Shared Services Canada

DNS/DHCP/IPAM (DDI) Solution

Request for Information

Table of Contents

National Security Exception

***National Security Exception**: The procurement related to this initiative is subject to National Security Exception and is, therefore, excluded from all of the obligations of the trade agreements.*

Purpose and Contents of this Request for Information

This is a Request for Information pertaining to DNS/DHCP/IPAM (DDI) Solution

of Shared Services Canada. It is a document written for the purpose of eliciting feedback from industry in regards to the DNS/DHCP/IPAM (DDI) Solution. The general contents of this Request for Information document are:

- **PART I - Request For Information Process**: Information about the intent of this Request for Information and the procedure for industry to follow for responding to this Request for Information;
- **PART II – Background of the DNS/DHCP/IPAM (DDI) Solution**
- **PART III – Anticipated Mandatory Requirements**: Requirements that Canada expects potential bidders to comply with.

PART I: REQUEST FOR INFORMATION PROCESS

1. INTRODUCTION

This is a Request for Information (RFI) pertaining to the DNS/DHCP/IPAM (DDI) Solution (DDI), which is an initiative of Shared Services Canada (SSC) to deliver a DNS/DHCP/IPAM (DDI) Solution (DDI)for SSC and the departments and agencies that it provides information technology (IT) services for, herein, referred to as SSC's "Partners". SSC will also offer the new service to other Government of Canada (GC) organizations on an optional basis.

SSC is seeking feedback from industry on the following subject matter:

(i) The ability to meet the anticipated mandatory requirements provided in Part III of this RFI;

The GC intends to use feedback from (i) to solidify its procurement approach and help determine the "way forward" for how the new DNS/DHCP/IPAM (DDI) Solution should be acquired.

1.1 Nature of this Request for Information

This is not a bid solicitation. This RFI will not result in the award of any contract. Potential suppliers of any goods or services described in this RFI should not reserve stock or facilities, nor allocate resources, as a result of any information contained in this RFI. Nor will this RFI result in the creation of any source list. Therefore, whether or not any potential DNS/DHCP/IPAM (DDI) Solution provider responds to this RFI, it will not preclude that provider from participating in any future procurement. Also, the procurement of any of the goods and services described in this RFI will not necessarily follow this RFI. This RFI is simply intended to solicit feedback from industry with respect to the subject matter described in this RFI.

2. INSTRUCTIONS FOR RESPONDING TO THIS REQUEST FOR INFORMATION.

2.1 Response Costs

Canada will not reimburse any organization for expenses incurred in responding to this RFI.

2.2 Treatment of Responses

Use of Responses: Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify the procurement approach, as well as any draft documentation contained in this RFI. Canada will review all responses received by the RFI closing date. Canada may, in its discretion, review responses received after the RFI closing date.

Review Team: A review team composed of representatives of SSC and its Partners (where applicable) and will review the responses. Canada reserves the right to hire any independent consultant, or use any GC resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

Confidentiality: Respondents should mark any portions of their response that they consider proprietary or confidential. Canada will handle the responses in accordance with the Access to Information Act.

2.3 Follow-up Activity

Canada may, in its discretion, contact any Respondents to follow-up with additional questions or for clarification of any aspect of a response either in writing or via RFI One-on-One meetings,

2.4 Contents of Document

This document remains a work in progress and Respondents should not assume that new clauses or requirements will not be added to any bid solicitation that is ultimately published by Canada. Nor should Respondents assume that none of the clauses or requirements will be deleted or revised. Comments regarding any aspect of the draft document are welcome.

2.5 Format of Responses

Cover Page: If the response includes multiple volumes, Respondents are requested to indicate on the front cover page of each volume the title of the response, the solicitation number, the volume number and the full legal name of the Respondent.

Title Page: The first page of each volume of the response, after the cover page, should be the title page, which should contain:

(i) The title of the Respondent's response and the volume number;

(ii) The name and address of the Respondent;

(iii) The name, address and telephone number of the Respondent's contact;

(iv) The date, and

(v) The RFI number.

Number of Copies: Canada requests that Respondents submit their response in unprotected PDF (e.g. no password) format by email to francois.richer@ssc-spc.gc.ca if the size of the document is less than 6MB. Alternatively, Canada requests that Respondents save a copy of their PDF (2003 or later) document onto each of 2 compact discs (CD-R) or 2 digital video discs (DVD-R) and send the discs by mail to the address specified in section 2.8. PDF format is being requested to allow Respondents to include any material (e.g. spreadsheet, white paper, brochure, etc.) with their written documentation in one file.

2.6 Enquiries

Since this is not a bid solicitation, Canada will not necessarily respond to enquiries in writing or by circulating answers to all Respondents. However, Respondents with questions regarding this RFI may direct their enquiries to:

Contracting Authority: Tom Mercer

Shared Services Canada

Procurement and Vendor Relations

180 Kent, 13 Floor, Room K074

Ottawa, ON

Email Address: tom,mercer@ssc-sps.gc.ca

Telephone: 613-8947493

2.7 Submission of Responses

Time and Place for Submission of Responses: Organizations interested in providing a response should deliver it to the Contracting Authority identified above by 2:00 p.m. January 30, 2014

Responsibility for Timely Delivery: Each Respondent is solely responsible for ensuring its response is delivered on time, to the correct location.

Identification of Response: Each Respondent should ensure that its name, return address, the solicitation number and the closing date appear legibly on the outside of the response.

PART II: BACKGROUND OF THE DNS/DHCP/IPAM (DDI) Solution

3. ORGANIZATIONAL OVERVIEW

3.1 Overview of Shared Services Canada

Shared Services Canada is mandated to operate and transform the government's IT infrastructure. Under the umbrella of that dual authority, we are responsible for providing our 43 Partner organizations with modern, reliable and secure IT infrastructure services that are cost-effective and which contribute to a greener government. In the process, we are building a new organization from the ground up.

From an operational perspective, SSC is establishing IT service delivery across the Government of Canada(GC). SSCis supporting a significant number of projects in cooperation with its Partners that will both modernize and streamline today's IT operations. The Operations Branch will support Projects & Client Relationship (PCR) Branch in contributing to the GC's Economic Action Plan efforts, enabling SSC to plan and build capacity to take on the larger, more ample transformative initiatives (under the leadership of Transformation, Service Strategy and Design (TSSD)).

SSC has identified the following four priorities for: (If we're going to have a 10 year contract, it would be of no added value to quote FY12-13.)

- Maintain and improve the delivery of IT infrastructure services to the Government of Canada through an enterprise approach.
- Launch the renewal of the Government of Canada's IT infrastructure: identify an email solution and develop initial plans to consolidate data centres, networks and telecommunications in a whole-of-government approach.
- Establish governance mechanisms and implement partnerships to clarify accountability and adopt enterprise approaches for the management of IT infrastructure services.
- Implement efficient and effective business management processes and services in support of the SSC mandate

In support of the top three priorities, SSC must renew several core foundational elements, which are key building blocks required for the transformation of the GC's IT infrastructure. Domain Name Services (DNS), Dynamic Host Configuration Protocol (DCHP), and IP Address Management (IPAM) infrastructure, collectively known as DDI, are three of the core foundation elements that must be renewed.

Several of SSC's partners have previously implemented third-party DDI and DNS solutions; however the contracts are split amongst various vendors without the possibility of easy consolidation. As SSC transitions to a single network and consolidated light out data centres, a national DDI infrastructure is paramount. In the future, DDI infrastructure will be a key in the delivery of online service for Canadians.

SSC needs the replacement technology to decrease time spent managing the DNS/DHCP infrastructure, decrease operational costs, decrease reoccurring maintenance costs, increase control, increase security and overall improve the service and stability of the DNS and DHCP infrastructure. SSC has determined that an appliance based DDI solution that centrally manages IP Address Management (IPAM), DNS and DHCP services is the optimal way to accomplish these goals. The solution must also address the following: automated upgrades, centralized management, support and full management of IPv4, IPv6, DNS, DHCP, DNSSEC and IPAM. The solution must also integrate with existing infrastructure which includes BIND servers, Microsoft DDNS servers, and VMware / Hyper-V hypervisors to maximize the cost savings and operational gains.

3.2 Current State

4. The GC infrastructure currently supports 377,000 end-users in 19,000 facilities. The current number of IP addressable devices is estimated to be over 900,000. Addressable devices include network infrastructure (routers, switches), servers, end-user devices (desktops, laptops, tablets, smartphones), VoIP phones, videoconferencing equipment, cameras, radios, and other IP enabled devices. For the most part, existing DNS and DHCP infrastructure is managed by SSC Portfolio Operations on a per Partner basis. In the future, Partner networks will be collapsed into a single enterprise GC network that will operate with an enterprise DDI solution managed by SSC Horizontal Operations. It is anticipated that number of managed IP addressable devices will grow to over 1,500,000 over the life of the contract.

PART III: ANTICIPATED MANDATORY REQUIREMENTS

Although SSC feels that these requirements will suffice the long-term requirements for an enterprise grade DDI solution, SSC is looking for input on any glaring errors, inconsistencies, and omissions in the mandatory requirements detailed below. Furthermore, should a respondent wish to bid on any forthcoming RFP but has determined that one or more of these requirements would deem the respondent non-compliant, SSC may be willing to drop one or more of the mandatory requirements. Hence, respondents are asked to explicitly identify mandatory requirements that they cannot meet using current generally available (GA) releases.

Req. #	***Requirement***
	Common Requirements
M 1.	All appliance(s) [i.e. DNS, DHCP and IPAM] must be a dedicated appliance-based platform (physical and virtual [VMWare and Hyper-V] certified appliances)
M 2.	Physical appliance(s) must be rack mountable within a standard 19 inch rack
M 3.	All appliance(s) must support two or more network interfaces that separate from any dedicated out-of-band interfaces
M 4.	All network interfaces of the DNS appliance(s) must provide support for link speeds of 10/100/1000 Mbps
M 5.	Primary appliance(s) must provide integrated support for high availability configurations without the requirement for licensing of additional third party software components
M 6.	All supporting database technology for all appliances must be integrated and provided at no additional cost or licensing requirement
M 7.	All appliances must support forwarding/redirection of logs to a defined syslog device as-well-as full console access and download capabilities
M 8.	Appliances must support monitoring using SNMP v2 and SNMP v3
M 9.	Technical documentation (in both hard and soft copy) for the appliances must be given to the Crown for administrative/support purposes. Soft copy documentation must be in searchable PDF, Word, and/or HTML formats
M 10.	All appliances must fully support IPv4 and IPv6
M 11.	All appliances must support NTP time synchronization (client-mode)
M 12.	All appliances must be licensed per appliance with no restrictions on the number of IPs and DNS names being managed
M 13.	All appliances must provide support for a centralized automated upgrade mechanism (preferably through the IPAM web interface)
M 14.	The solution must be able to support multiple appliance versions, negating the need to upgrade all appliances simultaneously
M 15.	The solution must expose full functionality of all solution components (i.e. appliances) through a CLI or equivalent scripting interface (i.e. allow for manipulation of appliance configurations, allow for import/export of data, etc.)
M 16.	All appliances must have power supplies that support 110v and 220v
M 17.	The operating system of all proposed appliances must be hardened and secured
M 18.	Appliances must integrate with multiple pass-through authentication options including LDAP, AD, RADIUS, and TACACS+
M 19.	System must be 100% compliant with DHCP Options and BOOTP Vendor Extensions (RFC 2132), DNS Update (RFC 2136), DNS SRV (RFC 2782), The

	Dynamic Host Configuration Protocol (DHCP) Client Fully Qualified Domain Name (FQDN) Option (RFC 4702), and support integration with Microsoft Active Directory
M 20.	Appliances offering DNS services must also be able to offer DHCP services
M 21.	Communication between the various appliances must be encrypted using a secure method of communication
M 22.	All communication between the administration interface and the appliance(s) must be encrypted – again what is the classification required here? (i.e. use of IPSEC tunnels, TLS, SCP-over-SSH, etc.)
M 23.	Encryption must support the use of industry standard Certificate Authorities (CAs) for the management web interface
	Common Maintenance/Support Requirements
M 24.	All appliances must be bundled with live support and maintenance services, and support must be available 24/7/365 via Internet, web support (i.e. unlimited access to Technical Support knowledgebase), email, telephone, and on-site support if necessary.
M 25.	Technical Support must be available with a response time of four (4) hours. This includes web support, email and telephone support.
M 26.	The bidder's website support must be available 24/7. All emails for maintenance support should be acknowledged within four (4) hours
M 27.	The bidder must provide software and maintenance updates in a timely manner and must be included as part of the warranty and maintenance services. The bidder must inform the customer of any new software and maintenance update including product software release within 30 days after such release. If applicable, the customer may request the applicable release in electronic format. The deliverable shall be provided by e-mail and electronic media (CD, DVD or memory stick) within 30 days after the request or available via a downloadable link from the Internet
M 28.	The Contractor shall provide two (2) business days Return-To-Depot (RTD), hardware maintenance on all equipment listed in "Annex B". The hardware must be returned with the same hardware configuration(s) and software requirements as described in detail in "Annex B"
M 29.	The two (2) day RTD period begins at 08:00 EST/EDT on the day following the assignment of a Tracking Number by the Contractor or the next business day if a Tracking Number has not been assigned by the end of the business day the problem is reported
M 30.	The Contractor shall have repaired or replaced all defective equipment within two (2) business days of the assignment of a Tracking Number or shall have delivered a replacement device identical to the failed equipment and meeting the specifications of this contract. The two (2) day RTD period ends at 16:00 EST/EDT on the second (2nd) business day following the beginning of the RTD period
M 31.	The Contractor must provide a web site capable of taking and recording all information concerning failed equipment and must issue a tracking number
M 32.	A Maintenance Report must be prepared by the Contractor's service representative for all repaired or replaced defective equipment. The report must include the following information: • The assigned tracking number • Date and Time call was received • Hardware serial number

	• Name of person who placed the service call and name of person who took the Information on the part of the Contractor. • Description of symptom(s) • Diagnosis of fault • Description of equipment including the hardware and software configuration. • List of all parts or modules replaced or installed (including DRAM and Flash and any pre-packaged assemblies) • The Identification number and/or serial number of each assembly removed or exchanged, including cards, modules, etc. • Hardware and Software configuration of the received hardware. • Hardware and Software configuration of the returned or replacement hardware The Contractor shall include one printed copy of this report with the returned equipment and shall forward one copy electronically to the Client Technical Authority
M 33.	Equipment returned from the Contractor shall be in the same physical configuration as when submitted for repair/replacement. Any parts, sub-assemblies, or modules, shall be of the same make and model as those in the defective equipment. In cases where sub-assemblies or modules have been replaced, the new and old serial numbers, if applicable, will be reported on the Maintenance Report. In cases where parts, sub-assemblies, or modules require replacement, this will be done before the equipment is returned. Equipment returned to the Client unassembled will be returned to the Contractor for assembly as a new RTD (Return to Depot) call. If the expectation is that equipment must always be returned to the Client/us fully assembled then we must state here that the equipment will be returned at the contractor's expense and that if there are any delays caused to the Client, that the Contractor will be fully responsible to supply a new piece of equipment of equal technical spec to do the work required until such time that the original piece of equip. Is returned and accepted by the client. In cases where an equipment or component part is/are no longer available, substitute of improved components shall be used.
M 34.	As a security pre-caution, the contractor must return all replaced non-volatile storage components (including hard drives, NVRAM, SSD, and others) to the client, so they may be destroyed as per the GC Security Policy. Why not ask the contractor to do this destruction for us and send us a certificate of destruction upon destruction completed – this would possibly generate cost savings to the Crown by “NOT shipping items back at our cost/destruction of equipment/parts on the Crown's tab/ and not to speak of the cost associated with the material handling etc. . Again, what level of security are we talking about here?
M 35.	A secure (to what level – it must indicated here) web site must be provided for the Client, to allow on-line tracking of the repair status of equipment sent for servicing.
M 36.	Shipping to and from the Depot must be at the Contractor's expense – delete this M.36 and insert in AofA's/T&C's – are we talking new equip. Or repairable equip going to and from to be fixed? verify SACC 4001/4002/4003.
M 37.	Returned Equipment shall have documentation included with the following information listed:

	• A printed copy of the Maintenance Report. • Device Make, Model, Serial Number, and description of the equipment received, including any installed cards or modules, and the device make, model, and serial number, including details of any cards or modules installed, of equipment returned to the Client. This also includes any DRAM/Flash for items mentioned in “ANNEX B” • Description of repairs made or serial numbers of old and new units if equipment is replaced. The Contractor is responsible for keeping their database up-to-date in regards to equipment replaced. (See also section on quarterly updates) • Hard copy printout of the current hardware and software configuration (specify for the product). • Proof that the equipment has been powered up and found to be operating and properly configured.
M 38.	When an updated “Annex B” is supplied to the Contractor, and has been approved, a Purchase Order will be issued by the Client. Once the Purchase Order has been issued, and acknowledged as received by the Contractor, the Contractor must apply the “Annex B” changes to all appropriate web sites within 10 business days. An electronic message (email) must be sent to the Technical Authority to confirm these changes have been completed by the Contractor. Failure to do so will result in the contractor applying a credit to the Client account equal to five percent (5%), of the cost of the outstanding product to be delivered. This same amount will be credited to the Client Account for each subsequent 10-day period that the updates are not applied
M 39.	The bidder must provide the ability to procure maintenance for additional years on the equipment after initial warranty expires. Written notice to the crown must be given within 1 year (365 days) as to when maintenance will no longer be available for the said item.
M 40.	The solution proposed by the bidder must be sustainable/supportable for a minimum period of five years
M 41.	At the end of the fifth year of the contract, the vendor must provide options and pricing for a technology refresh
M 42.	The bidder must allow the client to purchase Technical consulting services at a an hourly rate (pro-rated from daily rate) bid as part of the contract
	Training Requirements
M 43.	Requisite training must be given to operational personnel regarding the installation/setup and configuration of all solution components (DNS, DCHP, and IPAM) prior to production cutover
M 44.	Must be able to provide onsite training to large groups of technicians (i.e. groups of 15-30 employees)
M 45.	SSC’s expectations of training focus on the acquisition of the skills necessary to explain the operations of, manage, set parameters for and make use of the implemented environment. The contractor shall plan training adapted to the environment, based on the operating characteristics of SSC’s environment. This training must include practical exercises to facilitate learning.

	In order to enable SSC employees to complete the training program, the contractor shall implement the necessary technology at SSC's facilities. The price of installing the equipment required for this training should be included in the contractor's firm lot price for training.
M 46.	In preparing and delivering training activities, the contractor must: • Provide a description of the skills that SSC resources must master in order to set parameters for and make appropriate use of the implemented solutions; • Submit training programs in the form of a curriculum (listing skills to be mastered) and a course outline (brief description of the training), customized for each employee group (i.e. administrators, users) that will require training; • Provide an original copy of the training material for each of the sessions. This material should include the trainer's guide and a copy of the material used by students (for example, student manual, documents, presentations, etc.); • Hold training sessions at the SSC's facilities for the specific employee groups identified. • Documentation for employees (administrators, users), including the user guide and training manual, must be supplied in both French and English. This documentation must be available in one of more of the following document formats: PDF, Word, HTML
M 47.	The cost of training must be bid as part of the contract on a per session basis
M 48.	The contractor must provide an architecture and engineering resource to assist with the following: • Assist SSC in the performance of an environmental scan (i.e. existing IP addressing and DNS infrastructures) of the SSC and legacy forty-three partner networks; • Provide advice and guidance with regards to the integration or replacement of pre-existing DDI solutions; • Assist SSC to produce a technical architecture for a sustainable enterprise DDI implementation; • Assist SSC to determine the best implementation method for their equipment. • If required, provide a migration plan for any pre-existing DDI implementations to the new DDI solution; • If required, assist SSC in dealing with the implementation of overlapping private address plans within the IPAM solution; • If necessary, assist with the DDI migration (live production cutover); • Assist SSC in the documentation of detailed design specifications for DDI components including IPAM, DNS and DHCP appliances.
M 49.	The cost of architecture and engineering resources must be bid as part of the contract on an hourly basis

DNS Specific Requirements

This subsection details requirements specific to only the DNS component of the solution.

Req. #	Requirement
	DNS Specific Requirements
M 50.	The DNS system must support integration into IPAM
M 51.	DNS Software must interoperate ISC BIND compliant (with current GA release), supporting all relevant RFCs
M 52.	If contractor deploys a proprietary Bind implementation, the contractor must issue patches for known BIND vulnerabilities within 48 hrs of a vulnerability being exposed
M 53.	The solution must support DNSSEC
M 54.	DNSSEC functionality must be managed through the same user web interface session as DNS/DHCP
M 55.	It must be possible to manage Microsoft DNS servers through the IPAM user interface
M 56.	The solution must support zone transfers to ISC/BIND and Microsoft DNS servers
M 57.	Any changes to Microsoft DNS must be reflected in the IPAM system
M 58.	The DNS system must support remote management and administration through a cross platform management interface supporting secure (encrypted) connectivity
M 59.	Authenticated zone transfers must use TSIG
M 60.	The DNS system must provide an integrated and configurable firewall, without the requirement for additional licensing
M 61.	DNS processes running on the primary DNS system must be “jailed”
M 62.	Must support full DNS query logging capability for external recursive and authoritative servers
M 63.	Must support live DNS traffic monitoring capability
M 64.	Must provide the capability to configure black hole zones to use external data feeds
M 65.	DNS servers must support EDNS0 (Extended DNS) (RFC 2671)
M 66.	Each DNS appliance must be capable of supporting 20,000 queries per second
M 67.	The DNS system must support HA failover
M 68.	DNS system must support authoritative query rate limiting
M 69.	The solution must provide the ability to configure DNS appliances as recursive caching servers, with no authoritative/non-authoritative zones defined
M 70.	The DNS solution must support E.164 Number Mapping (ENUM) protocol as developed by the IETF that uses DNS system architecture to translate telephone numbers into IP addressing schemes (like SIP, H323 or Email). ENUM may contain a reference to a SIP URI, a telephone number to dial as well as a web page and an e-mail address
M 71.	The DNS solution must allow Name Authority Pointers (NAPTR) and Service (SRV) records for ENUM that includes URI schemes and domain name as specified by Canada.

M 72.	The DNS solution for ENUM must allow NAPTR record types for resolution to URI schemes that included but not limited:
	a) SIP;
	b) SIPS;
	c) H.323;
	d) Telephone

M 73.	The DNS solution for ENUM must allow delegating domain name and zones to

	DNS and ENUM services as specified by Canada
M 74.	The DNS solution for ENUM must allow assigning selected telephone numbers and ranges of telephone numbers to domain names as specified by Canada
M 75.	The DNS solution for ENUM records must allow redirecting TCP and UDP payload for: a) SIP and SIPS (secure SIP) requests to one or more port numbers and SIP servers; and b) H.323 requests to one or more port numbers and Gatekeepers
M 76.	The DNS solution for ENUM must allow SRV records that provide resolution that include redundancy or load balancing addresses as specified by Canada
M 77.	The DNS solution for ENUM must allow masking or aliasing NAPTR and/or SRV records as specified by Canada
M 78.	The DNS solution for ENUM must allow porting telephone numbers between GC domain names identified by Canada
M 79.	The DNS solution for ENUM must allow establishing an end-to-end connection using: a) abbreviated telephone numbers (e.g. 9181@gc.ucs.ca); b) E.164 telephones numbers (e.g. 21215559181@gc.ucs.ca); c) personally identifying information (e.g. john.doe@gc.ca); and d) aliases identifying information (e.g. agent123@gc.ca)
M 80.	The ENUM must comply to the following standards: a) [RFC 6116] The E.164 to Uniform Resource Identifiers (URI) Dynamic Delegation Discovery System (DDDS) Application (ENUM) b) [RFC 6117] IANA Registration of Enumservices: Guide, Template, and IANA Considerations c) [RFC 6118] Update of Legacy IANA Registrations of Enumservices d) [RFC 5527] Combined User and Infrastructure ENUM in the e164.arpa Tree e) [RFC 3482] Number Portability in the Global Switched Telephone Network (GSTN): f) [RFC 4114] E.164 Number Mapping for the Extensible Provisioning Protocol (EPP)
M 81.	The DNS solution for ENUM must provide the following and minimum capacity: a) 500,000 NAPTR records; b) 500,000 SRV records; and c) 1,000 domains or sub-domains
M 82.	The DNS solution for ENUM must allow queries from up to 250 different sources that are ENUM compliant.
M 83.	The DNS solution for ENUM must allow a minimum of 3,000 queries per second (qps) with a responses time that is less than 1 msec
M 84.	The DNS solution for ENUM Service Administration Activity must include the following: a) Adding, deleting or modifying a Domain Name entry; b) Adding, deleting or modifying any information associated with a NAPTR or SRV record; and c) Porting URI schemes to Domain name
M 85.	The DNS solution for ENUM Administration must allow: a) Adding, deleting or modifying a Domain Name entry; b) Adding, deleting or modifying any information associated with a NAPTR or SRV

	record; and c) Porting URI schemes to Domain name
M 86.	The DNS solution for ENUM must be accessible using a secure web browser.
M 87.	The DNS solution for ENUM must allow Canada to remotely view the ENUM Service configuration, including but not limited to NAPTR and SRV Records.
M 88.	The DNS solution for ENUM Service must allow producing URI schemes, telephone numbers and Domain name reports, including: a) searching and sorting for specific record type, for one or more fields in a record; and b) downloading search results in file naming convention specified by Canada and a COTS file format
M 89.	The DNS solution for ENUM must provide performance and traffic reports according to a time and date interval as specified by Canada

DHCP Specific Requirements

This subsection details requirements specific to only the DHCP component of the solution.

	DHCP Specific Requirements
M 90.	The DHCP appliance(s) must support integration with IPAM infrastructure
M 91.	The DHCP appliance(s) must provide an integrated and configurable firewall, without the requirement for additional licensing
M 92.	Each DHCP appliance must support at least 600 leases per second with ping before disabled
M 93.	Each DHCP appliance must be capable of supporting a minimum of 100,000 leases within each DHCP cluster
M 94.	The DHCP appliances must support HA failover

IPAM Specific Requirements

This subsection details requirements specific to only the IPAM component of the solution.

	IPAM Specific Requirements
M 95.	The solution must be able to centrally manage, configure, administer, control, and deploy the DNS and DHCP components within the enterprise (includes adding/removing/modifying zones, scopes, DNS records, etc.)
M 96.	IPAM user interface must be web-based
M 97.	When a user adds an address record that points to an IP address from a subnet that has not been defined in the IP space yet, the IPAM must issue a warning
M 98.	The solution must have the ability to support tree views for IP block/networks and domains. The tree must exist and update itself as soon as an IP block is defined. The tree must not necessitate extra steps to be updated other than creating blocks in the IP space
M 99.	The IPAM system must support HA failover
M 100.	The DNS system must provide support for user level authentication
M 101.	The DNS system must provide import/export to flat files

M 102.	The DNS system must provide the ability to backup and restore the DNS appliance configuration
M 103.	The DNS system must support delegated administration of particular zones or domains to defined administrators
M 104.	The DNS system must support granular rights administration limiting the function and rights to user and record level
M 105.	The DNS system must provide read-only support for defined domains and zones
M 106.	The DNS system must support automatic creation and update of reverse/PTR zones
M 107.	The solution must provide the ability to group, display, and search objects based on user-created custom fields
M 108.	The solution must have the ability to alert users when creating A Record with a Fully Qualified Domain Name (FQDN) that already exist in the same DNS zone with a different IP address i.e. avoid creating an FQDN that round robin without intending to
M 109.	Appliances must allow the use of loopback /30 for a single IP
M 110.	The solution must support RFC6177 (http://tool.ietf.org/html/rfc6177)
M 111.	The DHCP appliance(s) system must support VLSM
M 112.	The DHCP appliance(s) system must support CIDR
M 113.	The DHCP appliances (s) must support supernetting
M 114.	The DHCP appliance(s) must support multiple MAC pools
M 115.	The DHCP appliance(s) must provide support for MAC address exclusions
M 116.	The DHCP appliance(s) must support remote management and administration through a cross platform management interface supporting secure(encrypted) connectivity
M 117.	The DHCP appliance(s) must provide the ability to backup and restore the DHCP appliance configuration
M 118.	The DHCP appliance(s) must support delegated administration of scopes to defined administrators
M 119.	The DHCP appliance(s) must support granular rights administration limiting the function and rights to user and record level
M 120.	The DHCP appliance(s) must provide read-only support for defined scopes
M 121.	The IPAM appliance must provide the ability to backup and restore the appliance configuration
M 122.	The IPAM appliance must provide support for user level pass-through authentication that integrates with RADIUS, TACACS, Active Directory and LDAP
M 123.	The IPAM appliance must support granular role based user rights administration limiting the function and rights available to a user
M 124.	The IPAM appliance must provide read-only rights assignment
M 125.	The IPAM solution must be able to export reports in PDF format and raw data in flat file text format (i.e. plan text, CSV or delimited ASCII)
M 126.	The solution must have a change approval or workflow process
M 127.	The IPAM appliance must provide an integrated and configurable firewall, without the requirement for additional licensing.