encryption, Secured Shell
    e. Cryptographic modules must be FIPS 140-2 certified (Optional)

3. Class - Layer 4-7 Devices

Main Functionality: Network device to improve Layer 4-7 network data traffic.

3.1. Category – Layer 4-7 Application Switch

Technical Definition:

Network Layer 4-7 device to switch/ forward network data traffic. The device may include hardware and software modules with specialized functionality that must be integrated within the device.

Technical specifications for RFSO qualification only:

Propose one application switch model supporting the following requirements, features and protocols:

1) Architecture:
    a. Fixed configuration device or modular unit
    b. Redundant power supply (Optional)

2) Performance and Port Density:
    a. Port density: min. 2 Gigabit Ethernet (SFP or GBIC), or min. 4 RJ45 ports, GE or FE
    b. Overall throughput: no less than 1Gbps
    c. L7 requests per second: no less than 15000
    d. Min concurrent connections: 800,000
    e. SSL TPS: at least 1000 (Optional)
    f. Number of VLAN ID supported: min 512

3) Features:
    a. Load balancing:
        i. Layer 4-7 load balancing
        ii. Load balancing of any IP traffic, including but not limited to HTTP, HTTPS, FTP, TCP, UDP
        iii. IP address / port based load balancing redirection
        iv. Balancing methods: round-robin; least connections
        v. Dynamic balancing methods based on balanced object load and / or response time
        vi. Customizable balancing methods (user scriptable or GUI interface)
        vii. Content based customizable balancing methods (user scriptable or GUI interface)
        viii. L2-7 traffic shaping / rate limiting (Optional)
        ix. Support for all standard browsers (MS, Netscape)

b. Application acceleration (Optional):
   i. HTTP compression
   ii. Internal caching
   iii. TCP optimization
   iv. Compression support for HTML, XML, Javascript, CSS

c. SSL Acceleration (Optional):
   i. Integrated SSL acceleration (server offload)

d. Availability:
   i. Active-active and active-standby redundancy
   ii. Application health checking
   iii. User scriptable health checking

e. Session Persistence:
   i. TCP, HTTP session persistence
   ii. SSL offload is present: HTTPS session persistence (simultaneous support for cookie persistence and SSL) (Optional)

f. Security:
   i. Defends against SYN flooding attacks
   ii. Defends against DoS attacks
   iii. Radius authentication support
   iv. LDAP (Optional)
   v. Access control lists

g. Management:
   i. Sophisticated reporting: real-time and historical
   ii. Monitoring utilities
   iii. Command Line Interface (CLI)
   iv. Web browser management interface supporting HTTPS
   v. SNMPv1 (RFCs 1157, 1155, 1212, 1215) and SNMPv2c (RFCs 1901, 2578–2580, 3416-3418)
   vi. Central management software and SNMP MIB support (Optional)
   vii. A port must be provided for management and diagnostics

4) Access Speeds & Interfaces:
   a. 10 Base-TX / 100 Base-TX Speed and Duplex auto-sensing or 1000Base-TX on each RJ-45 port
   b. 1000 Base-SX SFP or GBIC
   c. 1000 Base-LX SFP or GBIC

5) Standards:
   a. 10Base-T as per IEEE 802.3 - 2002
   b. 100Base-TX as per IEEE 802.3 – 2002
   c. Gigabit Ethernet 1000Base-T or SX or LX as per IEEE 802.3 – 2002
   d. Auto-negotiation of speed and duplex mode for all data rates - IEEE 802.3 - 2002
   e. Manual setting for speed and duplex mode for all data rates - IEEE 802.3 - 2002

f. Full duplex mode as per IEEE 802.3- 2002
g. Ethernet prioritization and CoS as per IEEE 802.1Q -2003, IEEE 802.1p (Optional)
h. VLAN tagging as per IEEE 802.1Q
i. STP, RSTP, MSTP as per IEEE 802.1D, IEEE 802.1w, IEEE 802.1Q – 2003 (Optional)

6) IP Routing (Optional):
   a. Static Routes, RIPv1, RIPv2, as per RFC1058, RFC 2453
   b. OSPFv2 as per RFC 2328
   c. BGPv4 as per RFC 1771
   d. IPv6 ready logo certification
   e. IP v4 full support – RFC 1812, RFC2644

7) Certifications:
   a. SSL offload present (see 3ci): FIPS 140-2 (level 2) (Optional)

3.2. Category – WAN Acceleration Appliance

Technical Definition:

Network device for accelerating network data traffic over WAN links. The device may include hardware and software modules with specialized functionality, which must be integrated within the device.

Technical specifications for RFSO qualification only:

Propose one WAN accelerator appliance model supporting the following requirements, features and protocols:

1) Architecture:
   a. Fixed configuration device or modular unit
   b. Hot swappable dual redundant power supply (Optional)

2) Performance and Port Density:
   a. Port density: min 2 Fast Ethernet
   b. Concurrent sessions: min 200
   c. Throughput: min 500Kbps
   d. Data compression: at least 90%

3) Features:
   a. Data compression:
      i. Applicable to all types of applications, all protocols and all data types
      ii. Requirement deleted
      iii. Supports encrypted data transfers
      iv. Informational: data compression can be based on caching, dictionary of repeated patterns, protocol optimization, application optimization, etc.
   b. Availability:
      i. Fail to wire
      ii. Support for redundant router configuration
   c. Security:
      i. Authentication support TACACS+ or Radius

d. Management:
   i. Web browser management interface
   ii. SNMPv1 (RFCs 1157, 1155, 1212, 1215) and SNMPv2c (RFCs 1901, 2578–2580, 3416-3418)
   iii. Sophisticated reporting: real-time and historical
   iv. Export utilities
   v. Central management software and SNMP MIB support (Optional)
   vi. Secure HTTPS web browser management interface (Optional)
   vii. A port must be provided for management and diagnostics

4) Access Speed & Interfaces:
   a. 10Base-T / 100 Base-TX speed and duplex auto-sensing
   b. 1000 Base-T or 1000 Base-SX or LX SFP

5) Standards:
   a. 10Base-T as per IEEE 802.3 - 2002
   b. 100Base-TX as per IEEE 802.3 – 2002
   c. Gigabit Ethernet 1000Base-T or SX or LX as per IEEE 802.3 – 2002 (Optional)
   d. Auto-negotiation of speed and duplex mode for all data rates - IEEE 802.3 -2002
   e. Full duplex mode as per IEEE 802.3 -2002
   f. Support for VLAN tagging as per IEEE 802.1Q -2003 (Optional)

6) Minimum environmental operating and non-operating conditions applicable to category 3.2 WAN acceleration appliance:
   a. Operating conditions:
      i. Temperature: 10° - 35°C
      ii. Relative humidity (non-condensing): up to at least 80%
      iii. Altitude: 0 – 1500m
   b. Non-operating conditions:
      i. Temperature: -20° to +60°C
      ii. Relative humidity (non-condensing): up to at least 80%

4. Class - Firewalls (deleted)

5. Class – Intrusion Detection Systems

<u>Main Functionality:</u> Network device to detect, monitor and analyse activity on a network.

5.1. Category – Remote Response NIDS (Network Intrusion Detection Systems)

<u>Technical Definition:</u>

Network appliance for detecting anomalous and/or unauthorized activity on a network.

<u>Technical specifications for RFSO qualification only:</u>

Propose one NIDS model supporting the following requirements, features and protocols:

1) Port Density:
    a. Min port density 4 10/100 Base TX ports
    b. 1000Base-SX or LX or 1000Base-T port (Optional)
    c. Requirement deleted
    d. Min performance: peak throughput 400Mbps; Max concurrent sessions 250,000

2) Performance:
    a. The packet capture must supports 10/100 bit speeds with no loss (multiple interface support).
    b. IDS must be able to handle variations in traffic, both natural and induced, without failure or loss of coverage.

3) Standards:
    a. 10Base-T as per IEEE 802.3 - 2002
    b. 100Base-TX as per IEEE 802.3 – 2002
    c. Gigabit Ethernet 1000Base- T or SX or LX as per IEEE 802.3 – 2002
    d. Auto-negotiation of speed and duplex mode for all data rates as per IEEE 802.3 -2002 (Optional)
    e. Manual setting option for speed and duplex mode for all data rates as per IEEE 802.3 -2002
    f. Requirement deleted
    g. NTP v2 (or above) or Simple Network Time Protocol (SNTP) RFC 2030.
    h. VLAN Tagging as per 802.1Q – 2003
    i. SNMP
    j. Secure Shell SSH

4) Physical specifications:
    a. 19” Rack mountable unit

5) Architecture:
    a. Standalone system that has a passive detection component that does not sit in line.
    b. The NIDS must be able to work in what is known as “promiscuous mode”. This means that they must be able to examine every packet on a local segment.
    c. The NIDS sensors must allow monitoring of traffic on the wire in real time.
    d. Local console port should be included for remote and local sensor configuration and maintenance (Optional)
    e. The Supplier should support redundancy within the solution. Redundancy could be achieved by provisioning in a clustered environment and by providing dual power supplies. (Optional)

6) General:
    a. Analysis of packet information must occur at the sensor
    b. Processing of IP packets regardless of the Transport Layer overlying the IP packet
    c. The NIDS must be able to fully reassemble the original traffic flow.
    d. A time out mechanism must alert the management station if the sensor goes down.
    e. IDS should be VLAN aware (802.1Q). This means both being aware of VLAN groupings as well as being able to handle various forms of encapsulation. (Optional)
    f. IDS should be Multi-Protocol Label Switching (MPLS) Aware (Optional)
    g. IDS should have a built-in Defrag Processor (Optional)

7) Data Forensics, Logging and Auditing:
    a. All changes to system configuration must be recorded in logs
    b. Loss/establishment of time synchronization with NTP source must be noted in logs.
    c. The Operating System must allow audit-trail management, with recognition of user activity reflecting policy (Optional)
    d. All traffic alerts must be recorded in logs
    e. All unauthorized attempts to access the admin interface must be recorded
    f. The solution should allow logging in ASCII format (Optional)
    g. The solution must allow logging to alternate data stores and data sources
    h. The solution must support the ability to set filters
    i. The IDS must support some mechanism by which the entire packet or packets (payload and headers), which triggered an alarm, are captured
    j. Data logs must be exportable to third party products

8) Management Features:
    a. Graphical User Interface
    b. Command Line Interface (Optional)

c. Administrator and log viewing accounts having varying access and administrative privileges where access is restricted based on username, User ID and password
d. Administrator and log viewing accounts having varying access and administrative privileges where access is restricted based on source IP address and / or network (Optional)
e. The management software must be able to run on commonly used operating system platforms including Windows, Linux or Solaris (Optional)
f. A port must be provided for management and diagnostics

9) Central Management System (Optional):
   a. Security policy management, configuration and real-time log viewing capabilities from multiple remote management workstations
   b. Encrypted remote management and configuration capabilities (i.e. SSH or https)
   c. The solution should support the ability to prioritize attacks in order to show the most dangerous attacks that are currently happening
   d. The IDS should notify when packets are dropped
   e. The IDS should notify the overall percentage of collected traffic the dropped packets represent
   f. The solution should support the ability to notify an administrator via e-mail, pager, and/or SNMP trap
   g. The solution should support an acknowledgement function at the console via a pop up window or other similar mechanism if a specific event occurred
   h. The management package should support global properties to update sensors or components at once. The management package should allow remote sensor upgrade
   i. The management package functionality should include: establishing security policies, creating groups and assigning sensors to different groups
   j. The management package should support the ability to group attack signatures into groups or policies for applying to sensors
   k. Reporting features: generation of hourly, weekly, daily and ad hoc reports

10) Security Features:
   a. The NIDS sensors must examine packets in detail in order to detect patterns of misuse
   b. Content based scanning examines packets and traffic streams for specific patterns signatures (Match against a database of known “attack signatures”) and/ or behaviours
      i. Exploit-based signatures
      ii. Vulnerability-based signatures
      iii. Automated signature update process overview and frequency
      iv. Cryptographic controls using MD5 supporting signature integrity (Optional)

c. Protocol anomaly (traffic scrubbing): decodes packets and checks protocol fields for deviations from RFCs and from industry defined application protocols
d. Must perform packet inspection to ensure packets are part of established flows
e. Rate-based: detects unusual traffic which has not previously been observed (Optional):
   i. Must perform statistical analysis for abnormal activity patterns.
   ii. Statistical analysis must extend beyond IP Header and including TCP/UDP and ICMP
f. The solution must permit user/client to create and deploy its own customized signatures
g. The sensor must be able to monitor the protocols that are used to maintain the network infrastructure for known attack against protocols. This must include such protocols as OSPF and SNMP (Optional)
h. The sensor must be able to provide detection for a number of common application protocols. These must include DNS, RPC, HTTP, SMTP and FTP
i. The sensor must incorporate a hardened operating system
j. When suspicious activities are noticed, the network-based IDS must raise alerts
k. The IDS response must be configurable on a per attack or policy basis
l. The sensor must be able to detect attacks even if the attackers are using evasion technique such as IP fragmentation, TCP fragmentation, TCP stream and/or Unicode obfuscation

11) Security Certifications and Standards (Optional):
   a. The signature description should include links to CVE (Common Vulnerabilities and Exposures
   b. The system message structure should be compliant with current IDS data exchange format standards (IDMEF and/or SDEE)

5.2. Category – IDS Balancers

Technical Definition:

Network device for aggregating, filtering, and load balancing Network Intrusion Detection Systems (IDS) or network security monitoring solutions.

Technical specifications for RFSO qualification only:

Propose one NIDS balancer model supporting the following requirements, features and protocols:

1) Port Density: min 6 Fast Ethernet ports and min 4 GE ports

2) Access Speeds & Interfaces:
    a. 10/100Base-TX, speed and duplex auto-sensing on each port and the capability to statically set speed and duplex on all ports
    b. 1000Base- T or SX or LX

3) Standards:
    a. 10Base-T as per IEEE 802.3 - 2002
    b. 100Base-TX as per IEEE 802.3 - 2002
    c. Gigabit Ethernet 1000Base- T or SX or LX as per IEEE 802.3 - 2002
    d. Auto-negotiation or manual setting option of speed and duplex mode for all data rates as per IEEE 802.3 - 2002
    e. Flow control as per IEEE 802.3 - 2002
    f. 802.1Q VLAN tag stripping
    g. Ability to Load-balance across multiple IDS devices based on the type and source of network traffic.
    h. Traffic aggregation of multiple input ports.
    i. Mirror traffic to multiple output groups of IDS sensors
    j. Ability to mirror all standard network traffic traversing a network cable out through the monitoring interfaces, including network errors
    k. Ability to mirror all non-standard network traffic traversing a network cable, including network packets that do not conform to any established protocol standards, out through the monitoring interfaces

4) Performance:
    a. Rated or raw throughput: at least 400Mbps
    b. Concurrent sessions: at least 500,000
    c. Sessions teardown for deep packet inspection: at least 50,000/sec
    d. SYN Flood protection (from DOS attacks): at least 250,000/sec.

5) Management Features:
    a. Encrypted remote management and configuration capabilities
        i. Secure web interface using SSL v3.1 and/or TLS v1.0
        ii. SSH Version 2

b. A port must be provided for management and diagnostics

6) Security Features
    a. Remote management can only be done on an isolated physical port
    b. Traffic cannot physically travel from an output port out through an input port
    c. IP based Access Control lists in order to control which hosts can connect to the device in order to perform remote management
    d. All remote management traffic must be encrypted

5.3. Category – Network Non-aggregator Ethernet TAPs

Technical Definition:

Network device for monitoring and analysing network traffic activity over a single network segment. Includes single-port and multi-port TAPs.

Technical specifications for RFSO qualification only:

Propose non-aggregator TAPs supporting the following requirements, features and protocols:

1) Tapping Density:
    a. Min of one network and mirror traffic out of two monitoring interfaces (one for each direction of the tapped link).

2) Access Speeds & Interfaces:
    a. 10/100/ Base-TX
    b. 1000Base-T
    c. 10/100/1000Base-TX
    d. Gigabyte fibre 1000Base - SX or LX
    e. 10 Gigabyte fibre 10Gbase- SR or LR

3) Standards:
    a. 10Base-T as per IEEE 802.3 - 2002
    b. 100Base-TX as per IEEE 802.3 – 2002
    c. Gigabit Ethernet 1000Base- T or SX or LX as per IEEE 802.3 – 2002
    d. Ability to mirror all standard network traffic traversing a network cable out through the monitoring interfaces, including network errors
    e. Ability to mirror all non-standard network traffic traversing a network cable, including network packets that do not conform to any established protocol standards, out through the monitoring interfaces.
    f. Each direction of the tapped link is mirrored out separate monitoring ports (non-aggregated traffic mirroring)

4) Performance:
    a. TAP must mirror 100% of all traffic traversing the tapped link out through its monitoring ports with 0% packet loss
    b. A power failure on the TAP must not affect the tapped link
    c. A power restore on the TAP must not affect the tapped link
    d. The tap must not impact the tapped link in any way
    e. Compatible with Power over Ethernet applications
    f. Min: two power supplies for power redundancy

5) Management Features:
    a. LED indicators that show the TAPs power status

6) Security Features:
    a. Physically impossible for traffic to travel from a monitoring port out through the import port

5.4. Category – Network Aggregator Ethernet TAPs

Technical Definition:

Network device for monitoring and analysing network traffic activity over multiple network segments. Includes single-port and multi-port TAPs.

Technical specifications for RFSO qualification only:

Propose aggregator TAPs supporting the following requirements, features and protocols:

1) Tapping Density:
   a. Min one network and mirror to a single aggregated monitoring port.

2) Access Speeds & Interfaces:
   a. 10/100Base-TX
   b. 1000Base-T
   c. 10/100/1000Base-TX
   d. Gigabyte fibre 1000Base-SX or LX
   e. 10 Gigabyte fibre 10Gbase-SR or LR.
   f. All input and monitoring ports must be manually set to auto or static speed and duplex settings by using DIP switches (or similar method), except models that are built to operate in only one fixed mode (example: 10000BaseTX full duplex).

3) Standards:
   a. 10Base-T as per IEEE 802.3 - 2002
   b. 100Base-TX as per IEEE 802.3 - 2002
   c. Gigabit Ethernet 1000Base- T or SX or LX as per IEEE 802.3 - 2002
   d. Ten Gigabit Ethernet 10GBase-SR or LR as per IEEE 802.3ae
   e. Ability to mirror all standard network traffic traversing a network cable out through the monitoring interfaces, including network errors
   f. Each direction of the tapped link is mirrored out a single aggregated monitoring port

4) Performance:
   a. Min 16 megabytes buffers for 10/100Base-TX TAPs
   b. Min 128 megabytes for 1000Base-TX aggregator TAPs
   c. TAP must mirror 100% of network traffic traversing the tapped link out through its monitoring ports with 0% packet loss.
   d. A power failure on the TAP must not affect the tapped link.
   e. A power restore on the TAP must not affect the tapped link.
   f. TAP must not impact the tapped link in any way.
   g. Compatible with Power over Ethernet (PoE) applications
   h. Min two power supplies for power redundancy.

5) Management Features:
   a. LED indicators that show the TAPs power status
   b. LED indicators that show the status of each port

6) Security Features:
   a. Physically impossible for traffic to travel from a monitoring port out through the import port

6. Class – VPN Appliances

<u>Main Functionality:</u> Network device to enable secure and private data communication on a network.

6.1. Category – Small Remote Site VPN Appliance

<u>Technical Definition:</u>

Network device for deployment of IPSec VPNs over packet public switched networks, for small and remote sites, *with no remote client support*.

<u>Technical specifications for RFSO qualification only:</u>

Propose one VPN appliance model for small and remote sites supporting the following requirements, features and protocols:

1) Architecture:
    a. Single VPN appliance with integrated 4+ port switch
    b. A single flat subnet
    c. WAN connectivity - one of the following options:
        i. ADSL (via PPPoE or Optional on-board modem)
        ii. Ethernet
    d. Requirement deleted
    e. Requirement deleted
    f. No remote client support required for this category – branch-to-branch tunnel only

2) Standards:
    a. 10Base-T as per IEEE 802.3 - 2002
    b. 100Base-TX as per IEEE 802.3 - 2002
    c. ADSL - G.992.1 Annex A, Annex B; RFC 2364, RFC 2684 (on appliances with built-in ADSL modems) (Optional)

3) Protocol Support/Services:
    a. Network Time Protocol (NTP) v2 or above
    b. Simple Network Management Protocol
    c. Dynamic Host Configuration Protocol (DHCP) server for local clients
    d. Dynamic Host Configuration Protocol (DHCP) client for external interface
    e. Point-to-Point Protocol over Ethernet (PPPoE) client
    f. A port must be provided for management and diagnostics
    g. Telnet server or Secure Shell (SSH) for device management

4) Virtual Private Networking:
    a. Aggressive and main mode support
    b. Encryption cyphers

    i. 256-bit Advanced Encryption Standard (AES)
    ii. 128-bit Advanced Encryption Standard (AES)
    iii. 112-bit or 168-bit Triple Data Encryption Standard (3DES)
c. Hashing algorithms:
    i. Secure Hash algorithm (SHA-1) as per RFC 3174
    ii. Message Digest (MD5) as per RFC 1321
d. Internet Key Exchange (IKE) algorithm
e. Authentication for key management:
    i. Pre-shared secrets
    ii. 1024-bit and 2048-bit X.509 certificates
f. IP Security (IPSec):
    i. Authentication Header (AH) as per RFC 1826
    ii. Encapsulating Security Payload (ESP) as per RFC 1827
g. Diffie-Hellman asymmetric key algorithm with key lengths between 1024 and 1536 bits as per RFC 2631

5) IP Routing:
    a. Static route definition
    b. Network Address Translation (NAT)
    c. Routing Information Protocol (RIP) or Open Shortest Path First (OSPF)

6) Logging and Auditing:
    a. Detailed event log for use in troubleshooting
    b. All IPSec connection attempts (success or failure) must be logged

6.2. Category – Remote Access Node/Branch-to-Branch Terminator

Technical Definition:

Network device for deployment of IPSec VPNs over public packet switched networks, *with remote client support*. The device may include hardware and software modules with specialized functionality that must be integrated within the device.

Technical specifications for RFSO qualification only:

Propose one IPSec VPN model supporting the following requirements, features and protocols:

1) Typical Architecture:
   a. Requirement deleted
   b. All interfaces to support at least 100Base-TX full duplex
   c. Support for remote client connections – at least 200 concurrent per model Required VPN client to be included with VPN hardware
   d. Multiple concurrent gateway-to-gateway connections
   e. Requirement deleted
   f. Maximum IPSec throughput at least 100Mbps per appliance

2) Standards:
   a. 10Base-T as per IEEE 802.3 - 2002
   b. 100Base-TX as per IEEE 802.3 - 2002
   c. Gigabit Ethernet 1000Base - SX or LX or 1000Base-TX as per IEEE 802.3 -2002
   d. Link negotiation as per IEEE 802.3 - 2002
   e. Network Time Protocol (NTP) v2 or above
   f. VLAN tagging as per IEEE 802.1Q -2003
   g. VRRP RFC 3768 or an equivalent standby router/ redundancy protocol

3) Protocol Support/Services:
   a. Requirement deleted
   b. Simple Network Management Protocol
   c. Dynamic Host Configuration Protocol (DHCP) Server for local clients
   d. Dynamic Host Configuration Protocol (DHCP) Relay for local clients
   e. Dynamic Host Configuration Protocol (DHCP) Client for external interface
   f. Point-to-Point Protocol over Ethernet (PPPoE) client (Optional)
   g. A port must be provided for management and diagnostics
   h. Telnet server or Secure Shell (SSH) for device management
   i. Certificate Management Protocol (CMP) and/or Simple Certificate Enrollment Protocol (SCEP) and/or Certificate Management using CMS (CMC) for Entrust Certificate Management
   j. Certificate Revocation List (CRL) Retrieval

k. Authentication servers supported:
   i. Internal database
   ii. Lightweight Directory Access Protocol (LDAP)
   iii. Remote Authentication Dial-In User Service (RADIUS)

l. DNS Proxy for local clients (Optional)

m. Requirement deleted

n. Firewall:
   i. Inspection of all packets
   ii. Default firewall security policy is to deny all connections unless explicitly configured to be open
   iii. Support for firewall user authentication

4) Virtual Private Networking:

a. Federal Information Processing Standard (FIPS) 140-2 Certification; or "in-progress" FIPS 140-2 certification, provided that the offer is accompanied by appropriate documentation proving "in progress", to be compliant to the requirement and that the submission was made prior to May 1, 2009. The OEM must have completed FIPS140-2 certification and receive approval from the PWGSC Contracting Authority prior to making these products available through the NMSO.

b. Aggressive and main mode support

c. Encryption cyphers :
   i. 256-bit Advanced Encryption Standard (AES)
   ii. 128-bit Advanced Encryption Standard (AES)
   iii. 112-bit or 168-bit Triple Data Encryption Standard (3DES)

d. Hashing algorithms:
   i. Secure Hash Algorithm (SHA-1) as per RFC 3174
   ii. Message Digest (MD5) as per RFC 1321

e. Internet Key Exchange (IKE) algorithm

f. Authentication for key management:
   i. Pre-shared secrets
   ii. 1024-bit and 2048-bit X.509 certificates

g. IP Security (IPSec):
   i. Authentication Header (AH) as per RFC 1826 (Optional)
   ii. Encapsulating Security Payload (ESP) as per RFC 1827

h. Diffie-Hellman asymmetric key algorithm with key lengths between 1024 and 1536 bits as per RFC 2631

i. Network Address Translation (NAT) Traversal

j. SSL VPN Support – min 200 concurrent sessions (Optional)

5) Quality of Service:

a. Differentiated Services (Diff Serv)

b. Bandwidth throttling

c. Weighted Fair Queuing (WFQ) or Low Latency Queueing (LLC)

6) IP routing:
    a. Static route definition
    b. VRRP RFC 3768 or an equivalent standby router/ redundancy protocol
    c. Network Address Translation (NAT)
    d. Routing Information Protocol (RIP)
    e. OSPFv2 as per RFC 2328

7) Logging and Auditing:
    a. Detailed event log for use in troubleshooting
    b. All IPSec connection attempts (success or failure) must be logged
    c. Logging of all configuration changes must be logged
    d. External logging support (SYSLOG or other third party logging format)

6.3. Category – SSL VPN Appliance

Technical Definition:

Network device for deployment of SSL VPNs over public packet switched networks.

Technical specifications for RFSO qualification only:

Propose one SSL VPN model supporting the following requirements, features and protocols:

1) Architecture:
   a. Requirement deleted
   b. Requirement deleted
   c. Support for at least 1000 concurrent SSL sessions (1000 concurrent users)
   d. May be deployed as a single unit or multiple units in an active/active configuration for high availability and load balancing.

2) Interfaces:
   a. Min of one external 10/100Base-TX and one internal 10/100Base-TX
   b. Serial interface for console access (Optional)

3) Standards:
   a. 10Base-T as per IEEE 802.3 - 2002
   b. 100Base-TX as per IEEE 802.3 -2002
   c. Link negotiation as per IEEE 802.3 - 2002
   d. Network Time Protocol (NTP) v2 or above as per RFC 1119, RFC1305.

4) Security Features:
   a. Federal Information Processing Standard (FIPS) 140-2 Certification (Optional)
   b. Authentication Options:
      i. Simple username / password from local database
      ii. Simple username / password from a RADIUS server
      iii. Active directory
      iv. One-time password via RADIUS
      v. Digital certificates (x.509)
      vi. Simple username / password from a Windows Domain (Optional)
   c. Zero footprint upon session termination (no residual cache)
   d. Configurable session timeouts for inactivity
   e. URL aliasing (Optional)
   f. Ciphers:
      i. 3DES
      ii. Optional: AES
   g. Hashing algorithms:
      i. Secure Hash Algorithm (SHA-1)

ii. Message Digest (MD5)

h. Endpoint policy compliance checking (Optional):

i. Personal firewall and anti-virus detection

ii. Anti-virus signature file checking

iii. Windows Registry setting checking

iv. File or directory checks

5) Access Control Mechanisms:

a. Restrict / control access by user group

b. Restrict / control access by destination IP

c. Restrict / control access by destination port

d. Restrict / control access by time-of-day; day of week; limits on date (Optional)

e. Restrict / control access by authentication method (Optional)

f. Restrict / control access by client platform (i.e., Java-enabled; cookie-enabled) (Optional)

6) Management:

a. Ability to use web browser to manage the system

b. Console cable management (Optional)

c. Ability for multiple users to manage simultaneously

d. Delegated management - allowing users to manage configuration subsets

e. Partitioned management - allowing users to manage only certain functions

f. Real-time reporting

g. Historical reporting

h. Active session management (ability to log users off)

i. Simple Network Management Protocol (SNMP) Support

j. A port must be provided for management and diagnostics

7) Supported Applications:

a. Web applications:

i. HTML

ii. Java applets

iii. JavaScript

iv. ActiveX

v. HTTP

vi. HTTPS

vii. DHTML

b. E-Mail:

i. Microsoft Outlook

ii. Microsoft Outlook Web Access

iii. Lotus Notes

iv. Lotus iNotes Web Access

v. SMTP/ POP3

vi. IMAP

c. MS Terminal Server

    d. Citrix nFuse/Citrix Access Gateway

8) Auditing, Logging, and Accounting:
    a. Auditing
        i. All successful or unsuccessful login attempts are to be logged
        ii. All changes made to system configuration need to be logged
    b. Accounting
        i. External RADIUS accounting support
    c. Logging
        i. Audit and log information need to be stored locally
        ii. Local log stores buffers need to be retrievable via TFTP or FTP (Optional)
        iii. SYSLOG support
        iv. User Activity is to be logged

9) High-Availability (non-FIPS mode) (Optional):
    a. Modes:
        i. Active/Passive
        ii. Active/Active

6.4. Category – SSL Proxy

Technical Definition:

Network device for intercepting, decrypting and content checking network data traffic or redirecting it to a content checking appliance.

Technical specifications for RFSO qualification only:

SSL Proxy appliance is used between an end user browser on a private network and any SSL web server located on the Internet. The requirement is not for a proxy between a web server and the Internet. The proxy is required to decrypt SSL sessions from employees browsing to SSL protected sites. The SSL proxy appliance must be capable of intercepting, decrypting and content checking traffic or redirecting it to a content checking appliance. Once the content checker has scanned the traffic, it must then be re-encrypted and sent to the intended Internet based https (SSL) server. The SSL protected site could be any https site located on the Internet.

Propose one SSL Proxy model supporting the following requirements, features and protocols:

1. Access Speeds & Interfaces:
   a. 10/100/1000 Base-TX, speed and duplex auto-sensing on each port and the capability to statically set speed and duplex on all ports.

2. Standards:
   a. 10Base-T as per IEEE 802.3 - 2002
   b. 100Base-TX as per IEEE 802.3 - 2002
   c. Gigabit Ethernet 1000Base-T as per IEEE 802.3 - 2002
   d. Auto-negotiation of speed and duplex mode for all data rates - IEEE 802.3 - 2002
   e. Full duplex mode as per IEEE 802.3 - 2002

3. Architecture:
   a. SSL proxy must be configured to act as a certificate authority for internal web browsers
   b. SSL proxy must be able to verify HTTPS certificate and deny access to the site if the certificate has any problems, such as it is expired or the URL does not match the certificate, based on a configurable security policy.
   c. When an employee browses to any SSL protected site located on the Internet than she or he must see a pop up message stating that the SSL session will be decrypted and monitored (0ptional)
   d. SSL proxy must be compatible with proxy chaining. (Optional)
   e. Decryption and encryption of all inbound and outbound SSL traffic
   f. Must be compatible with at least three third party content checking applications (Optional)

   g. HTML error pages must be customizable (example: certificate invalid; site not found) (Optional).

4. Performance:
   a. At a minimum, must have the ability for one single unit to proxy 900 https (SSL) simultaneous connections from employees web browsers to Internet https web sites
   b. Scalability to proxy HTTPS (SSL) sessions for a network composed of up to 60,000 internal users

5. Management Features:
   a. Encrypted remote management and configuration capabilities (i.e. HTTPS, SSH)
   b. Multi-device management application that can control all SSL proxies and L4-7 switch (Optional)
   c. Console port management or local keyboard/ Mouse/ monitor management (Optional)
   d. A port must be provided for management and diagnostics

6. Security Features:
   a. Remote management can only be done on an isolated physical port
   b. IP based Access Control lists in order to control which hosts can connect to the device in order to perform remote management (Optional).
   c. All remote management traffic must be encrypted
   d. LED indicators that show the SSL proxies' power status
   e. LED indicators that show the status of each of the SSL proxies' ports

7. Certifications:
   a. Cryptographic modules must be FIPS 140-2 certified. (Optional)

7. Class - Optical Networking Devices

Main Functionality: Network device that enables the transmission of optical network data traffic.

7.1. Category – WDM Optical Network Device

Technical Definition:

Wavelength-division multiplexing (WDM) optical switch. The device may include hardware and software modules with specialized functionality that must be integrated within the device.

Technical specifications for RFSO qualification only:

Propose one WDM optical switch model supporting the following requirements, features and protocols:

1. Architecture:
   a. Must be 19" Rack mountable.
   b. Redundant Power Supply must be proposed
   c. Support for 32 wavelengths with growth to 64 wavelengths
   d. Support from 2.5Gbps to 10Gbps per wavelength
   e. Support for optical or protocol protection
   f. Support for aggregation of min 4 FC200 ports per 10Gbps wavelength
   g. Support for aggregation of min 8 FC100 ports per 10Gbps wavelength
   h. Support for aggregation of min 8 FICON ports per 10Gbps wavelength
   i. Support for aggregation of min 8 GE ports per 10Gbps wavelength
   j. Support for 10GE over a single wavelength
   k. Ability to mix FC, FICON and GE over the same wavelength
   l. Support for reconfigurable Optical Add/Drop Mulitplexer (ROADM)

2. Access Speeds & Interfaces:
   a. 1000 Base-SX
   b. 1000 Base-LX
   c. 10Gbase-LX4 or 10Gbase-LR or 10GBase-LRM
   d. 1-Gbps Fibre Channel
   e. 2-Gbps Fibre Channel
   f. 4-Gbps Fibre Channel
   g. FICON
   h. ESCON
   i. SONET OC-3
   j. SONET OC-12
   k. SONET OC-48

3. Standards:
    a. Gigabit Ethernet 1000Base-SX or LX as per IEEE 802.3 – 2002
    b. Ten Gigabit Ethernet 10GBase-LX4 or LR or 10Gbase - LRM or LR as per IEEE 802.3ae
    c. Support for ITU G.709 digital wrapper
    d. SONET/ ANSI system compliant

4. Network Management Interface:
    a. SNMP
    b. CLI (Command Line Interface) or TL1 (Transaction Language 1)
    c. A port must be provided for management and diagnostics
    d. Network management through a web browser

5. Security Features:
    a. Support user authentication via Radius or TACACS+
    b. Support password encryption

7.2. Category – SONET Optical Device

Technical Definition:

Synchronous optical networking (SONET) device. The device may include hardware and software modules with specialized functionality that must be integrated within the device.

Technical specifications for RFSO qualification only:

Propose one SONET optical device model supporting the following requirements, features and protocols:

1. Architecture:
    a. Must be 19” rack mountable.
    b. Redundant Power Supply must be proposed
    c. Support for optical transport bit rates up to OC-192 as per the SONET standard.
    d. Support for SONET protection protocols (unidirectional path switched ring, 2- fiber bidirectional line switched ring, 1 + 1 automatic protection switching)
    e. Support for SONET topologies (Ring, Linear and Mesh topologies)
    f. Requirement deleted
    g. Support for FC100 ports with flexible bandwidth assignment
    h. Support for FICON ports with flexible bandwidth assignment
    i. Support for aggregation of min 8 GE ports
    j. Requirement deleted
    k. Requirement deleted
    l. Support for Virtual Concatenation (VCAT)
    m. Support for Link Capacity Adjustment Scheme (LCAS)
    n. Support for General Framing Procedure (GFP)
    o. Support for SONET protection protocol: 4-fiber bidirectional line switched ring (Optional)

2. Access Speeds & Interfaces:
    a. 100 Base - FX
    b. 1000 Base - SX
    c. 1000 Base – LX
    d. DS1, DS3
    e. OC-3, OC-12, OC-48 and OC-192
    f. 1-Gbps Fibre Channel
    g. FICON

3. Standards:
    a. Gigabit Ethernet 1000Base-T or SX or LX as per IEEE 802.3 - 2002
    b. SONET/ ANSI system
    c. Ethernet prioritization and CoS as per IEEE 802.1Q - 2003, IEEE 802.1p

   d. VLAN Tagging as per IEEE 802.1Q - 2003

4. Network Management Interface:
   a. SNMP
   b. CLI (Command Line Interface) or TL-1 (GR-189-CORE and GR-833-CORE)
   c. A port must be provided for management and diagnostics
   d. Network Management through HTTPS access

5. Security Features
   a. Support user authentication via Radius or TACACS+
   b. Support password encryption

8. Class – Multi Class Equipment

<u>Main Functionality:</u> Network device that performs multiple class functions within a single unit.

8.1. Category – Unified Threat Management (UTM) Appliances

<u>Technical Definition:</u>

Unified Threat Management (UTM) appliance integrates a range of security features into a single device. The device must provide the following features; firewall, IPSec VPN, IPS, Content filtering, Antispam and Antivirus. The device may include hardware and software modules with specialized functionality that must be integrated within the device.

<u>Technical specifications for RFSO qualification only:</u>

Propose one UTM device supporting the following requirements, features and protocols:

1) Security Features:
    a. Firewall
    b. IPSec VPN
    c. Intrusion protection (IPS
    d. Antispam
    e. Antivirus
    f. Content filtering
    g. DHCP relay and DHCP server (Optional)
    h. RIP v.2 dynamic routing protocol
    i. OSPF as per RFC 2328 (Optional)
    j. Policy-based traffic shaping, guaranteed bandwidth and priority
    k. A port must be provided for management and diagnostics
    l. SNMP
    m. Authentication via local database, RADIUS/LDAP
    n. Command line interface (CLI) and GUI interface for configuration and reporting
    o. E-mail notifications of threats
    p. Customizable reporting

2) Port Density:
    a. Min of 4 full-featured ports 10/100M Ethernet
    b. Min of 2 full-featured ports Gigabit Ethernet (copper or fiber or both)

3) Performance:
    a. Min 200Mbps throughput with 3-DES or AES
    b. Min 500 VPN tunnels
    c. Min 100Mbps throughput with Firewall inspection

d. Min 1000 Firewall policies

4) Features (Optional):
   a. GRE tunnelling - RFC2784
   b. Multicast routing
   c. IGMP RFC 1112, RFC 2236, RFC 3376
   d. Routing between 802.1Q VLANs
   e. VRRP RFC 3768 or an equivalent standby router / redundancy protocol
   f. NTP - RFC 1305

8.2. Category – Traffic Management Appliances

Technical Definition:

Traffic Management devices, designed to complement routers and network management tools, typically deployed behind a router at a remote branch location or central office. Provides management features, such as class-based queuing, compression, traffic rate shaping, TCP optimization, performance measurement and protocol reporting.

Technical specifications for RFSO qualification only:

Propose one Traffic Management device supporting the following requirements, features and protocols:

1) Performance Features:
   a. Automatic bypass mode
   b. Hardware compression applied automatically or to user defined flows (Optional)
   c. QoS features to enable the prioritization of selected applications
   d. QoS features to guarantee bandwidth to selected applications
   e. TCP acceleration techniques such as window size optimization, fast start-ups, local acknowledgements, etc. (Optional)
   f. Must collect volumetric on aggregate protocol usage and per user protocol usage. The volumetric must contain at least:
      i. Application
      ii. Port number, IP address
      iii. URL
      iv. TOS, Policy class
      v. Throughput, Byte count, packet count
      vi. Selectable time periods
   g. Web-based configuration and reporting interface from appliance and via management station.
   h. Customizable reporting

2) Minimum capacity and performance parameters:
   a. Two Ethernet 10/100-TX ports
   b. 2Mbps throughput with all features enabled
   c. Minimum of 10 compression tunnels (Optional)

3) Management Features:
   a. CLI support (command line interface)
   b. SNMP
   c. Telnet (RFC 854)
   d. Secure web interface using SSL v3.1 and/or TLS v1.0
   e. SSH Version 2
   f. A port must be provided for management and diagnostics

4) Security Features:
    a. Standard security with access control lists
    b. Support user authentication via Radius or TACACS+
    c. Password encryption for login validation for admin privileges
    d. Cryptographic modules must be FIPS 140-2 certified (Optional)

9. Class – Wireless Systems

Main Functionality: Network device to deploy Enterprise grade Wireless Local Area Network (WLAN) equipment.

9.1. Category – Enterprise Wireless Components

Technical Definition:

Wireless network components working together to form a fully functional WLAN system.

Technical specifications for RFSO qualification only:

Propose wireless components supporting the following requirements, features and protocols:

Note: Category 9.1 consists of the following components: Wireless Access Points (including associated antenna complement), Stand Alone Wireless Controllers, and any other specialized Wireless Appliances (e.g. Wireless intrusion detection, location, and correlation), working together to form a fully functional, scalable, and secure WLAN system.

Wireless Access Point (AP) Requirements

1) Architecture:
    a. Flexible installation options (mounting hardware must be include):
        i. Wall
        ii. Ceiling
        iii. Above ceiling
    b. Rated for installation in plenum areas
    c. Single and dual antenna system (propose all antenna models available)
    d. Power over Ethernet (PoE) support IEEE 802.3af
    e. Outdoor AP (Optional)

2) Standards:
    a. Operating Frequency Spectrum (ISM 2.4 GHz and/or UNII 5 GHz unlicensed spectrums);
    b. Virtual LAN capabilities IEEE 802.1Q VLAN tagging (e.g. corporate VLAN, guest VLAN)
    c. Single (access only) or multifunction (access, RF monitoring, WIDS/WIPS) Access Points

3) Performance
    a. Min Rx sensitivity (measured at the antenna port) as in the following table:

	Rx Sensitivity	
Data rate [Mbps]	2.4 Ghz band	5.5 Ghz band
1	-92dBm	n/a
6	-86dBm	-85dBm
12	-84dBm	-84dBm
24	-79dBm	-78dBm
54	-70dBm	-69dBm

    b. Max Tx power (measured at the antenna port):
        i. Minimum: 100mW for 802.11b
        ii. Minimum: 50mW for 802.11a and 802.11g
    c. Min number of terminal stations supported: 50

4) Management:
    a. CLI – Console port or Telnet
    b. Secure web interface using SSL v3.0 and/or TLS v1.0
    c. SNMP v1, v2c, v3

Stand Alone Wireless Controller Requirements

1) Performance:
    a. Number of WLAN Access Points supported without performance degradation: min 8
    b. Min number of client mobile stations supported: min 256

2) WLAN Features:
    a. Management and configuration for APs within the controller domain
    b. WLAN controller domain must be extended over multiple subnets
    c. Dynamic Radio Channel Assignment
    d. Dynamic downstream power control – APs TX power dynamically adapts to radio channel conditions
    e. Radio Interference - management avoidance
    f. WLAN traffic / load balancing – dynamically balances radio traffic between APs
    g. QoS support:
        i. MAC based
        ii. 802.1 Q/p based
    h. Seamless roaming between APs, without breaking the active session:
        i. Within same IP subnet
        ii. Across different IP subnets
        iii. Across different controller domains

3) Standards:
    a. 10Base - T as per IEEE 802.3 - 2002
    b. 100Base - TX as per IEEE 802.3 - 2002
    c. Gigabit Ethernet (1000Base-T or 1000Base - SX or 1000Base-LX) as per IEEE 802.3 - 2002
    d. Ethernet prioritization and CoS as per IEEE 802.1Q - 2003, IEEE 802.1p
    e. VLAN tagging as per IEEE 802.1Q - 2003

4) Security Features:
    a. IEEE 802.11i full compliance, including CCMP mode using AES with 128 bit minimum key size
    b. Supports AAA management (IEEE 802.1x, Radius RFC 1238, LDAP, Windows active directory, Novell directory)
    c. WLAN IDS/ IPS, including:
        i. Rogue AP detection
        ii. Rogue AP shut-down
        iii. Wireless threat detection and location

5) Management:
    a. A port must be provided for management and diagnostics
    b. SNMP:
        i. SNMPv1 as per RFCs 1157, 1155, 1212, 1215
        ii. SNMPv2c as per RFCs 1901, 2578–2580, 3416-3418
        iii. SNMPv3 as per RFCs 3410 – 3415, 3584
        iv. SNMP MIB as per RFC 3418
    c. Encrypted remote management and configuration capabilities:
        i. Secure web interface using SSL v3.0 and/or TLS v1.0
        ii. SSH Version 2
    d. Telnet as per RFC854
    e. RMON I as per RFC 2819
    f. WLAN network management and planning system must be proposed

10. Class – Intrusion Prevention System

Main Functionality: Network device to detect and prevent anomalous or unauthorized activity on a network.

10.1. Category – In-line NIPS (Network Intrusion Prevention Systems)

Technical Definition:

Network device for detecting and blocking anomalous and/or unauthorized network activity.

Technical specifications for RFSO qualification only:

Propose one Intrusion Prevention device supporting the following requirements, features and protocols:

1) Architecture:
   a. Stand alone in-line device
   b. Monitoring of traffic must be in real time.
   c. Should packet filter via port, IP address, or network (Optional)
   d. Should rate limit as a percentage of traffic, or an absolute number (Optional)
   e. Local console port should be included for remote and local sensor configuration and maintenance (Optional)
   f. Critical system components such as fans and power supplies should be redundant and hot swappable. (Optional)
   g. Capacity to add a redundant unit which must assume processing if the primary unit becomes unavailable (Active-passive high availability)
   h. The IPS must support fail-open and fail-closed actions on a per-segment basis within the unit.

2) Physical specifications:
   a. 19" Rack mountable unit

3) Port Density:
   a. Monitoring interfaces: min 3 Fast Ethernet ports and 1 GE port
   b. Requirement deleted

4) Performance:
   a. Peak throughput supported: min 500Mbps
   b. Max concurrent sessions: no less than 300,000
   c. Requirement deleted
   d. Packet capture must support 10/100/1000 bit speeds with no loss (multiple interface support).

e. Must be able to handle variations in traffic, both natural and induced, without failure or loss of coverage.
f. Requirement deleted

5) Standards:
a. 10Base-T as per IEEE 802.3 - 2002
b. 100Base-TX as per IEEE 802.3 - 2002
c. Gigabit Ethernet 1000Base – T or SX or LX as per IEEE 802.3 - 2002
d. Auto-negotiation of speed and duplex mode for all data rates as per IEEE 802.3 - 2002 (Optional)
e. Manual setting option for speed and duplex mode for all data rates as per IEEE 802.3 - 2002
f. NTP v2 (or above) or Simple Network Time Protocol (SNTP) RFC 2030
g. VLAN Tagging as per 802.1Q - 2003
h. SNMP
i. Secure Shell SSH

6) General Requirements:
a. Analysis of packet information must occur at the sensor
b. Processing of IP packets regardless of the Transport Layer overlying the IP packet
c. NIPS must be able to fully reassemble the original traffic flow.
d. A time out mechanism must alert the management station if the sensor goes down.
e. NIPS must be VLAN aware (802.1Q). This means both being aware of VLAN groupings as well as being able to handle VLAN tagging.
f. NIPS should have a built-in Defrag Processor (Optional)
g. NIPS should be Multi-Protocol Label Switching (MPLS) Aware (Optional)
h. NIPS must only be network addressable on a management interface

7) Data Forensics, Logging and Auditing:
a. All changes to system configuration must be recorded in logs
b. Loss/establishment of NTP time synchronization must be recorded in the logs
c. The Operating System should allow audit-trail management, with recognition of user activity reflecting policy (Optional)
d. All traffic alerts must be recorded in logs
e. All unauthorized attempts to access the admin interface must be recorded
f. IDS should allow logging linear/ASCII format (Optional)
g. IDS must support the ability to export or log remotely in standard data formats such as syslog, SNMP, IDMEF, or SDEE
h. Must support the ability to set filters
i. IDS must support some mechanism by which the entire packet or packets (payload and headers), which triggered an alarm, are captured.
j. Data logs must be exportable to third party products.

8) Security Features:
   a. NIPS sensors must examine packets in detail in order to detect patterns of misuse.
   b. Content based scanning must examine packets and traffic streams for specific patterns or signatures (Match against a database of known "attack signatures") and / or behaviours, including:
      i. Exploit-based signatures
      ii. Vulnerability-based signatures
      iii. Automated signature update – include process overview and frequency
      iv. Cryptographic controls supporting signature integrity using RSA (Optional)
   c. Protocol anomaly (traffic scrubbing): decodes packets and checks protocol fields for deviations from RFCs and from industry defined application protocols
   d. Performs packet filtering to ensure packets are part of established flows
   e. Rate-based - detects unusual traffic which has not previously been observed (Optional):
      i. Perform statistical analysis for abnormal activity patterns
      ii. Statistical Analysis must extend beyond IP Header and including TCP/UDP and ICMP
   f. Must permit user/client to create and deploy its own customized signatures.
   g. The sensor should be able to monitor the protocols that are used to maintain the network infrastructure. This should include such protocols as OSPF and SNMP (Optional)

   h. NIPS must be able to provide detection for a number of common application protocols. These must include DNS, RPC, HTTP, SMTP and FTP
   i. NIPS must incorporate a hardened operating system
   j. When suspicious activities are noticed, the network-based IPS must be capable of both raising alerts and terminating the offending network traffic immediately by blocking the flows or hosts.
   k. NIPS response must be configurable on a per attack or policy basis
   l. Countermeasure capability:
      i. Discarding all suspect packets in real time and blocking the remainder of the flow. The response must be configurable on a per attack or policy basis
      ii. Should be able to reroute particular session when events occur (I.e. to a 'Honey Pot') (Optional)
      iii. Should be able to throttle back excessive bandwidth on attacks based on ICMP Source Quench Packets; (Optional)
      iv. Should be able to backtrack hack attempts to source reconnaissance including detecting if IP source is legitimate or spoofed (Optional)

m. NIPS must be able to detect attacks even if the attackers are using evasion techniques such as IP fragmentation, TCP fragmentation, TCP stream, unicode obfuscation

9) Security Certifications and Standards (Optional):
   a. The signature description should include links to CVE (Common Vulnerabilities
   b. The system message structure should be compliant with current IDS data exchange format standards (IDMEF and/or SDEE)

10) Management Features:
   a. Graphical User Interface
   b. Command Line Interface (Optional)
   c. Administrator and log viewing accounts having varying access and administrative privileges where access is restricted based on username/UserID and password (Optional)
   d. Administrator and log viewing accounts having varying access and administrative privileges where access is restricted based on source IP address and/or network (Optional)
   e. The management software should be able to run on commonly used operating system platforms including Windows, Linux or Solaris (Optional)
   f. Requirement deleted
   g. Encrypted remote management and configuration capabilities:
      i. Secure web interface using SSL v3.1 and/or TLS v1.0
      ii. SSH Version 2
   h. A port must be provided for management and diagnostics

11) Central management system (Optional):
   a. Security policy management, configuration and real-time log viewing capabilities from multiple remote management workstations
   b. Encrypted remote management and configuration capabilities
      i. Secure web interface using SSL v3.1 and/or TLS v1.0
      ii. SSH Version 2
   c. Ability to prioritize attacks in order to show the most dangerous attacks that are currently happening.
   d. Notify when packets are dropped.
   e. Should notify the overall percentage of collected traffic the dropped packets represent.
   f. Support the ability to notify an administrator via e-mail, pager, and/or SNMP trap.
   g. Support an acknowledgement function at the console via a pop up window or other similar mechanism if a specific event occurred.
   h. The management package should support global properties to update sensors or components at once. The management package should allow remote sensor upgrade

i. The management package functionality should include: establishing security policies, creating groups and assigning sensors to different groups
j. Support the ability to group attack signatures into groups or policies for applying to sensors
k. Reporting features: generation of hourly, weekly, daily and ad hoc reports

11. Class - Uninterruptible Power Supply (UPS)

Main Functionality: Network device for providing continuous electric power to data network equipment.

11.1. Category – Enterprise Uninterruptible Power Supply

Technical Definition:

Devices that maintain continuous supply of electric power to equipment by supplying power from a separate source when utility power is not available. This includes specialized accessories, which facilitate the deployment of UPS devices (i.e.power conditioners, surge-suppression, rack mounted power distribution). Motor-generator sets are not included in this category.

Technical specifications for RFSO qualification only:

Propose one Uninterruptible Power Supply device supporting the following requirements, features and protocols:

1) Architecture:
   a. Requirement deleted
   b. Requirement deleted
   c. Modular chassis/rack mountable solutions
   d. Hard-wire 3-wire (2PH+G) 208V input and 6000W/7500VA output
   e. 2 NEMA L6-20R outlets and 2 NEMA L6-30R outlets
   f. Should support internal redundancy by adding Optional power module (Optional)

2) Performance and capacity must meet or exceed:
   a. Battery backup time: no less than 7 minutes at full load (6000W)

3) Standards:
   a. 10Base-T, 100Base-TX as per IEEE 802.3 - 2002
   b. Internet Protocol (IP) as per RFC 791
   c. Auto-negotiation of speed and duplex mode for 10/100 data rates as per IEEE 802.3
   d. Flash-upgradeable firmware
   e. Frequency and voltage regulation
   f. User-replaceable batteries
   g. Boost and Trim Automatic Voltage Regulation (AVR)
   h. Power conditioning

4) Management Features:
   a. CLI support (command line interface)
   b. Web browser support

- c. Access through SSH V2
- d. Integral SNMP (Simple Network Management Protocol) agent as per RFC’s 1155-1157 without using external proxy agents
- e. Logfile for history
- f. TELNET as per RFC 854
- g. NTP (Network Time Protocol) as per RFC1305
- h. Audible alarms
- i. Automatic self-test
- j. A port must be provided for management and diagnostics
- k. The chassis must provide a visual indication of the status of the device:
    - i. For on-line power and on-battery power
    - ii. For battery bypass and/or internal fault
    - iii. Overload
    - iv. Replace battery
    - v. Meter or multi-LED load indicator
    - vi. Meter or multi-LED battery charge indicator
    - vii. Ethernet status

5) Security Features:
- a. SSH Version 2
- b. SCP Secure Copy (Optional)
- c. SSL v3.0 and/or TLS v1.0
- d. Provide local user identification for support management (Optional)

12. Common Requirements – All Classes

12.1. Interoperability and Performance Testing for RFSO Qualification

At the discretion of Canada, any offered equipment may be tested to demonstrate that it will meet or exceed Canada's mandatory technical specifications.

The Offeror must deliver the equipment proposed to either a location designated by Canada, or to an industry-recognized independent, mutually agreed to, third party testing firm location, no later than 15 calendar days following a written request by Canada. The Offeror must be available to answer questions and provide further information as requested concerning its equipment. All of the associated costs related to this testing will be the responsibility of the Offeror.

A formal methodology and test plan will be provided by Canada in advance of any testing. The testing will focus on the technical specifications identified in this Annex.

At Canada's discretion the required testing can be waived provided the Offeror submits a relevant performance test report from a recognized independent 3rd party-testing firm acceptable to Canada. The report must be based on testing done on the identical equipment, hardware and firmware versions being offered and includes testing against all mandatory technical specifications of the Category.

The following Technical specifications are only applicable for RFSO qualification:

12.2. Certifications and Regulatory Compliance

The following certification and compliance requirements are mandatory for all equipment in all Categories, unless otherwise indicated in the technical specifications in the specific Category:

1) Safety – CSA – 22.2 No. 60950 or cUL 60950
2) EMI – ICES – 003 Class A
3) Telecom – CS-03 (applicable only to equipment including any of the following PSTN interfaces: Dial-up, ISDN, xDSL, DS1)

12.3. Environmental Requirements

The following are the minimum environmental operating and non-operating conditions applicable to all Categories, except where specific requirements are listed within the section for the respective Category:

1) Operating Conditions:
   a. Temperature: 5° - 40°C
   b. Relative Humidity (non-condensing): up to at least 85%
   c. Altitude: 0 – 1500m

2) Non-operating Conditions:
   a. Temperature: -20° to +60°C
   b. Relative Humidity (non-condensing): up to at least 95%

13. Acronyms

ACL	Access Control List
ADSL	Asymmetric Digital Subscriber Line
AES	Advanced Encryption Standard
ATM	Asynchronous Transfer Mode
BGP	Border Gateway Protocol
CLI	Command Line Interface
CoS	Class of Service
CSS	Cascading Style Sheets
DES	Data Encryptions Standard
DHCP	Dynamic Host Configuration Protocol
DHTML	Dynamic HTML
DLSw	Data Link Switching
DNS	Domain Name System
DSCP	Distributed Services Code point
DVRMP	Distance Vector Multicasting Routing Protocol
FTP	File Transfer Protocol
GBIC	Gigabit Interface Converter
GUI	Graphical User Interface
HIDS	Host Intrusion Detection System
HTML	Hypertext Mark-up Language
HTTP	Hypertext Transfer Protocol
HTTPS	Secure Sockets Layer (SSL)
ICMP	Internet Control Message Protocol
IDS	Intrusion Detection System
IETF	Internet Engineering Task Force
IGMP	Internet Group Management Protocol
IKE	Internet Key Exchange
IMAP	Internet Message Access Protocol
IPS	Intrusion Prevention System
IPX	Internetwork Packet Exchange
ISDN	Integrated Services Digital Network
L2	OSI Layer 2
LDAP	Lightweight Directory Access Protocol
LLC	Logical Link Control
MAC	Media Access Control
MPLS	Multi Protocol Label Switching
MSTP	Multiple Spanning Tree Protocol
NAT	Network Address Translation
NIPS	Network based Intrusion Prevention System
NTP	Network Time Protocol
NVRAM	Non Virtual Random Access Memory
OSPF	Open Shortest Path First (protocol)
PAT	Port Address Translation
PBR	Policy Based Routing

PIM	Protocol Independent Multicasting
QoS	Quality of Service
RIP	Routing Information Protocol
RMON	Remote Monitoring
RPC	Remote Procedure Call
RSTP	Rapid Spanning Tree Protocol
RSVP	Resource Reservation Setup Protocol
SDLC	Synchronous Data Link Control
SFP	Small Form Pluggable
SIP	Session Initiation Protocol
SNMP	Simple Network Management Protocol
SQL	Structured Query Language
SSH	Secure Shell
SSL	Secure Sockets Layer
STP	Spanning Tree Protocol
TACACS	Terminal Access Controller Access Control System,
TCP	Transmission Control Protocol
TFTP	Trivial File Transfer Protocol
UDP	User Datagram Protocol
VLAN	Virtual Local Area Network
VPN	Virtual Private Network
VRRP	Virtual Router Redundancy Protocol
XML	Extensible Markup Language