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

RETURN BIDS TO:
RETOURNER LES SOUMISSIONS À:

Bid Receiving - PWGSC / Réception des soumissions - TPSGC
11 Laurier St., / 11, rue Laurier
Place du Portage, Phase III
Core 0B2 / Noyau 0B2
Gatineau
Québec
K1A 0S5
Bid Fax: (819) 997-9776

LETTER OF INTEREST
LETTRE D'INTÉRÊT

Title - Sujet
JUSTICE CANADA HELP DESK SERVICES

Solicitation No. - N° de l'invitation	Date
19335-160056/B	2017-01-30
Client Reference No. - N° de référence du client	**GETS Ref. No. - N° de réf. de SEAG**
19335-160056	PW-$$EL-626-31037
File No. - N° de dossier	**CCC No./N° CCC - FMS No./N° VME**
626el.19335-160056	

Solicitation Closes - L'invitation prend fin
at - à 02:00 PM
on - le 2017-03-10

Time Zone
Fuseau horaire
Eastern Daylight Saving Time EDT

F.O.B. - F.A.B.
Plant-Usine: ☐ **Destination:** ☐ **Other-Autre:** ☐

Address Enquiries to: - Adresser toutes questions à:	Buyer Id - Id de l'acheteur
Dubé, Jonah	626el
Telephone No. - N° de téléphone	**FAX No. - N° de FAX**
(873) 469-4980 ( )	( ) -

Destination - of Goods, Services, and Construction:
Destination - des biens, services et construction:

Specified Herein
Précisé dans les présentes

Comments - Commentaires

Instructions: See Herein

Instructions: Voir aux présentes

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

Delivery Required - Livraison exigée	Delivery Offered - Livraison proposée
See Herein	

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

Telephone No. - N°de téléphone
Facsimile No. - N° de télécopieur

Name and title of person authorized to sign on behalf of Vendor/Firm (type or print)
Nom et titre de la personne autorisée à signer au nom du fournisseur/ de l'entrepreneur (taper ou écrire en caractères d'imprimerie)

Signature **Date**

Issuing Office - Bureau de distribution
Informatics Professional Services - EL Division/Services professionnels en informatique - division EL
4C2, Place du Portage
Gatineau
Québec
K1A 0S5

Canada

REQUEST FOR INFORMATION REGARDING

THE ACQUISITION OF IT HELP DESK AND DESK-SIDE SUPPORT SERVICES

FOR

THE DEPARTMENT OF JUSTICE

TABLE OF CONTENTS

REQUEST FOR INFORMATION REGARDING

THE ACQUISITION OF IT HELP DESK AND DESK-SIDE SUPPORT SERVICES

FOR

THE DEPARTMENT OF JUSTICE (JUS)

1. Background and Purpose of this Request for Information (RFI)

The intent of this Request for Information (RFI) is to solicit feedback from industry on all aspects detailed in the draft Annex A – Request for Proposal.

Following feedback that will be received in response to this RFI, it is the Government of Canada's intention to publish a Request for Proposal (RFP) based on the draft copy mentioned above.

The main objectives of this RFI are as follows:

(a) Provide industry with an early opportunity to assess and comment on the JUS requirement in order to maximize best value to Canada should a RFP be posted;
(b) Determine the capability of suppliers to provide services described in this RFI;
(c) Solicit feedback and recommendations on any issues that would impact a supplier's ability to fulfill the JUS requirement; and
(d) Solicit industry knowledge and expertise with regards to best practices that would increase the likelihood of a successful outcome for this project.

Overview

JUS requires informatics professional services to operate a responsive service through a centralized national Help Centre, in addition to providing desk-side support services in the National Capital Region (NCR), as well as national desktop engineering services. The service will provide Level 1 Help Desk Services, Level 2 Desk-side Support and Break/Fix Support Services, Level 3 Engineering and Support Services, and professional services through a task authorization on an as and when requested basis for; Project Manager, Solution Architect, Security Architect, Business Analyst, On-site Services Team Leader and On-site Services Representative.

2. Nature of Request for Information

The material in the RFI package is for the solicitation of feedback only. Responding to this RFI is not a prerequisite to receiving any resulting RFP related to this JUS requirement. The industry is encouraged to indicate their level of interest by responding to the questions found at Section 7, in order to facilitate a better understanding of the requirements and capabilities from both JUS and industry perspectives.

This is not a bid solicitation. This RFI will not result in the award of any contract. As a result, 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 supplier responds to this RFI will not preclude that supplier 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 matters described in this RFI.

3. Nature and Format of Responses Requested

Respondents are requested to provide their comments, concerns and, where applicable, alternative recommendations regarding how the requirements or objectives described in this RFI could be satisfied. Respondents are also invited to provide comments regarding the content, format and/or organization of any draft documents included in this RFI. Respondents should explain any assumptions they make in their responses.

4. Response Costs

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

5. Treatment of Responses

(a) **Use of Responses**: Responses will not be formally evaluated. However, the responses received may be used by Canada to develop or modify procurement strategies or any draft documents 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.

(b) **Review Team**: A review team composed of representatives of the client (where applicable) and Public Services and Procurement Canada (PSPC) will review the responses. Canada reserves the right to hire any independent consultant, or use any Government resources that it considers necessary to review any response. Not all members of the review team will necessarily review all responses.

(c) **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*.

(d) **Follow-up Activity**: At its discretion, Canada may meet with respondents who indicate in their responses that they wish to participate in a follow-up meeting and provide written responses to the questions found at Section 7. Canada currently anticipates holding any such meetings during the week of April 03 to April 07, 2017. In order to allow PSPC to establish the schedule for such meetings, respondents are requested to include in their responses an indication of whether they wish to meet with Canada, together with a list of the individuals from their organization who would be attending the meeting, and their three preferred meeting times (see the grid below). PSPC cannot guarantee that any respondent will be allocated any of its preferred meeting times. The Contracting Authority will advise respondents in due course of the time slot that is available for their meeting.

	Date (during week of April 03 to April 07)	Time (between the hours of 09:00 and 15:00)
Preferred Time Slot #1		
Preferred Time Slot #2		
Preferred Time Slot #2		

6. Contents of this RFI

(a) This RFI contains a draft bid solicitation. 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.

(b) This RFI also contains specific questions addressed to the industry.

7. Questions to Industry

(a) Describe the current business environment for the provision of IT service desk and desk-side support services to both public and private sector organizations. What are the trends and challenges?

(b) Based on your experience as a service provider, how does the business culture of the client organization play into these trends or challenges?

(c) Are there particular factors that can have a significant impact on pricing of such services?

(d) Considering new business opportunities, what are the key factors that you look for, to determine if there is a good fit with the service you offer? What information do you require?

i. What does a compelling IT service desk and desk-side support service business opportunity look like?

(e) Describe the features of a modernized IT service desk and some of the recent enhancements in the user interface (e.g., web interface, on-line chat, virtual assistant, etc.).

i. From your experience in providing this service to client organizations, how do users typically receive such enhancements?
ii. Are there particular features that are more successful than others?
iii. Are there features that do not work as well, and why?
iv. Does telephone contact still play an important role?
v. Do you have specific recommendations regarding user interface?

(f) Are there recent changes in how VIP users are provided with service, and if so please describe them.

i. What works well and what is less successful?
ii. Do you have recommendations on how to best support VIP users?

(g) Do you have any general recommendations for Justice Canada regarding the planned tender for IT service desk and technical support services?

(h) If you chose not to respond to Justice Canada regarding the Help Desk and Support Services RFP (19335-160056/A) which was published on September 6, 2016, are there particular reasons and would you care to describe these?

(i) Are there specific comments or suggestions that you have regarding the security-related requirements of the draft RFP included herein?

i. Is there an effective approach for articulating security requirements that you would recommend?
ii. In providing similar services to current clients, how do you ensure the protection and security of client information and services?

(j) Would the review of the security requirements in the draft RFP included herein be made clearer by the addition of a High Level Design diagram, which depicts the requirements of the service desk service at a high level? What type of information would be useful with this approach?

(k) Are there particular security requirements in the draft RFP included herein that appear more stringent than you would expect for a government organization, and if so, would you provide examples and explain further?

(l) From your experience in providing IT service desk and desk-side support services to client organizations, do you have recommendations on service level targets that are effective and correlate well with user satisfaction?

i. What are the recent trends or relevant benchmarking data?
ii. What works well and what is less successful?

(m) Are there specific comments or suggestions that you have regarding the service level target requirements of the draft RFP included herein (which are found in Section 7 of SOW - Annex A)?

(n) From your experience in providing IT service desk and desk-side support services to client organizations, do you have recommendations or best practices for assessing operational readiness of the service provider, the associated phase-gates, deliverables and approvals, while reducing the complexity of this assessment?

(o) What is the range in time interval from the date of Contract Award until the Service Go Live date, based on your experience in providing IT service desk and desk-side support services to client organizations?

i. What is a reasonable duration (in days) for transition of these types of IT services?
ii. What are the factors that impact this, and are there best practices that facilitate the managing of this interval to a reasonable duration?
iii. Conversely, what are typical factors that result in this interval being elongated?

(p) Are there specific comments or suggestions that you have regarding the operational readiness and/or acceptance of the work requirements of the draft RFP included herein (which are found in Sections 2 and 3 of SOW - Annex A)?

(q) Do you have specific comments or suggestions on the evaluation criteria of the draft RFP included herein?

8. Volumetric Data

All data, including the Current State Information, is being provided to respondents purely for information purposes. Although it represents the best information currently available to PSPC, Canada does not guarantee that the data is complete or free from error.

9. Format of Responses

(a) **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.

(b) **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.

(c) **Numbering System**: Respondents are requested to prepare their response using a numbering system corresponding to the one in this RFI. All references to descriptive material, technical manuals and brochures included as part of the response should be referenced accordingly.

(d) **Number of Copies**: Canada requests that respondents submit three hard copies of their responses.

10. Enquiries

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

Contracting Authority:	Jonah Dubé
E-mail Address:	Jonah.dube@pwgsc.gc.ca
Telephone:	(873)-469-4980

11. Submission of Responses

(a) **Time and Place for Submission of Responses**: Suppliers interested in providing a response should deliver it to the following location by the time and date indicated on the cover page of this document:

ATTN: Jonah Dubé
Public Services and Procurement Canada Bid Receiving Unit
Portage III, 0A1
11 Laurier Street
Gatineau, Quebec K1A 0S5

Responses should not be sent directly to the Contracting Authority.

(b) **Responsibility for Timely Delivery**: Each respondent is solely responsible for ensuring its response is delivered on time to the correct location.

(c) **Bid Receiving Unit Address Solely for Delivery of Responses**: The above address is only for bid submission. No other communications are to be forwarded to this address.

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

Annex A
Draft Request for Proposal

Attached hereto.

BID SOLICITATION
FOR A CONTRACT AGAINST A SUPPLY ARRANGEMENT FOR SOLUTION- BASED INFORMATICS PROFESSIONAL SERVICES (SBIPS)

FOR
THE DEPARTMENT OF JUSTICE

Table of Contents

List of Annexes to the Resulting Contract:
Annex A: Statement of Work General
Annex B: Basis of Payment
Annex C: Security Requirements Check List

List of Attachments to Part 1 (General Information):
Attachment 1: Current State Information

List of Attachment to Part 3 (Bid Preparation Instructions):
Attachment 2: Bid Submission Form

List of Attachment to Part 4 (Evaluation Procedures and Basis of Selection):
Attachment 3: Mandatory Bid Evaluation Criteria
Attachment 4: Point-Rated Bid Evaluation Criteria
Attachment 5: Pricing Schedule
Attachment 6: Federal Contractors Program for Employment Equity - Certification

List of Appendices to Annex A:
Appendix A to Annex A – Service Domain: JUS Service Desk Service
Appendix B to Annex A – Service Domain: JUS On-Site Support Service
Appendix C to Annex A – Service Domain: JUS Engineering Service
Appendix D to Annex A – Security Requirements
Appendix E to Annex A – Definitions
Appendix F to Annex A – Standard Hardware and Software
Appendix G to Annex A – Tasking Procedures
Appendix H to Annex A – Task Authorization (TA) Form
Appendix I to Annex A – Resource Assessment Criteria and Response Tables
Appendix J to Annex A – Certifications at the TA stage

BID SOLICITATION
FOR A CONTRACT AGAINST A SUPPLY ARRANGEMENT FOR SOLUTION- BASED INFORMATICS PROFESSIONAL SERVICES (SBIPS)

FOR
THE DEPARTMENT OF JUSTICE

PART 1 - GENERAL INFORMATION

1.1 Introduction

This document states terms and conditions that apply to this bid solicitation. It is divided into seven parts plus attachments and annexes, as follows:

Part 1 General Information: provides a general description of the requirement;

Part 2 Bidder Instructions: provides the instructions, clauses and conditions applicable to the bid solicitation;

Part 3 Bid Preparation Instructions: provides Bidders with instructions on how to prepare their bid;

Part 4 Evaluation Procedures and Basis of Selection: indicates how the evaluation will be conducted, the evaluation criteria that must be addressed in the bid, if applicable, and the basis of selection;

Part 5 Certifications and Additional Information: includes the certifications and additional information to be provided;

Part 6 Security, Financial and Other Requirements: includes specific requirements that must be addressed by Bidders; and

Part 7 Resulting Contract Clauses: includes the clauses and conditions that will apply to any resulting contract.

The annexes include the Statement of Work and any other annexes and appendices.

1.2 Summary

(a) This bid solicitation is being issued to satisfy the requirement of the Department of Justice (the "**Client**") for Solution-Based Informatics Professional Services (SBIPS) under the SBIPS Supply Arrangement (SA) method of supply.

(b) It is intended to result in the award of one contract for four years plus two one-year irrevocable options allowing Canada to extend the term of the contract.

(c) There are security requirements associated with this requirement. For additional information, consult Part 6 - Security, Financial and Other Requirements, and Part 7 – Resulting Contract Clauses. For more information on personnel and organization security screening or security clauses, Bidders should refer to the, Industrial Security Program (ISP) of Public Works and Government Services Canada (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website.

(d) The requirement is subject to the provisions of the World Trade Organization Agreement on Government Procurement (WTO-AGP), the North American Free Trade Agreement (NAFTA), the Canada-Chile Free Trade Agreement (CCFTA), the Canada-Peru Free Trade Agreement

(CPFTA), the Canada-Colombia Free Trade Agreement (CColFTA), and the Canada-Panama Free Trade Agreement (CPanFTA), and the Agreement on Internal Trade (AIT).

(e) The Federal Contractor's Program (FCP) for employment equity applies to this procurement; see Part 5 – Certifications, Part 7 – Resulting Contract Clauses and the attachment titled "Federal Contractor's Program for Employment Equity – Certification".

(f) Only SBIPS SA Holders currently holding an SBIPS SA for Tier 2, in the Managed Services Domain of Expertise and in the National Capital Region, under the EN537-05IT01 series of SAs, are eligible to compete. The SBIPS SA EN537-05IT01 is incorporated by reference and forms part of this bid solicitation, as though expressly set out in it, subject to any express terms and conditions contained in this bid solicitation. The capitalized terms not defined in this bid solicitation have the meaning given to them in the SBIPS SA.

(g) SA Holders that are invited to compete as a joint venture must submit a bid as that joint venture SA Holder, forming no other joint venture to bid. Any joint venture must be already qualified under the SA # EN537-05IT01 as that joint venture at the time of bid closing in order to submit a bid.

1.3 Debriefings

After contract award, bidders may request a debriefing on the results of the bid solicitation process. Bidders should make the request to the Contracting Authority within 15 working days from receipt of the results of the bid solicitation process. The debriefing may be provided in writing, by telephone or in person.

1.4 Conflict of Interest

(a) Bidders are advised to refer to Conflict of Interest provisions at Article 18 of SACC 2003, Standard Instructions – Goods or Services – Competitive Requirements (dated 2016-04-04) available on the PWGSC Website https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual.

(b) Without limiting in any way the provisions above, Bidders are advised that Canada has engaged the assistance of the following private sector contractors who have provided services in preparing strategies and documentation related to this procurement process:

(i) Gartner Group Canada; and
(ii) BP&M Consulting.

PART 2 - BIDDER INSTRUCTIONS

2.1 Standard Instructions, Clauses and Conditions

(a) All instructions, clauses and conditions identified in the bid solicitation by number, date and title are set out in the *Standard Acquisition Clauses and Conditions Manual* (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

(b) Bidders who submit a bid agree to be bound by the instructions, clauses and conditions of the bid solicitation and accept the clauses and conditions of the resulting contract(s).

(c) The 2003 (2016-04-04) Standard Instructions - Goods or Services - Competitive Requirements are incorporated by reference into and form part of the bid solicitation. If there is a conflict between the provisions of 2003 and this document, this document prevails.

(d) Subsection 3.a) of Section 01, Integrity Provisions - Bid of Standard Instructions 2003 incorporated by reference above is deleted in its entirety and replaced with the following:

a. at the time of submitting an arrangement under the Request for Supply Arrangement (RFSA), the Bidder has already provided a list of names, as requested under the *Ineligibility and Suspension Policy*. During this procurement process, the Bidder must immediately inform Canada in writing of any changes affecting the list of names.

(e) Subsection 5(4) of 2003, Standard Instructions – Goods and Services – Competitive Requirements is amended as follows:

(i) Delete: 60 days

(ii) Insert: 180 days

2.2 Submission of Bids

(a) Bids must be submitted only to the Public Works and Government Services Canada (PWGSC) Bid Receiving Unit by the date, time and at the PWGSC address indicated on page one of the bid solicitation.

(b) Due to the nature of the bid solicitation, bids transmitted by facsimile or electronic mail to PWGSC will not be accepted.

2.3 Enquiries - Bid Solicitation

(a) All enquiries must be submitted in writing to the Contracting Authority no later than five calendar days before the bid closing date. Enquiries received after that time may not be answered.

(b) Bidders should reference as accurately as possible the numbered item of the bid solicitation to which the enquiry relates. Care should be taken by Bidders to explain each question in sufficient detail in order to enable Canada to provide an accurate answer. Technical enquiries that are of a proprietary nature must be clearly marked "proprietary" at each relevant item. Items identified as “proprietary” will be treated as such except where Canada determines that the enquiry is not of a proprietary nature. Canada may edit the questions or may request that the Bidder do so, so that the proprietary nature of the question is eliminated, and the enquiry can be answered with copies to all Bidders. Enquiries not submitted in a form that can be distributed to all Bidders may not be answered by Canada.

2.4 Former Public Servant

(a) Contracts awarded to former public servants (FPS) in receipt of a pension or of a lump sum payment must bear the closest public scrutiny, and reflect fairness in the spending of public

funds. In order to comply with Treasury Board policies and directives on contracts awarded to FPSs, Bidders must provide the information required below before contract award. If the answer to the questions and, as applicable the information required have not been received by the time the evaluation of bids is completed, Canada will inform the Bidder of a time frame within which to provide the information. Failure to comply with Canada's request and meet the requirement within the prescribed time frame will render the bid non-responsive.

(b) Definitions

For the purposes of this clause,"*former public servant*" is any former member of a department as defined in the *Financial Administration Act*, R.S., 1985, c. F-11, a former member of the Canadian Armed Forces or a former member of the Royal Canadian Mounted Police. A former public servant may be:

(i) an individual;

(ii) an individual who has incorporated;

(iii) a partnership made of former public servants; or

(iv) a sole proprietorship or entity where the affected individual has a controlling or major interest in the entity.

"*lump sum payment period*" means the period measured in weeks of salary, for which payment has been made to facilitate the transition to retirement or to other employment as a result of the implementation of various programs to reduce the size of the Public Service. The lump sum payment period does not include the period of severance pay, which is measured in a like manner.

"*pension*" means a pension or annual allowance paid under the *Public Service Superannuation Act* (PSSA), R.S., 1985, c. P-36, and any increases paid pursuant to the *Supplementary Retirement Benefits Act*, R.S., 1985, c. S-24 as it affects the PSSA. It does not include pensions payable pursuant to the *Canadian Forces Superannuation Act*, R.S., 1985, c. C-17, the *Defence Services Pension Continuation Act*, 1970, c. D-3, the *Royal Canadian Mounted Police Pension Continuation Act* , 1970, c. R-10, and the *Royal Canadian Mounted Police Superannuation Act*, R.S., 1985, c. R-11, the *Members of Parliament Retiring Allowances Act*, R.S. 1985, c. M-5, and that portion of pension payable to the *Canada Pension Plan Act*, R.S., 1985, c. C-8.

(c) Former Public Servant in Receipt of a Pension

As per the above definitions, is the Bidder a FPS in receipt of a pension? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information, for all FPSs in receipt of a pension, as applicable:

(i) name of former public servant;

(ii) date of termination of employment or retirement from the Public Service.

By providing this information, Bidders agree that the successful Bidder's status, with respect to being a former public servant in receipt of a pension, will be reported on departmental websites as part of the published proactive disclosure reports in accordance with Contracting Policy Notice: 2012-2 and the Guidelines on the Proactive Disclosure of Contracts.

(d) Work Force Adjustment Directive

Is the Bidder a FPS who received a lump sum payment pursuant to the terms of the Work Force Adjustment Directive? **Yes** ( ) **No** ( )

If so, the Bidder must provide the following information:

(i) name of former public servant;

(ii) conditions of the lump sum payment incentive;

(iii) date of termination of employment;

(iv) amount of lump sum payment;

(v) rate of pay on which lump sum payment is based;

(vi) period of lump sum payment including start date, end date and number of weeks;

(vii) number and amount (professional fees) of other contracts subject to the restrictions of a work force adjustment program.

For all contracts awarded during the lump sum payment period, the total amount of fees that may be paid to a FPS who received a lump sum payment is $5,000, including Applicable Taxes.

2.5 Applicable Laws

(a) Any resulting contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

Note to Bidders: *Bidders may, at their discretion, substitute the applicable laws of a Canadian province or territory of their choice without affecting the validity of its bid, by deleting the name of the Canadian province or territory specified and inserting the name of the Canadian province or territory of its choice. If no change is made, it acknowledges that the applicable laws specified are acceptable to the Bidder. Bidders are requested to indicate the Canadian province or territory they wish to apply to any resulting contract in their Bid Submission Form.*

2.6 Improvement of Requirement During Solicitation Period

Should bidders consider that the specifications or Statement of Work contained in the bid solicitation could be improved technically or technologically, bidders are invited to make suggestions, in writing, to the Contracting Authority named in the bid solicitation. Bidders must clearly outline the suggested improvement as well as the reasons for the suggestion. Suggestions that do not restrict the level of competition nor favour a particular bidder will be given consideration provided they are submitted to the Contracting Authority in accordance with the article entitled "Enquiries - Bid Solicitation". Canada will have the right to accept or reject any or all suggestions.

2.7 Volumetric Data

The Current State Information (Attachment 1) data has been provided to Bidders to assist them in preparing their bids. The inclusion of this data in this bid solicitation does not represent a commitment by Canada that Canada's future usage of the service identified in this bid solicitation will be consistent with this data. It is provided purely for information purposes.

PART 3 - BID PREPARATION INSTRUCTIONS

3.1 Bid Preparation Instructions

(a) **Copies of Bid**: Canada requests that Bidders provide their bid in separately bound sections as follows:

(i) Section I: Technical Bid (five hard copies and five soft copies on USB key)

(ii) Section II: Financial Bid (two hard copies)

(iii) Section III: Certifications not included in the Technical Bid (two hard copies)

(iv) Section IV: Additional Information (two hard copies)

If there is a discrepancy between the wording of the soft copy and the hard copy, the wording of the hard copy will have priority over the wording of the soft copy.

Prices must appear in the financial bid only. No prices must be indicated in any other section of the bid.

(b) **Format for Bid**: Canada requests that Bidders follow the format instructions described below in the preparation of their bid:

(i) use 8.5 x 11 inch (216 mm x 279 mm) paper;

(ii) use a numbering system that corresponds to the bid solicitation;

(iii) include a title page at the front of each volume of the bid that includes the title, date, bid solicitation number, bidder's name and address and contact information of its representative; and

(iv) include a table of contents.

(c) **Canada's Policy on Green Procurement**: In April 2006, Canada issued a policy directing federal departments and agencies to take the necessary steps to incorporate environmental considerations into the procurement process. See the Policy on Green Procurement (http://www.tpsgc-pwgsc.gc.ca/ecologisation-greening/achats-procurement/politique-policy-eng.html). To assist Canada in reaching its objectives, Bidders should:

(i) use paper containing fibre certified as originating from a sustainably-managed forest and/or containing a minimum of 30% recycled content; and

(ii) use an environmentally-preferable format including black and white printing instead of colour printing, printing double sided/duplex, and using staples or clips instead of cerlox, duotangs or binders.

(d) **Submission of Only One Bid**:

(i) A Bidder, including related entities, will be permitted to submit only one bid in response to this bid solicitation. If a Bidder or any related entities participate in more than one bid (participating means being part of the Bidder, not being a subcontractor), Canada will provide those Bidders with 2 working days to identify the single bid to be considered by Canada. Failure to meet this deadline will result in all the affected bids being disqualified.

(ii) For the purposes of this Article, regardless of the jurisdiction where any of the entities concerned is incorporated or otherwise formed as a matter of law (whether that entity is a natural person, corporation, partnership, etc), an entity will be considered to be "**related**" to a Bidder if:

(A) they are the same legal entity (i.e., the same natural person, corporation, partnership, limited liability partnership, etc.);

(B) they are "related persons" or "affiliated persons" according to the Canada Income Tax Act;

(C) the entities have now or in the two years before bid closing had a fiduciary relationship with one another (either as a result of an agency arrangement or any other form of fiduciary relationship); or

(D) the entities otherwise do not deal with one another at arm's length, or each of them does not deal at arm's length with the same third party.

(iii) Individual members of a joint venture cannot participate in another bid, either by submitting a bid alone or by participating in another joint venture.

(e) Joint Venture Experience:

(i) Where the Bidder is a joint venture with existing experience as that joint venture, it may submit the experience that it has obtained as that joint venture.

Example: A bidder is a joint venture consisting of members L and O. A bid solicitation requires that the bidder demonstrate experience providing maintenance and help desk services for a period of 24 months to a customer with at least 10,000 users. As a joint venture (consisting of members L and O), the bidder has previously done the work. This bidder can use this experience to meet the requirement. If member L obtained this experience while in a joint venture with a third party N, however, that experience cannot be used because the third party N is not part of the joint venture that is bidding.

(ii) A joint venture bidder may rely on the experience of one of its members to meet any given technical criterion of this bid solicitation.

Example: A bidder is a joint venture consisting of members X, Y and Z. If a solicitation requires: (a) that the bidder have 3 years of experience providing maintenance service, and (b) that the bidder have 2 years of experience integrating hardware with complex networks, then each of these two requirements can be met by a different member of the joint venture. However, for a single criterion, such as the requirement for 3 years of experience providing maintenance services, the bidder cannot indicate that each of members X, Y and Z has one year of experience, totaling 3 years. Such a response would be declared non-responsive.

(iii) Joint venture members cannot pool their abilities with other joint venture members to satisfy a single technical criterion of this bid solicitation. However, a joint venture member can pool its individual experience with the experience of the joint venture itself. Wherever substantiation of a criterion is required, the Bidder is requested to indicate which joint venture member satisfies the requirement. If the Bidder has not identified which joint venture member satisfies the requirement, the Contracting Authority will provide an opportunity to the Bidder to submit this information during the evaluation period. If the Bidder does not submit this information within the period set by the Contracting Authority, its bid will be declared non-responsive.

Example: A bidder is a joint venture consisting of members A and B. If a bid solicitation requires that the bidder demonstrate experience providing resources for a minimum number of 100 billable days, the bidder may demonstrate that experience by submitting either:

- Contracts all signed by A;
- Contracts all signed by B; or
- Contracts all signed by A and B in joint venture, or
- Contracts signed by A and contracts signed by A and B in joint venture, or
- Contracts signed by B and contracts signed by A and B in joint venture.

That show in total 100 billable days.

(iv) Any Bidder with questions regarding the way in which a joint venture bid will be evaluated should raise such questions through the Enquiries process as early as possible during the bid solicitation period.

3.2 Section I: Technical Bid

(a) The technical bid consists of the following:

(i) **Bid Submission Form**: Bidders are requested to include the Bid Submission Form - Attachment 2 with their bids. It provides a common form in which bidders can provide information required for evaluation and contract award, such as a contact name and the Bidder's Procurement Business Number, etc. Using the form to provide this information is not mandatory, but it is recommended. If Canada determines that the information required by the Bid Submission Form is incomplete or requires correction, Canada will provide the Bidder with an opportunity to do so.

(ii) **Security Clearance**: Bidders are requested to submit the following security information for each of the proposed resources with their bids on or before the bid closing date:

SECURITY INFORMATION	
Name of individual as it appears on security clearance application form	
Level of security clearance obtained	
Validity period of security clearance obtained	
Security Screening Certificate and Briefing Form file number	

If the Bidder has not included the security information in its bid, the Contracting Authority will provide an opportunity to the Bidder to submit the security information during the evaluation period. If the Bidder has not submitted the security information within the period set by the Contracting Authority, its bid will be declared non-responsive.

(iii) **Substantiation of Technical Compliance**: The technical bid must substantiate the compliance with the specific articles of Attachment 3 and Attachment 4, which is the requested format for providing the substantiation. The substantiation must not simply be a repetition of the requirement(s), but must explain and demonstrate how the Bidder will meet the requirements and carry out the required Work. Simply stating that the Bidder or its proposed solution or resources comply is not sufficient. Where Canada determines that the substantiation is not complete, the Bidder will be considered non-responsive and disqualified. The substantiation may refer to additional documentation submitted with the bid - this information can be referenced in the "Bidder's Response" column of Attachment 3 and Attachment 4, where Bidders are requested to indicate where in the bid the reference material can be found, including the title of the document, and the page and paragraph numbers; where the reference is not sufficiently precise, Canada may request that the Bidder direct Canada to the appropriate location in the documentation.

(iv) **For Proposed Resources**: The technical bid must include the number of résumés, per Resource Category, as identified in Attachment 3. The same individual must not be proposed for more than one Resource Category. The Technical bid must demonstrate that each proposed individual meets the qualification requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). With respect to the proposed resources:

(A) Proposed resources may be employees of the Bidder or employees of a subcontractor, or these individuals may be independent contractors to whom the Bidder would subcontract a portion of the Work (refer to Part 5, Certifications).

(B) For educational requirements for a particular degree, designation or certificate, PWGSC will only consider educational programs that were successfully completed by the resource by the time of bid closing. If the degree, designation or certification was issued by an educational institution outside of Canada, the Bidder must provide a copy of the results of the academic credential assessment and qualification recognition service issued by an agency or organization recognized by the Canadian Information Centre for International Credentials (CICIC).

(C) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of bid closing and must continue, where applicable, to be a member in good standing of the profession or membership throughout the evaluation period and Contract Period. Where the designation or membership must be demonstrated through a certification, diploma or degree, such document must be current, valid and issued by the entity specified in this solicitation. If the entity is not specified, the issuer must have been an accredited or otherwise recognized body, institution or entity at the time the document was issued. If the degree, diploma or certification was issued by an educational institution outside of Canada, the Bidder must provide a copy of the results of the academic credential assessment and qualification recognition service issued by an agency or organization recognized by the Canadian Information Centre for International Credentials (CICIC).

(D) For work experience, PWGSC will not consider experience gained as part of an educational program, except for experience gained through a formal co-operative program at a post-secondary institution.

(E) For any requirements that specify a particular time period (e.g., 2 years) of work experience, PWGSC will disregard any information about experience if the technical bid does not include the relevant dates (month and year) for the experience claimed (i.e., the start date and end date). Canada will evaluate only the duration that the resource actually worked on a project or projects (from his or her start date to end date), instead of the overall start and end date of a project or a combination of projects in which a resource has participated.

(F) For work experience to be considered by Canada, the technical bid must not simply indicate the title of the individual's position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. In situations in which a proposed resource worked at the same time on more than one project, the duration of any overlapping time period will be counted only once toward any requirements that relate to the individual's length of experience.

(v) **Customer Reference Contact Information**:

(A) The Bidder must provide customer references. The customer reference must each confirm, if requested by PWGSC, the facts identified in the Bidder's bid, as required by Attachment 3 and Attachment 4.

(B) The form of question to be used to request confirmation from customer references is as follows:

[Sample Question to Customer Reference: "Has [the Bidder] provided your organization with [describe the services and, if applicable, describe any required time frame within which those services must have been provided]?"

___ Yes, the Bidder has provided my organization with the services described above.

___ No, the Bidder has not provided my organization with the services described above.

___ I am unwilling or unable to provide any information about the services described above.

(C) For each customer reference, the Bidder must, at a minimum, provide the name and e-mail address for a contact person.

Bidders are also requested to include the title of the contact person. It is the sole responsibility of the Bidder to ensure that it provides a contact who is knowledgeable about the services the Bidder has provided to its customer and who is willing to act as a customer reference. Crown references will be accepted.

(vi) **Corporate Profile**: The Bidder is requested to provide a corporate profile, which should include an overview of the Bidder and any subcontractors, and/or authorized agents of the Bidder that would be involved in the performance of the Work on the Bidder's behalf. The Bidder is requested to provide a brief description of its size, corporate structure, years in business, business activities, major customers, number of employees and their geographic presence. This information is requested for information purposes only and will not be evaluated.

3.3 Section II: Financial Bid

(a) **Pricing**: Bidders must submit their financial bid in accordance with the Pricing Schedule provided in Attachment 5. The total amount of Applicable Taxes must be shown separately, if applicable. Unless otherwise indicated, bidders must include a single, firm, all-inclusive per diem rate quoted in Canadian dollars in each cell requiring an entry in the pricing tables.

(b) **Variation in Resource Rates By Time Period**: For any given resource category, where the financial tables provided by Canada allow different firm rates to be charged for a resource category during different time periods:

(i) the rate bid must not increase by more than 5% from one time period to the next, and

(ii) the rate bid for the same resource category during any subsequent time period must not be lower than the rate bid for the time period that includes the first month of the Initial Contract Period.

(c) **All Costs to be Included**: The financial bid must include all costs for the requirement described in the bid solicitation for the entire Contract Period, including any option periods. The identification of all necessary equipment, software, peripherals, cabling and components required to meet the requirements of the bid solicitation and the associated costs of these items is the sole responsibility of the Bidder.

(d) **Blank Prices**: Bidders are requested to insert "$0.00" for any item for which it does not intend to charge or for items that are already included in other prices set out in the tables. If the Bidder leaves any price blank, Canada will treat the price as "$0.00" for evaluation purposes and may request that the Bidder confirm that the price is, in fact, $0.00. No bidder will be permitted to add or change a price as part of this confirmation. Any bidder who does not confirm that the price for a blank item is $0.00 will be declared non-responsive.

3.4 Section III: Certifications

It is a requirement that bidders submit the certifications identified under Part 5.

3.5 Section IV: Additional Information

(a) **Bidder's Proposed Site(s) or Premises Requiring Safeguarding Measures**

As indicated in Part 6 under Security Requirements, the Bidder must provide the full address(es) of the Bidder's and proposed individual(s)' site(s) or premises for which safeguarding measures are required for Work Performance.

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

The Company Security Officer (CSO) must ensure through the Industrial Security Program (ISP) that the Bidder and proposal individual(s) hold a valid security clearance at the required level, as indicated in Part 6 – Security, Financial and Other Requirements.

Bidders are requested to indicate this information on their Bid Submission Form.

PART 4 - EVALUATION PROCEDURES AND BASIS OF SELECTION

4.1 Evaluation Procedures

(a) Bids will be assessed in accordance with the entire requirement of the bid solicitation including the technical and financial evaluation criteria. There are several steps in the evaluation process, which are described below. Even though the evaluation and selection will be conducted in steps, the fact that Canada has proceeded to a later step does not mean that Canada has conclusively determined that the Bidder has successfully passed all the previous steps. Canada may conduct steps of the evaluation in parallel.

(b) An evaluation team composed of representatives of the Client and PWGSC will evaluate the bids on behalf of Canada. Canada may hire any independent consultant, or use any Government resources, to evaluate any bid. Not all members of the evaluation team will necessarily participate in all aspects of the evaluation.

(c) In addition to any other time periods established in the bid solicitation:

(i) **Requests for Clarifications**: If Canada seeks clarification or verification from the Bidder about its bid, the Bidder will have two working days (or a longer period if specified in writing by the Contracting Authority) to provide the necessary information to Canada. Failure to meet this deadline will result in the bid being declared non-responsive.

(ii) **Requests for Further Information**: If Canada requires additional information in order to do any of the following pursuant to the Section entitled "Conduct of Evaluation" in 2003, Standard Instructions - Goods or Services - Competitive Requirements:

(A) verify any or all information provided by the Bidder in its bid; or

(B) contact any or all references supplied by the Bidder (e.g., references named in the résumés of individual resources) to verify and validate any information submitted by the Bidder,

the Bidder must provide the information requested by Canada within two working days of a request by the Contracting Authority.

(iii) **Extension of Time**: If additional time is required by the Bidder, the Contracting Authority may grant an extension in his or her sole discretion.

4.2 Technical Evaluation

(a) **Mandatory Technical Criteria:**

(i) Each bid will be reviewed for compliance with the mandatory requirements of the bid solicitation. Any element of the bid solicitation that is identified specifically with the words "must" or "mandatory" is a mandatory requirement. Bids that do not comply with each and every mandatory requirement will be declared non-responsive and be disqualified.

(ii) The mandatory technical criteria are described in Attachment 3.

(b) **Point-Rated Technical Criteria:**

(i) Each bid will be rated by assigning a score to the rated requirements, which are identified in the bid solicitation by the word "rated" or by reference to a score. Bidders who fail to submit complete bids with all the information requested by this bid solicitation will be rated accordingly.

(ii) The rated requirements are described in Attachment 4.

(c) **Number of Resources Evaluated**:

Only a certain number of resources per Resource Category will be evaluated as part of this bid solicitation as identified in Attachment 3. Additional Resources will only be assessed after contract award once specific tasks are requested of the Contractor. After contract award, the

Task Authorization process will be in accordance with Part 7 – Resulting Contract Clauses, the Article titled "Task Authorization". When a Task Authorization Form (TA Form) is issued, the Contractor will be requested to propose a resource to satisfy the specific requirement based on the TA Form's Statement of Work. The proposed resource will then be assessed against the criteria identified in the Contract's Statement of Work in accordance with Appendix I of Annex A.

(d) **Reference Checks**:

(i) Whether or not to conduct reference checks is discretionary. However, if PWGSC chooses to conduct reference checks for any given rated or mandatory requirement, it will check the references for that requirement for all bidders to be recommended for contract award.

(ii) For reference checks, Canada will conduct the reference check in writing by email. Canada will send all email reference check requests to contacts supplied by all the Bidders on the same day using the email address provided in the bid. Canada will not award any points and/or a bidder will not meet the mandatory experience requirement (as applicable) unless the response is received within 5 working days of the date that Canada's email was sent.

(iii) If Canada does not receive a response from the contact person within the 5 working days, Canada will not contact the Bidder and will not permit the substitution of an alternate contact person.

(iv) Wherever information provided by a reference differs from the information supplied by the Bidder, the information supplied by the reference will be the information evaluated.

(v) Points will not be allocated and/or a bidder will not meet the mandatory experience requirement (as applicable) if (1) the reference customer states he or she is unable or unwilling to provide the information requested, or (2) the customer reference is not a customer of the Bidder itself (for example, the customer cannot be the customer of an affiliate of the Bidder instead of being a customer of the Bidder itself). Nor will points be allocated or a mandatory met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Bidder.

4.3 Financial Evaluation

(a) The financial evaluation will be conducted by calculating the Total Bid Price using the Pricing Tables in Attachment 5 completed by the bidders.

(b) **Substantiation of Professional Services Rates**

In Canada's experience, bidders will from time to time propose rates at the time of bidding for one or more categories of resources that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. When evaluating the rates bid for professional services, Canada may, but will have no obligation to, require price support in accordance with this Article. If Canada requests price support, it will be requested from all otherwise responsive bidders who have proposed a rate that is at least 20% lower than the median rate bid by all responsive bidders for the relevant resource category or categories. If Canada requests price support, the Bidder must provide the following information:

(i) an invoice (referencing a contract serial number or other unique contract identifier) that shows that the Bidder has provided and invoiced a customer (with whom the Bidder deals at arm's length) for services performed for that customer similar to the services that would be provided in the relevant resource category, where those services were provided for at least three months within the eighteen months before the date of this request for rate substantiation, and the fees charged were equal to or less than the rate offered to Canada;

(ii) in relation to the invoice in (i), evidence from the Bidder's customer that the services identified in the invoice include at least 50% of the tasks listed in the Statement of Work

for the category of resource being assessed for an unreasonably low rate. This evidence must consist of either a copy of the contract (which must describe the services to be provided and demonstrate that at least 50% of the tasks to be performed are the same as those to be performed under the Statement of Work in this bid solicitation) or the customer's signed certification that the services subject to the charges in the invoice included at least 50% of the same tasks to be performed under the Statement of Work in this bid solicitation;

(iii) in respect of each contract for which an invoice is submitted as substantiation, a résumé for the resource that provided the services under that contract that demonstrates that, in relation to the resource category for which the rates are being substantiated, the resource would meet the mandatory requirements and achieve any required pass mark for any rated criteria; and

(iv) the name, telephone number and, if available, e-mail address of a contact person at the customer who received each invoice submitted under (i), so that Canada may verify any information provided by the Bidder.

Once Canada requests substantiation of the rates bid for any resource category, it is the sole responsibility of the Bidder to submit information (as described above and as otherwise may be requested by Canada, including information that would allow Canada to verify information with the resource proposed) that will allow Canada to determine whether it can rely, with confidence, on the Bidder's ability to provide the required services at the rates bid. If Canada determines that the information provided by the Bidder does not adequately substantiate the unreasonably low rates, the bid will be declared non-responsive.

(c) **Formulae in Pricing Tables**

If the pricing tables provided to bidders include any formulae, Canada may re-input the prices provided by bidders into a fresh table, if Canada believes that the formulae may no longer be functioning properly in the version submitted by a Bidder.

4.4 Basis of Selection

(a) To be declared responsive, a bid must:

(i) comply with all the requirements of the bid solicitation;

(ii) meet all mandatory criteria; and

(iii) obtain the required minimum pass mark for the technical evaluation criteria which are subject to point rating.

(b) Bids not meeting (i) or (ii) or (iii) will be declared non-responsive.

(c) The selection will be based on the highest responsive combined rating of technical merit and price. The ratio will be 60% for the technical merit and 40% for the price.

(d) To establish the technical merit score, the overall technical score for each responsive bid will be determined as follows:

total number of points obtained / maximum number of points available multiplied by the ratio of 60%.

(e) To establish the pricing score, each responsive bid will be prorated against the lowest evaluated price and the ratio of 40%.

(f) For each responsive bid, the technical merit score and the pricing score will be added to determine its combined rating.

(g) Neither the responsive bid obtaining the highest technical score nor the one with the lowest evaluated price will necessarily be accepted. The responsive bid with the highest combined rating of technical merit and price will be recommended for award of a contract.

(h) The table below illustrates an example where all three bids are responsive and the selection of the contractor is determined by a 60/40 ratio of technical merit and price, respectively. The total available points equals 135 and the lowest evaluated price is $45,000 (45).

Basis of Selection - Highest Combined Rating Technical Merit (60%) and Price (40%)				
		BIDDER 1	BIDDER 2	BIDDER 3
Overall Technical Score		115/135	89/135	92/135
Total Bid Price		$55,000.00	$50,000.00	$45,000.00
Calculations	**Technical Merit Score**	115/135 x 60 = 51.11	89/135 x 60 = 39.56	92/135 x 60 = 40.89
	Pricing Score	45/55 x 40 = 32.72	45/50 x 40 = 36.00	45/45 x 40 = 40.00
Combined Rating		83.83	75.56	80.89
Overall Rating		1st	3rd	2nd

(i) One contract may be awarded in total as a result of this bid solicitation.

(j) Bidders should note that all contract awards are subject to Canada's internal approvals process, which includes a requirement to approve funding in the amount of any proposed contract. Despite the fact that the Bidder may have been recommended for contract award, a contract will only be awarded if internal approval is granted according to Canada's internal policies. If approval is not granted, no contract will be awarded.

(k) If more than one Bidder is ranked first because of identical overall scores, then the Bidder with the higher Technical Score will become the top-ranked bidder.

PART 5 – CERTIFICATIONS AND ADDITIONAL INFORMATION

Bidders must provide the required certifications and additional information to be awarded a contract.

The certifications provided by Bidders to Canada are subject to verification by Canada at all times. Canada will declare a bid non-responsive, or will declare a contractor in default if any certification made by the Bidder is found to be untrue, whether made knowingly or unknowingly, during the bid evaluation period or during the contract period.

The Contracting Authority will have the right to ask for additional information to verify Bidder's certifications. Failure to comply and to cooperate with any request or requirement imposed by the Contracting Authority will render the bid non-responsive or constitute a default under the Contract.

5.1 Certifications Precedent to Contract Award and Additional Information

The certifications and additional information listed below should be submitted with the bid, but may be submitted afterwards. If any of these required certifications or additional information is not completed and submitted as requested, the Contracting Authority will inform the Bidder of a time frame within which to provide the information. Failure to provide the certifications or the additional information listed below within the time frame provided will render the bid non-responsive.

(a) Federal Contractors Program for Employment Equity - Bid Certification

By submitting a bid, the Bidder certifies that the Bidder, and any of the Bidder's members if the Bidder is a Joint Venture, is not named on the Federal Contractors Program (FCP) for employment equity "FCP Limited Eligibility to Bid" list (http://www.labour.gc.ca/eng/standards_equity/eq/emp/fcp/list/inelig.shtml) available from Employment and Social Development Canada (ESDC) - Labour's website.

Canada will have the right to declare a bid non-responsive if the Bidder, or any member of the Bidder if the Bidder is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list at the time of contract award.

Canada will also have the right to terminate the Contract for default if a Contractor, or any member of the Contractor if the Contractor is a Joint Venture, appears on the "FCP Limited Eligibility to Bid" list during the period of the Contract.

The Bidder must provide the Contracting Authority with a completed Attachment 6, Federal Contractors Program for Employment Equity - Certification, before contract award. If the Bidder is a Joint Venture, the Bidder must provide the Contracting Authority with a completed Attachment Federal Contractors Program for Employment Equity - Certification, for each member of the Joint Venture.

5.2 Additional Certifications Precedent to Contract Award

(a) Professional Services Resources

(i) By submitting a bid, the Bidder certifies that, if it is awarded a contract as a result of the bid solicitation, every individual proposed in its bid will be available to perform the Work as required by Canada's representatives and at the time specified in the bid solicitation or agreed to with Canada's representatives.

(ii) By submitting a bid, the Bidder certifies that all the information provided in the résumés and supporting material submitted with its bid, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Bidder to be true and accurate. Furthermore, the Bidder warrants that every individual proposed by the Bidder for the requirement is capable of performing the Work described in the resulting contract.

(iii) If a Bidder has proposed any individual who is not an employee of the Bidder, by submitting a bid, the Bidder certifies that it has the permission from that individual to

propose his/her services in relation to the Work to be performed and to submit his/her résumé to Canada. The Bidder must, upon request from the Contracting Authority, provide a written confirmation, signed by the individual, of the permission given to the Bidder and of his/her availability. Failure to comply with the request may result in the bid being declared non-responsive.

(b) **Submission of Only One Bid**

By submitting a bid, the Bidder is certifying that it does not consider itself to be related to any other bidder.

PART 6 - SECURITY, FINANCIAL AND OTHER REQUIREMENTS

6.1 Security Requirement

(a) At the date of bid closing, the following conditions must be met:

(i) the Bidder must hold a valid organization security clearance as indicated in Part 7 - Resulting Contract Clauses;

(ii) the Bidder's proposed individuals requiring access to classified or protected information, assets or sensitive work site(s) must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses; and

(iii) the Bidder's proposed location of work performance and document safeguarding must meet the security requirements as indicated in Part 7 - Resulting Contract Clauses;

(iv) the Bidder must provide the address(es) of proposed site (s) or premises of work performance and document safeguarding as indicated in Part 3 - Section IV Additional Information.

(b) For additional information on security requirements, Bidders should refer to the Industrial Security Program (ISP) of Public Works and Government Services Canada (http://ssi-iss.tpsgc-pwgsc.gc.ca/index-eng.html) website.

(c) In the case of a joint venture bidder, each member of the joint venture must meet the security requirements.

6.2 Financial Capability

(a) SACC Manual clause A9033T (2012-07-16) Financial Capability applies, except that subsection 3 is deleted and replaced with the following: "If the Bidder is a subsidiary of another company, then any financial information required by the Contracting Authority in 1(a) to (f) must be provided by each level of parent company, up to and including the ultimate parent company. The financial information of a parent company does not satisfy the requirement for the provision of the financial information of the Bidder; however, if the Bidder is a subsidiary of a company and, in the normal course of business, the required financial information is not generated separately for the subsidiary, the financial information of the parent company must be provided. If Canada determines that the Bidder is not financially capable but the parent company is, or if Canada is unable to perform a separate assessment of the Bidder's financial capability because its financial information has been combined with its parent's, Canada may, in its sole discretion, award the contract to the Bidder on the condition that the parent company grant a performance guarantee to Canada."

(b) In the case of a joint venture bidder, each member of the joint venture must meet the financial capability requirements.

PART 7 - RESULTING CONTRACT CLAUSES

The following clauses apply to and form part of any contract resulting from the bid solicitation.

7.1 Requirement

(a) _____ (the "**Contractor**") agrees to supply to the Client the services described in the Contract, including the Statement of Work, in accordance with, and at the prices set out in, the Contract. This includes providing professional services as and when requested by Canada, to one or more locations to be designated by Canada, excluding any locations in areas subject to any of the Comprehensive Land Claims Agreements.

(b) **Client**: Under the Contract, the "**Client**" is the Department of Justice.

(c) **Reorganization of Client**: The Contractor's obligation to perform the Work will not be affected by (and no additional fees will be payable as a result of) the renaming, reorganization, reconfiguration, or restructuring of any Client. The reorganization, reconfiguration and restructuring of the Client includes the privatization of the Client, its merger with another entity, or its dissolution, where that dissolution is followed by the creation of another entity or entities with mandates similar to the original Client. In connection with any form of reorganization, Canada may designate another department or government body as the Contracting Authority or Technical Authority, as required to reflect the new roles and responsibilities associated with the reorganization.

(d) **Defined Terms**: Words and expressions defined in the General Conditions or Supplemental General Conditions and used in the Contract have the meanings given to them in the General Conditions or Supplemental General Conditions. Any reference to an Identified User in the Supply Arrangement is a reference to the Client. Also, any reference to a "deliverable" or "deliverables" includes all documentation outlined in this Contract. A reference to a "local office" of the Contractor means an office having at least one full time employee that is not a shared resource working at that location.

7.2 Task Authorization

(a) **As-and-when-requested Task Authorizations**: The Work or a portion of the Work to be performed under the Contract will be on an "as-and-when-requested basis" using a Task Authorization (TA). The Work described in the TA must be in accordance with the scope of the Contract. The Contractor must not commence work until a validly issued TA has been issued by Canada and received by the Contractor. The Contractor acknowledges that any work performed before such issuance and receipt will be done at the Contractor's own risk.

(b) **Assessment of Resources Proposed at TA Stage**: Processes for issuing, responding to and assessing Task Authorizations are further detailed in Appendices G, H, I and J of Annex A.

(c) **Form and Content of draft Task Authorization**:

(i) The Technical Authority will provide the Contractor with a description of the task in a draft Task Authorization using the form specified in Appendix H to Annex A.

(ii) The draft Task Authorization will contain the details of the activities to be performed, and must also contain the following information:

(A) the task number;

(B) The date by which the Contractor's response must be received (which will appear in the draft Task Authorization, but not the issued Task Authorization);

(C) the details of any financial coding to be used;

(D) the categories of resources and the number required;

(E) a description of the work for the task outlining the activities to be performed and identifying any deliverables (such as reports);

(F) the start and completion dates;

(G) milestone dates for deliverables and payments (if applicable);

(H) the number of person-days of effort required;

(I) whether the work requires on-site activities and the location;

(J) the language profile of the resources required;

(K) the level of security clearance required of resources; and

(L) any other constraints that might affect the completion of the task.

(d) **Contractor's Response to Draft Task Authorization**: The Contractor must provide to the Technical Authority, within two working days of receiving the draft Task Authorization (or within any longer time period specified in the draft TA), the proposed total price for performing the task and a breakdown of that cost, established in accordance with the Basis of Payment specified in the Contract. The Contractor's quotation must be based on the rates set out in the Contract. The Contractor will not be paid for preparing or providing its response or for providing other information required to prepare and validly issue the TA.

(e) **Task Authorization Limit and Authorities for Validly Issuing Task Authorizations**:

To be validly issued, a TA must include the following signatures:

(i) for any TA, inclusive of revisions, with a value less than or equal to $300,000.00 (excluding Applicable Taxes), the TA must be signed by the Technical Authority; and

(ii) for any TA with a value greater than this amount, a TA must be signed by the Technical Authority and Contracting Authority.

Any TA that does not bear the appropriate signature(s) is not validly issued by Canada. Any work performed by the Contractor without receiving a validly issued TA is done at the Contractor's own risk. If the Contractor receives a TA that is not appropriately signed, the Contractor must notify the Contracting Authority. By providing written notice to the Contractor, the Contracting Authority may suspend the Client's ability to issue TA's at any time, or reduce the dollar value threshold described in sub-article (i) above; any suspension or reduction notice is effective upon receipt.

(f) **Periodic Usage Reports**:

(i) The Contractor must compile and maintain records on its provision of services to the federal government under Task Authorizations validly issued under the Contract. The Contractor must provide this data to Canada in accordance with the reporting requirements detailed below. If some data is not available, the reason must be indicated. If services are not provided during a given period, the Contractor must still provide a "NIL" report. The data must be submitted on a quarterly basis to the Contracting Authority. From time to time, the Contracting Authority may also require an interim report during a reporting period.

(ii) The quarterly periods are defined as follows:

(A) 1st quarter: April 1 to June 30;

(B) 2nd quarter: July 1 to September 30;

(C) 3rd quarter: October 1 to December 31; and

(D) 4th quarter: January 1 to March 31.

The data must be submitted to the Contracting Authority no later than 15 calendar days after the end of the reporting period.

(iii) Each report must contain the following information for each validly issued TA (as amended):

(A) the Task Authorization number and the Task Authorization Revision number(s), if applicable;

(B) a title or a brief description of each authorized task;

(C) the name, Resource Category and level of each resource involved in performing the TA, as applicable;

(D) the total estimated cost specified in the validly issued TA of each task, exclusive of Applicable Taxes;

(E) the total amount, exclusive of Applicable Taxes, expended to date against each authorized task;

(F) the start and completion date for each authorized task; and

(G) the active status of each authorized task, as applicable (e.g., indicate whether work is in progress or if Canada has cancelled or suspended the TA, etc.).

(iv) Each report must also contain the following cumulative information for all the validly issued TA's (as amended):

(A) the amount, exclusive of Applicable Taxes, specified in the Contract (as last amended, as applicable) as Canada's total liability to the Contractor for all validly issued TA's; and

(B) the total amount, exclusive of Applicable Taxes, expended to date against all validly issued TA's.

(g) **Consolidation of TA's for Administrative Purposes**: The Contract may be amended from time to time to reflect all validly issued Task Authorizations to date, to document the Work performed under those TA's for administrative purposes.

7.3 Standard Clauses and Conditions

All clauses and conditions identified in the Contract by number, date and title are set out in the Standard Acquisition Clauses and Conditions Manual (https://buyandsell.gc.ca/policy-and-guidelines/standard-acquisition-clauses-and-conditions-manual) issued by Public Works and Government Services Canada.

(a) **General Conditions**:

(i) 2035 (2016-04-04), General Conditions - Higher Complexity - Services, apply to and form part of the Contract.

With respect to Section 30 - Termination for Convenience, of General Conditions 2035, Subsection 04 is deleted and replaced with the following Subsections 04, 05 and 06:

4. The total of the amounts, to which the Contractor is entitled to be paid under this section, together with any amounts paid, due or becoming due to the Contractor must not exceed the Contract Price.

5. Where the Contracting Authority terminates the entire Contract and the Articles of Agreement include a Minimum Work Guarantee, the total amount to be paid to the Contractor under the Contract will not exceed the greater of:

(a) the total amount the Contractor may be paid under this section, together with any amounts paid, becoming due other than payable under the Minimum Revenue Guarantee, or due to the Contractor as of the date of termination, or

(b) the amount payable under the Minimum Work Guarantee, less any amounts paid, due or otherwise becoming due to the Contractor as of the date of termination.

6. The Contractor will have no claim for damages, compensation, loss of profit, allowance arising out of any termination notice given by Canada under this section except to the extent that this section expressly provides. The Contractor agrees to repay immediately

to Canada the portion of any advance payment that is unliquidated at the date of the termination.

(b) **Supplemental General Conditions**:

The following Supplemental General Conditions:

(i) 4006 (2010-08-16), Supplemental General Conditions - Contractor to Own Intellectual Property Rights in Foreground Information;

(ii) 4008 (2008-12-12), Supplemental General Conditions - Personal Information;

apply to and form part of the Contract.

7.4 Protection and Security of Data Stored in Databases

(a) The Contractor must ensure that all the databases containing any information related to the Work are located in Canada or, if the Contracting Authority has first consented in writing, in another country where:

(i) equivalent protections are given to personal information as in Canada under legislation such as the Privacy Act, R.S. 1985, c.P-21, and the Personal Information Protection and Electronic Documents Act, S.C. 2000, c.5, and under any applicable policies of the Government of Canada; and

(ii) the laws do not allow the government of that country or any other entity or person to seek or obtain the right to view or copy any information relating to the Contract without first obtaining the Contracting Authority's written consent.

In connection with giving its consent to locating a database in another country, the Contracting Authority may, at its option, require the Contractor to provide a legal opinion (from a lawyer qualified in the foreign country) that the laws in that country meet the above requirements, or may require the Contractor to pay for Canada to obtain such a legal opinion. Canada has the right to reject any request to store Canada's data in a country other than Canada if there is any reason to be concerned about the security, privacy, or integrity of Canada's data. Canada may also require that any data sent or processed outside of Canada be encrypted with Canada-approved cryptography and that the private key required to decrypt the data be kept in Canada in accordance with key management and storage processes approved by Canada.

(b) The Contractor must control access to all databases on which any data relating to the Contract is stored so that only individuals with the appropriate security clearance are able to access the database, either by using a password or other form of access control (such as biometric controls).

(c) The Contractor must ensure that all databases on which any data relating to the Contract is stored are physically and logically independent (meaning there is no direct or indirect connection of any kind) from all other databases, unless those databases are located in Canada (or in an another country approved by the Contracting authority under subsection (a)) and otherwise meet the requirements of this article.

(d) The Contractor must ensure that all data relating to the Contract is processed only in Canada or in another country approved by the Contracting Authority under subsection (a).

(e) The Contractor must ensure that all domestic network traffic (meaning traffic or transmissions initiated in one part of Canada to a destination or individual located in another part of Canada) is routed exclusively through Canada, unless the Contracting Authority has first consented in writing to an alternate route. The Contracting Authority will only consider requests to route domestic traffic through another country that meets the requirements of subsection (a).

(f) Despite any section of the General Conditions relating to subcontracting, the Contractor must not subcontract (including to an affiliate) any function that involves providing a subcontractor with access to any data relating to the Contract unless the Contracting Authority first consents in writing.

7.5 Security Requirement

(a) General

(i) The Contractor must, at all times during the performance of the Contract, hold a valid Facility Security Clearance at the level of SECRET, with approved Document Safeguarding at the level of SECRET, issued by the Canadian Industrial Security Directorate (CISD), Public Works and Government Services Canada (PWGSC).

(ii) The Contractor personnel requiring access to PROTECTED/CLASSIFIED information, assets or sensitive work site(s) must EACH hold a valid personnel security screening at the level of SECRET, granted or approved by the CISD/PWGSC.

(iii) The Contractor MUST NOT utilize its Information Technology systems to electronically process, produce or store any sensitive PROTECTED/CLASSIFIED information until CISD/PWGSC has issued written approval. After approval has been granted, these tasks may be performed at the level of SECRET and an IT Link at the level of SECRET.

(iv) Subcontracts which contain security requirements are NOT to be awarded without the prior written permission of CISD/PWGSC.

(v) The Contractor must comply with the provisions of the:

(A) Security Requirements Check List and security guide (if applicable), attached at Annex C;
(B) Industrial Security Manual (Latest Edition).

(b) Contractor's Site(s) or Premises Requiring Safeguarding Measures

(i) The Contractor must diligently maintain up-to-date, the information related to the Contractor's and individual(s) site(s) or premises, where safeguarding measures are required in the performance of the Work, for the following address:

Street Number / Street Name, Unit / Suite / Apartment Number
City, Province, Territory / State
Postal Code / Zip Code
Country

(ii) The Company Security Officer (CSO) must ensure through the Industrial Security Program (ISP) that the Contractor and individual(s) hold a valid security clearance at the required level.

7.6 Contract Period

(a) **Contract Period**: The "**Contract Period**" is the entire period of time during which the Contractor is obliged to perform the Work, which includes:

(i) The "**Initial Contract Period**", which begins on the date the Contract is awarded and ends four years later; and

(ii) The period during which the Contract is extended, if Canada chooses to exercise any options set out in the Contract.

(b) **Option to Extend the Contract**:

(i) The Contractor grants to Canada the irrevocable option to extend the term of the Contract by up to two additional 1-year periods under the same terms and conditions. The Contractor agrees that, during the extended period of the Contract, it will be paid in accordance with the applicable provisions set out in the Basis of Payment.

(ii) Canada may exercise this option at any time by sending a written notice to the Contractor before the expiry date of the Contract. The option may only be exercised by the

Contracting Authority, and will be evidenced, for administrative purposes only, through a contract amendment.

7.7 Authorities

(a) Contracting Authority

The Contracting Authority for the Contract is:

Name: Jonah Dubé
Title: Supply Specialist
Public Works and Government Services Canada
Acquisitions Branch
Directorate: Informatics and Telecommunications Systems Procurement Directorate
Address: 11 Laurier St., Gatineau, Québec
Telephone: 873-469-4980
E-mail address: Jonah.dube@tpsgc-pwgsc.gc.ca

The Contracting Authority is responsible for the management of the Contract and any changes to the Contract must be authorized in writing by the Contracting Authority. The Contractor must not perform work in excess of or outside the scope of the Contract based on verbal or written requests or instructions from anybody other than the Contracting Authority.

(b) Technical Authority

The Technical Authority for the Contract is:

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: _____
Facsimile: _____
E-mail address: _____

The Technical Authority is the representative of the department or agency for whom the Work is being carried out under the Contract and is responsible for all matters concerning the technical content of the Work under the Contract. Technical matters may be discussed with the Technical Authority; however, the Technical Authority has no authority to authorize changes to the scope of the Work. Changes to the scope of the Work can only be made through a contract amendment issued by the Contracting Authority.

(c) **Contractor's Representative**

Name: _____
Title: _____
Organization: _____
Address: _____
Telephone: _____
Facsimile: _____
E-mail address: _____

7.8 Proactive Disclosure of Contracts with Former Public Servants

By providing information on its status, with respect to being a former public servant in receipt of a Public Service Superannuation Act (PSSA) pension, the Contractor has agreed that this information will be reported on departmental web sites as part of the published proactive disclosure reports, in accordance with Contracting Policy Notice: 2012-2 of the Treasury Board Secretariat of Canada.

7.9 Payment

(a) **Basis of Payment**

(i) **Professional Services provided under a Task Authorization with a Maximum Price**: For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor, in arrears, up to the Maximum Price for the TA, for actual time worked and any resulting deliverables in accordance with the firm all-inclusive per diem rates set out in Annex B, Basis of Payment, Applicable Taxes extra. Partial days will be prorated based on actual hours worked based on a 7.5-hour workday**.**

(ii) **Professional Services provided under a Task Authorization with a Firm Price**: For professional services requested by Canada, in accordance with a validly issued Task Authorization, Canada will pay the Contractor the firm price set out in the Task Authorization (based on the firm, all-inclusive per diem rates set out in Annex B), Applicable Taxes extra.

(iii) **Firm Monthly Price**: Canada will pay the Contractor the firm monthly price set out in the Contract (based on the firm, all-inclusive monthly prices and per user monthly prices set out in Annex B), Applicable Taxes extra.

(iv) **Replacement Parts:** For replacement parts required to perform Level 2 On-Site and Break/Fix Services as described in the Statement of Work, Canada will pay the Contractor the laid down cost plus the firm mark-up rate set out in Annex B, Basis of Payment, Applicable Taxes extra.

(v) **Travel and Living Expenses – National Joint Council Travel Directive**: Canada will not pay any travel or living expenses associated with performing the Work.

(vi) **Competitive Award**: The Contractor acknowledges that the Contract has been awarded as a result of a competitive process. No additional charges will be allowed to compensate for errors, oversights, misconceptions or underestimates made by the Contractor when bidding for the Contract.

(vii) **Professional Services Rates**: In Canada's experience, bidders from time to time propose rates at the time of bidding for one or more Resource Categories that they later refuse to honour, on the basis that these rates do not allow them to recover their own costs and/or make a profit. This denies Canada of the benefit of the awarded contract. If the Contractor does not respond or refuses to provide an individual with the qualifications described in the Contract within the time described in the Contract (or proposes instead to provide someone from an alternate category at a different rate), whether or not Canada terminates the Contract as a whole or in part or chooses to exercise any of the rights provided to it under the general conditions, Canada may impose sanctions or take other measures in accordance with the PWGSC Vendor Performance Corrective Measure Policy (or equivalent) then in effect, which measures may include an assessment that results in conditions applied against the Contractor to be fulfilled before doing further business with Canada, or full debarment of the Contractor from bidding on future requirements.

(b) **Limitation of Expenditure**

(i) Canada's total liability to the Contractor under the Contract must not exceed the amount set out on page 1 of the Contract, less any Applicable taxes. With respect to the amount set out on page 1 of the Contract, Customs duties are included and Applicable Taxes are included. Any commitments to purchase specific amounts or values of goods or services are described elsewhere in the Contract.

(ii) No increase in the total liability of Canada or in the price of the Work resulting from any design changes, modifications or interpretations of the Work, will be authorized or paid to the Contractor unless these design changes, modifications or interpretations have been approved, in writing, by the Contracting Authority before their incorporation into the Work. The Contractor must not perform any work or provide any service that would result in Canada's total liability being exceed before obtaining the written approval of the

Contracting Authority. The Contractor must notify the Contracting Authority in writing as to the adequacy of this sum:

(A) when it is 75 percent committed, or

(B) 4 months before the Contract expiry date, or

(C) as soon as the Contractor considers that the contract funds provided are inadequate for the completion of the Work,

whichever comes first.

(iii) If the notification is for inadequate contract funds, the Contractor must provide to the Contracting Authority a written estimate for the additional funds required. Providing this information does not increase Canada's liability.

(c) **Method of Payment - Monthly Payment**

Canada will pay the Contractor on a monthly basis for work performed during the month covered by the invoice in accordance with the payment provisions of the Contract if:

(i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

(ii) all such documents have been verified by Canada; and

(iii) the Work performed has been accepted by Canada.

(d) **Method of Payment for Task Authorizations with a Maximum Price**: For each Task Authorization validly issued under the Contract that contains a maximum price:

(i) Canada will pay the Contractor no more frequently than once a month in accordance with the Basis of Payment. The Contractor must submit time sheets for each resource showing the days and hours worked to support the charges claimed in the invoice.

(ii) Once Canada has paid the maximum TA price, Canada will not be required to make any further payment, but the Contractor must complete all the work described in the TA, all of which is required to be performed for the maximum TA price. If the work described in the TA is completed in less time than anticipated, and the actual time worked (as supported by the time sheets) at the rates set out in the Contract is less than the maximum TA price, Canada is only required to pay for the time spent performing the work related to that TA.

(e) **Method of Payment for Task Authorizations with a Firm Price - Lump Sum Payment on Completion**: Canada will pay the Contractor upon completion and delivery of all the Work associated with the validly issued Task Authorization in accordance with the payment provisions of the Contract if:

(i) an accurate and complete invoice and any other documents required by the Contract have been submitted in accordance with the invoicing instructions provided in the Contract;

(ii) all such documents have been verified by Canada; and

(iii) the Work delivered has been accepted by Canada.

(f) **Time Verification**

Time charged and the accuracy of the Contractor's time recording system are subject to verification by Canada, before or after payment is made to the Contractor. If verification is done after payment, the Contract must repay any overpayment, at Canada's request.

(g) **Payment Credits**

(i) **Late Completion of Client Transition Phase:** If the Contractor does not provide Help Desk and Support Services to Canada by the Service Go Live Date specified in the Contract, the Contractor must provide a credit to Canada of $2,000 for each calendar day of delay.

(ii) **Failure to Meet Service Level Targets:** If the Contractor fails to meet any of the following Service Level Targets (as described in Annex A), it must provide a credit to Canada in the amount of 10% of the total billing for that month:

(A) Service Level Target Service Delivery Portal Maximum Service Outage Time (SLT-SDP-MSOT);

(B) Service Level Target Service Delivery Portal Maximum Time to Restore Service (SLT-SDP-MTRS);

(C) Service Level Target Service Desk Maximum Time to Answer (SLT-SD-MTA);

(D) Service Level Target Service Desk Maximum Time on Hold (SLT-SD-MTOH);

(E) Service Level Target Service Desk Maximum Time to Escalate (Standard) (SLT-SD-MTTE-1);

(F) Service Level Target Service Desk Maximum Time to Escalate (Premium) (SLT-SD-MTTE-2);

(G) Service Level Target Service Desk Maximum Time to Respond to Alternate Service Channel Incidents (SLT-SD-MTRASCI);

(H) Service Level Target Service Desk Minimum Level 1 Resolution Rate (SLT-SD-ML1RR);

(I) Service Level Target Escalated Support Maximum Time to Respond to Incident (Standard) (SLT-ES-MTTRTI-1);

(J) Service Level Target On-Site Support Maximum Time to Respond to Incident (Premium) (SLT-ES-MTTRTI-2);

(K) Service Level Target On-Site Support Maximum Time to Resolve from Incident (Standard) (SLT-ES-MTTRFI-1);

(L) Service Level Target On-Site Support Maximum Time to Resolve from Incident (Premium) (SLT-ES-MTTRFI-2);

(M) Service Level Target Engineering Support Maximum Time to Deploy Critical Security Update (SLT-ES-MTDCSU); and

(N) Service Level Target Service Request Fulfilment (SLT-SRF).

(iii) **Service Credit Calculation for Failure to Meet Service Levels:** The Contractor must calculate service credits based on the performance of the Work against the Service Level Targets for the previous month beginning on the first day of each calendar month and ending on the last day of that calendar month.

(iv) **Earn Back Credits:** If the Contractor succeeds in meeting all Service Level Targets for three consecutive months following the month of one or more missed Service Level Targets (i.e. a month where a service credit was remitted to Canada), the Contractor will earn back 50% of the service credit. If the Contractor succeeds in meeting all Service Level Targets for an additional three consecutive months (i.e. for a total of six consecutive months) the Contractor will earn back the remaining 50% of the service credit.

(v) **Failure to Provide Resource**: If the Contractor does not provide a required professional services resource that has all the required qualifications within the time prescribed by the Contract, the Contractor must credit to Canada an amount equal to the per diem rate

(based on a 7.5-hour workday) of the required resource for each day (or partial day) of delay in providing the resource, up to a maximum of 10 days.

(vi) **Corrective Measures**: If credits are payable under this Article for two consecutive months or for three months in any 12-month period, the Contractor must submit a written action plan describing measures it will implement or actions it will undertake to eliminate the recurrence of the problem. The Contractor will have five working days to deliver the action plan to the Client and the Contracting Authority and 20 working days to rectify the underlying problem.

(vii) **Termination for Failure to Meet Service Level Targets**: In addition to any other rights it has under the Contract, Canada may terminate the Contract for default in accordance with the General Conditions by giving the Contractor three months' written notice of its intent, if any of the following apply:

(A) the total amount of credits for a given monthly billing cycle reach a level of 10% of the total billing for that month; or

(B) the corrective measures required of the Contractor described above are not met.

This termination will be effective when the three month notice period expires, unless Canada determines that the Contractor has implemented the corrective measures to Canada's satisfaction during those three months.

(viii) **Credits Apply during Entire Contract Period**: The Parties agree that the credits apply throughout the Contract Period.

(ix) **Credits represent Liquidated Damages**: The Parties agree that the credits are liquidated damages and represent their best pre-estimate of the loss to Canada in the event of the applicable failure. No credit is intended to be, nor will it be construed as, a penalty.

(x) **Canada's Right to Obtain Payment**: The Parties agree that these credits are a liquidated debt. To collect the credits, Canada has the right to hold back, draw back, deduct or set off from and against any money Canada owes to the Contractor from time to time.

(xi) **Canada's Rights & Remedies not Limited**: The Parties agree that nothing in this Article limits any other rights or remedies to which Canada is entitled under the Contract (including the right to terminate the Contract for default) or under the law generally.

(xii) **Audit Rights**: The Contractor's calculation of credits under the Contract is subject to verification by government audit, at the Contracting Authority's discretion, before or after payment is made to the Contractor. The Contractor must cooperate fully with Canada during the conduct of any audit by providing Canada with access to any records and systems that Canada considers necessary to ensure that all credits have been accurately credited to Canada in the Contractor's invoices. If an audit demonstrates that past invoices contained errors in the calculation of the credits, the Contractor must pay to Canada the amount the audit reveals was required to be credited to Canada, plus interest, from the date Canada remitted the excess payment until the date of the refund (the interest rate is the Bank of Canada's discount annual rate of interest in effect on the date the credit was first owed to Canada, plus 1.25% per year). If, as a result of conducting an audit, Canada determines that the Contractor's records or systems for identifying, calculating or recording the credits are inadequate, the Contractor must implement any additional measures required by the Contracting Authority.

(h) **No Responsibility to Pay for Work not performed due to Closure of Government Offices**

(i) Where the Contractor, its employees, subcontractors, or agents are providing services on government premises under the Contract and those premises are inaccessible because of the evacuation or closure of government offices, and as a result no work is performed,

Canada is not responsible for paying the Contractor for work that otherwise would have been performed if there had been no evacuation or closure.

(ii) If, as a result of any strike or lock-out, the Contractor or its employees, subcontractors or agents cannot obtain access to government premises and, as a result, no work is performed, Canada is not responsible for paying the Contractor for work that otherwise would have been performed if the Contractor had been able to gain access to the premises

7.10 Invoicing Instructions

(a) The Contractor must submit invoices in accordance with the information required in the General Conditions.

(b) The Contractor's invoice must include a separate line item for each subparagraph in the Basis of Payment provision, and must show all applicable Task Authorization numbers.

(c) By submitting invoices, the Contractor is certifying that the goods and services have been delivered and that all charges are in accordance with the Basis of Payment provision of the Contract, including any charges for work performed by subcontractors.

(d) The Contractor must provide the original of each invoice to the Technical Authority. On request, the Contractor must provide a copy of any invoices requested by the Contracting Authority.

7.11 Certifications

(a) The continuous compliance with the certifications provided by the Contractor in its bid, any TA quotation and the ongoing cooperation in providing additional information are conditions of the Contract. Certifications are subject to verification by Canada during the entire Contract Period. If the Contractor does not comply with any certification, or fails to provide the additional information, or if it is determined that any certification made by the Contractor in its bid is untrue, whether made knowingly or unknowingly, Canada has the right, pursuant to the default provision of the Contract, to terminate the Contract for default.

7.12 Federal Contractors Program for Employment Equity - Default by Contractor

The Contractor understands and agrees that, when an Agreement to Implement Employment Equity (AIEE) exists between the Contractor and Employment and Social Development Canada (ESDC)-Labour, the AIEE must remain valid during the entire period of the Contract. If the AIEE becomes invalid, the name of the Contractor will be added to the "FCP Limited Eligibility to Bid" list. The imposition of such a sanction by ESDC will constitute the Contractor in default as per the terms of the Contract.

7.13 Applicable Laws

The Contract must be interpreted and governed, and the relations between the parties determined, by the laws in force in Ontario.

7.14 Priority of Documents

If there is a discrepancy between the wording of any documents that appear on the following list, the wording of the document that first appears on the list has priority over the wording of any document that appears later on the list:

(a) these Articles of Agreement, including any individual SACC clauses incorporated by reference in these Articles of Agreement;

(b) Supplemental General Conditions, in the following order:

(i) 4006 (2010-08-16), Supplemental General Conditions - Contractor to Own Intellectual Property Rights in Foreground Information;

(ii) 4008 (2008-12-12), Supplemental General Conditions - Personal Information.

(c) General Conditions 2035 (2016-04-04), Higher Complexity - Services;

(d) Annex A, Statement of Work, including its Appendices as follows;

(i) Appendix A to Annex A – Service Domain: JUS Service Desk Service

(ii) Appendix B to Annex A – Service Domain: JUS On-Site Support Service

(iii) Appendix C to Annex A – Service Domain: JUS Engineering Service

(iv) Appendix D to Annex A – Security Requirements

(v) Appendix E to Annex A – Definitions

(vi) Appendix F to Annex A – Standard Hardware and Software

(vii) Appendix G to Annex A – Tasking Procedures

(viii) Appendix H to Annex A – Task Authorization (TA) Form

(ix) Appendix I to Annex A – Resource Assessment Criteria and Response Tables

(x) Appendix J to Annex A – Certifications at the TA stage

(e) Annex B, Basis of Payment;

(f) Annex C, Security Requirements Check List;

(g) the validly issued Task Authorizations and any required certifications (including all of their annexes, if any); and

(h) the Contractor's bid dated _____.

7.15 Foreign Nationals (Canadian Contractor)

(a) SACC Manual clause A2000C (2006-06-16), Foreign Nationals (Canadian Contractor)

Note to Bidders: *Either this clause or the one that follows, whichever applies (based on whether the successful Bidder is a Canadian Contractor or Foreign Contractor), will be included in any resulting contract.*

7.16 Foreign Nationals (Foreign Contractor)

(a) SACC Manual clause A2001C (2006-06-16), Foreign Nationals (Foreign Contractor)

7.17 Insurance Requirements

(a) **Compliance with Insurance Requirements**

(i) The Contractor must comply with the insurance requirements specified in this Article. The Contractor must maintain the required insurance coverage for the duration of the Contract. Compliance with the insurance requirements does not release the Contractor from or reduce its liability under the Contract.

(ii) The Contractor is responsible for deciding if additional insurance coverage is necessary to fulfill its obligation under the Contract and to ensure compliance with any applicable law. Any additional insurance coverage is at the Contractor's expense, and for its own benefit and protection.

(iii) The Contractor should forward to the Contracting Authority within ten (10) days after the date of award of the Contract a Certificate of Insurance evidencing the insurance coverage. Coverage must be placed with an Insurer licensed to carry out business in Canada and the Certificate of Insurance must confirm that the insurance policy complying with the requirements is in force. If the Certificate of Insurance has not been completed and submitted as requested, the Contracting Authority will so inform the Contractor and provide the Contractor with a time frame within which to meet the requirement. Failure to

comply with the request of the Contracting Authority and meet the requirement within the time period will constitute a default under the General Conditions. The Contractor must, if requested by the Contracting Authority, forward to Canada a certified true copy of all applicable insurance policies.

(b) **Commercial General Liability Insurance**

(i) The Contractor must obtain Commercial General Liability Insurance, and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature, but for not less than $2,000,000 per accident or occurrence and in the annual aggregate.

(ii) The Commercial General Liability policy must include the following:

(A) Additional Insured: Canada is added as an additional insured, but only with respect to liability arising out of the Contractor's performance of the Contract. The interest of Canada should read as follows: Canada, as represented by Public Works and Government Services Canada.

(B) Bodily Injury and Property Damage to third parties arising out of the operations of the Contractor.

(C) Products and Completed Operations: Coverage for bodily injury or property damage arising out of goods or products manufactured, sold, handled, or distributed by the Contractor and/or arising out of operations that have been completed by the Contractor.

(D) Personal Injury: While not limited to, the coverage must include Violation of Privacy, Libel and Slander, False Arrest, Detention or Imprisonment and Defamation of Character.

(E) Cross Liability/Separation of Insureds: Without increasing the limit of liability, the policy must protect all insured parties to the full extent of coverage provided. Further, the policy must apply to each Insured in the same manner and to the same extent as if a separate policy had been issued to each.

(F) Blanket Contractual Liability: The policy must, on a blanket basis or by specific reference to the Contract, extend to assumed liabilities with respect to contractual provisions.

(G) Employees and, if applicable, Volunteers must be included as Additional Insured.

(H) Employers' Liability (or confirmation that all employees are covered by Worker's compensation (WSIB) or similar program)

(I) Broad Form Property Damage including Completed Operations: Expands the Property Damage coverage to include certain losses that would otherwise be excluded by the standard care, custody or control exclusion found in a standard policy.

(J) Notice of Cancellation: The Insurer will endeavour to provide the Contracting Authority thirty (30) days written notice of policy cancellation.

(K) If the policy is written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Contract.

(L) Owners' or Contractors' Protective Liability: Covers the damages that the Contractor becomes legally obligated to pay arising out of the operations of a subcontractor.

(M) Advertising Injury: While not limited to, the endorsement must include coverage for piracy or misappropriation of ideas, or infringement of copyright, trademark, title or slogan.

(c) **Errors and Omissions Liability Insurance**

(i) The Contractor must obtain Errors and Omissions Liability (a.k.a. Professional Liability) insurance, and maintain it in force throughout the duration of the Contract, in an amount usual for a contract of this nature but for not less than $1,000,000 per loss and in the annual aggregate, inclusive of defence costs.

(ii) If the Professional Liability insurance is written on a claims-made basis, coverage must be in place for a period of at least 12 months after the completion or termination of the Contract.

(iii) The following endorsement must be included:

Notice of Cancellation: The Insurer will endeavour to provide the Contracting Authority thirty (30) days written notice of cancellation.

7.18 Limitation of Liability - Information Management/Information Technology

(a) This section applies despite any other provision of the Contract and replaces the section of the general conditions entitled "Liability". Any reference in this section to damages caused by the Contractor also includes damages caused by its employees, as well as its subcontractors, agents, and representatives, and any of their employees. This section applies regardless of whether the claim is based in contract, tort, or another cause of action. The Contractor is not liable to Canada with respect to the performance of or failure to perform the Contract, except as described in this section and in any section of the Contract pre-establishing any liquidated damages. The Contractor is only liable for indirect, special or consequential damages to the extent described in this Article, even if it has been made aware of the potential for those damages.

(b) **First Party Liability**:

(i) The Contractor is fully liable for all damages to Canada, including indirect, special or consequential damages, caused by the Contractor's performance or failure to perform the Contract that relate to:

(A) any infringement of intellectual property rights to the extent the Contractor breaches the section of the General Conditions entitled "Intellectual Property Infringement and Royalties";

(B) physical injury, including death.

(ii) The Contractor is liable for all direct damages caused by the Contractor's performance or failure to perform the Contract affecting real or tangible personal property owned, possessed, or occupied by Canada.

(iii) Each of the Parties is liable for all direct damages resulting from any breach of confidentiality under the Contract. Each of the Parties is also liable for all indirect, special or consequential damages in respect of any unauthorized disclosure of the other Party's trade secrets (or trade secrets of a third party provided by one Party to another under the Contract) relating to information technology.

(iv) The Contractor is liable for all direct damages relating to any encumbrance or claim relating to any portion of the Work for which Canada has made any payment. This does not apply to encumbrances or claims relating to intellectual property rights, which are addressed under (i)(A) above.

(v) The Contractor is also liable for any other direct damages to Canada caused by the Contractor's performance or failure to perform the Contract that relate to:

(A) any breach of the warranty obligations under the Contract, up to the total amount paid by Canada (including any applicable taxes) for the goods and services affected by the breach of warranty; and

(B) Any other direct damages, including all identifiable direct costs to Canada associated with re-procuring the Work from another party if the Contract is terminated either in whole or in part for default, up to an aggregate maximum for this subparagraph (B) of the greater of .75 times the total estimated cost (meaning the dollar amount shown on the first page of the Contract in the cell titled "Total Estimated Cost" or shown on each call-up, purchase order or other document used to order goods or services under this instrument), or $1,000,000.00.

In any case, the total liability of the Contractor under subparagraph (v) will not exceed the total estimated cost (as defined above) for the Contract or $1,000,000.00, whichever is more.

(vi) If Canada's records or data are harmed as a result of the Contractor's negligence or willful act, the Contractor's only liability is, at the Contractor's own expense, to restore Canada's records and data using the most recent back-up kept by Canada. Canada is responsible for maintaining an adequate back-up of its records and data.

(c) **Third Party Claims**:

(i) Regardless of whether a third party makes its claim against Canada or the Contractor, each Party agrees that it is liable for any damages that it causes to any third party in connection with the Contract as set out in a settlement agreement or as finally determined by a court of competent jurisdiction, where the court determines that the Parties are jointly and severally liable or that one Party is solely and directly liable to the third party. The amount of the liability will be the amount set out in the settlement agreement or determined by the court to have been the Party's portion of the damages to the third party. No settlement agreement is binding on a Party unless its authorized representative has approved the agreement in writing.

(ii) If Canada is required, as a result of joint and several liability or joint and solidarily liable, to pay a third party in respect of damages caused by the Contractor, the Contractor must reimburse Canada by the amount finally determined by a court of competent jurisdiction to be the Contractor's portion of the damages to the third party. However, despite Sub-article (i), with respect to special, indirect, and consequential damages of third parties covered by this Section, the Contractor is only liable for reimbursing Canada for the Contractor's portion of those damages that Canada is required by a court to pay to a third party as a result of joint and several liability that relate to the infringement of a third party's intellectual property rights; physical injury of a third party, including death; damages affecting a third party's real or tangible personal property; liens or encumbrances on any portion of the Work; or breach of confidentiality.

(iii) The Parties are only liable to one another for damages to third parties to the extent described in this Sub-article (c).

7.19 Joint Venture Contractor

(a) The Contractor confirms that the name of the joint venture is _____ and that it is comprised of the following members:

(b) With respect to the relationship among the members of the joint venture Contractor, each member agrees, represents and warrants (as applicable) that:

(i) _____ has been appointed as the "representative member" of the joint venture Contractor and has fully authority to act as agent for each member regarding all matters relating to the Contract;

(ii) by giving notice to the representative member, Canada will be considered to have given notice to all the members of the joint venture Contractor; and

(iii) all payments made by Canada to the representative member will act as a release by all the members.

(c) All the members agree that Canada may terminate the Contract in its discretion if there is a dispute among the members that, in Canada's opinion, affects the performance of the Work in any way.

(d) All the members are jointly and severally or solidarily liable for the performance of the entire Contract.

(e) The Contractor acknowledges that any change in the membership of the joint venture (i.e., a change in the number of members or the substitution of another legal entity for an existing member) constitutes an assignment and is subject to the assignment provisions of the General Conditions.

(f) The Contractor acknowledges that all security and controlled goods requirements in the Contract, if any, apply to each member of the joint venture Contractor.

Note to Bidders: *This Article will be deleted if the Bidder awarded the contract is not a joint venture. If the contractor is a joint venture, this clause will be completed with information provided in its bid.*

7.20 Professional Services - General

(a) The Contractor must provide professional services on request as specified in this Contract. All resources provided by the Contractor must meet the qualifications described in the Contract (including those relating to previous experience, professional designation, education, language proficiency and security clearance) and must be competent to provide the required services by any delivery dates described in the Contract.

(b) If the Contractor fails to deliver any deliverable (excluding delivery of a specific individual) or complete any task described in the Contract on time, in addition to any other rights or remedies available to Canada under the Contract or the law, Canada may notify the Contractor of the deficiency, in which case the Contractor must submit a written plan to the Technical Authority within ten working days detailing the actions that the Contractor will undertake to remedy the deficiency. The Contractor must prepare and implement the plan at its own expense.

(c) In General Conditions 2035, the Article titled "Replacement of Specific Individuals" is deleted and the following applies instead:

Replacement of Specific Individuals

(i) If the Contractor is unable to provide the services of any specific individual identified in the Contract to perform the services, the Contractor must within five working days of having this knowledge, the individual's departure or failure to commence Work (or, if Canada has requested the replacement, within ten working days of Canada's notice of the requirement for a replacement) provide to the Contracting Authority:

(A) the name, qualifications and experience of a proposed replacement immediately available for Work; and

(B) security information on the proposed replacement as specified by Canada, if applicable.

The replacement must have qualifications and experience that meet or exceed those obtained for the original resource.

(ii) Subject to an Excusable Delay, where Canada becomes aware that a specific individual identified under the Contract to provide services has not been provided or is not performing, the Contracting Authority may elect to:

(A) exercise Canada's rights or remedies under the Contract or at law, including terminating the Contract in whole or in part for default under the Article titled "Default of the Contractor", or

(B) assess the information provided under (c) (i) above or, if it has not yet been provided, require the Contractor to propose a replacement to be rated by the Technical Authority. The replacement must have qualifications and experience that are similar or exceed those obtained for the original resource and be acceptable to Canada. Upon assessment of the replacement, Canada may accept the replacement, exercise the rights in (ii) (A) above, or require another replacement in accordance with this sub-article (c).

Where an Excusable Delay applies, Canada may require (c) (ii) (B) above instead of terminating under the "Excusable Delay" Article. An Excusable Delay does not include resource unavailability due to allocation of the resource to another Contract or project (including those for the Crown) being performed by the Contractor or any of its affiliates.

(iii) The Contractor must not, in any event, allow performance of the Work by unauthorized replacement persons. The Contracting Authority may order that an original or replacement resource stop performing the Work. In such a case, the Contractor must immediately comply with the order. The fact that the Contracting Authority does not order a resource to stop performing the Work does not relieve the Contractor from its responsibility to meet the requirements of the Contract.

(iv) The obligations in this article apply despite any changes that Canada may have made to the Client's operating environment.

7.21 Safeguarding Electronic Media

(a) Before using them on Canada's equipment or sending them to Canada, the Contractor must use a regularly updated product to scan electronically all electronic media used to perform the Work for computer viruses and other coding intended to cause malfunctions. The Contractor must notify Canada if any electronic media used for the Work are found to contain computer viruses or other coding intended to cause malfunctions.

(b) If magnetically recorded information or documentation is damaged or lost while in the Contractor's care or at any time before it is delivered to Canada in accordance with the Contract, including accidental erasure, the Contractor must immediately replace it at its own expense.

7.22 Representations and Warranties

The Contractor made statements regarding its own and its proposed resources' experience and expertise in its bid that resulted in the award of the Contract and the issuance of TA's. The Contractor represents and warrants that all those statements are true and acknowledges that Canada relied on those statements in awarding the Contract and adding work to it through TA's. The Contractor also represents and warrants that it has, and all its resources and subcontractors that perform the Work have, and at all times during the Contract Period they will have and maintain, the skills, qualifications, expertise and experience necessary to perform and manage the Work in accordance with the Contract, and that the Contractor (and any resources or subcontractors it uses) has previously performed similar services for other customers.

7.23 Access to Canada's Property and Facilities

Canada's property, facilities, equipment, documentation, and personnel are not automatically available to the Contractor. If the Contractor would like access to any of these, it is responsible for making a request to the Technical Authority. Unless expressly stated in the Contract, Canada has no obligation to provide any of these to the Contractor. If Canada chooses, in its discretion, to make its property, facilities, equipment, documentation or personnel available to the Contractor to perform the Work, Canada may require an adjustment to the Basis of Payment and additional security requirements may apply.

7.24 Identification Protocol Responsibilities

The Contractor will be responsible for ensuring that each of its agents, representatives or subcontractors (hereinafter referred to as Contractor Representatives) complies with the following self-identification requirements:

(a) Contractor Representatives who attend a Government of Canada meeting (whether internal or external to Canada's offices) must identify themselves as Contractor Representatives prior to the commencement of the meeting, to ensure that each meeting participant is aware of the fact that the individual is not an employee of the Government of Canada;

(b) During the performance of any Work at a Government of Canada site, each Contractor Representative must be clearly identified at all times as being a Contractor Representative; and

(c) If a Contractor Representative requires the use of the Government of Canada's e-mail system in the performance of the Work, then the individual must clearly identify him or herself as an agent or subcontractor of the Contractor in all electronic mail in the signature block as well as under "Properties." This identification protocol must also be used in all other correspondence, communication, and documentation.

(d) If Canada determines that the Contractor is in breach of any obligation stated in this Article, upon written notice from Canada the Contractor must submit a written action plan describing corrective measures it will implement to eliminate the recurrence of the problem. The Contractor will have five working days to deliver the action plan to the Client and the Contracting Authority, and twenty working days to rectify the underlying problem.

(e) In addition to any other rights it has under the Contract, Canada may terminate the Contract for default if the corrective measures required of the Contractor described above are not met.

ANNEX A

STATEMENT OF WORK

Attached hereto.

APPENDIX A TO ANNEX A

SERVICE DOMAIN: JUS SERVICE DESK SERVICE

Attached hereto.

APPENDIX B TO ANNEX A

SERVICE DOMAIN: JUS ON-SITE SUPPORT SERVICE

Attached hereto.

APPENDIX C TO ANNEX A

SERVICE DOMAIN: JUS ENGINEERING SERVICE

Attached hereto.

APPENDIX D TO ANNEX A
SECURITY REQUIREMENTS

Attached hereto.

APPENDIX E TO ANNEX A
DEFINITIONS

Attached hereto.

APPENDIX F TO ANNEX A
STANDARD HARDWARE AND SOFTWARE

Attached hereto.

APPENDIX G TO ANNEX A

TASKING ASSESSMENT PROCEDURE

1. Where a requirement for a specific task is identified, a draft Task Authorization Form (TA Form) as attached at Appendix H to Annex A will be provided to the Contractor. Once a draft TA Form is received, the Contractor must submit to the Technical Authority a quotation of rates to supply the requested Resource Categories based on the information identified in the TA Form. The quotation must be signed and submitted to Canada within the time for response identified in the TA Form. The Contractor will be given a minimum of 48 hours turnaround time to submit a quotation.

2. For each proposed resource the Contractor must supply a résumé, the requested security clearance information and must complete the Response Tables at Appendix I of Annex A applicable to the Resource Categories identified in the draft TA. The same individual must not be proposed for more than one Resource Category. The résumés must demonstrate that each proposed individual meets the qualification requirements described (including any educational requirements, work experience requirements, and professional designation or membership requirements). With respect to the proposed resources:

   (i) Proposed resources may be employees of the Contractor or employees of a subcontractor, or these individuals may be independent contractors to whom the Contractor would subcontract a portion of the Work. (Refer to Appendix J to Annex A, Certifications).

   (ii) For educational requirements for a particular degree, designation or certificate, Canada will only consider educational programmes that were successfully completed by the resource before the date the draft TA was first issued to the Contractor.

   (iii) For requirements relating to professional designation or membership, the resource must have the required designation or membership by the time of draft TA issuance and must continue, where applicable, to be a member in good standing of the profession or membership throughout the assessment period and Contract Period. Where the designation or membership must be demonstrated through a certification, diploma or degree, such document must be current, valid and issued by the entity specified in this Contract or if the entity is not specified, the issuer must have been an accredited or otherwise recognized body, institution or entity at the time the document was issued.

   (iv) For work experience, Canada will not consider experience gained as part of an educational programme, except for experience gained through a formal co-operative programme at a post-secondary institution.

   (v) For any requirements that specify a particular time period (e.g., 2 years) of work experience, Canada will disregard any information about experience if the résumé does not include the relevant dates (month and year) for the experience claimed (i.e., the start date and end date). Canada will evaluate only the duration that the resource actually worked on a project or projects (from his or her start date to end date), instead of the overall start and end date of a project or a combination of projects in which a resource has participated.

   (vi) A résumé must not simply indicate the title of the individual's position, but must demonstrate that the resource has the required work experience by explaining the responsibilities and work performed by the individual while in that position. Only listing experience without providing any supporting data to describe responsibilities, duties and relevance to the requirement, or reusing the same wording as the TA Form, will not be considered "demonstrated" for the purposes of the assessment. The Contractor should provide complete details as to where, when, month and year, and how, through which activities/responsibilities, the stated qualifications / experience were obtained. In situations in which a proposed resource worked at the same time on more than one

project, the duration of any overlapping time period will be counted only once toward any requirements that relate to the individual's length of experience.

3. The qualifications and experience of the proposed resources will be assessed against the requirements set out in Appendix I to Annex A to determine each proposed resource's compliance with the mandatory and rated criteria. Canada may request proof of successful completion of formal training, as well as reference information. Canada may conduct reference checks to verify the accuracy of the information provided. If reference checks are done, they will be conducted in writing by e-mail (unless the contact at the reference is only available by telephone). Canada will not assess any points or consider a mandatory criterion met unless the response is received within 5 working days. On the third working day after sending out the e-mails, if Canada has not received a response, Canada will notify the Contractor by e-mail, to allow the Contractor to contact its reference directly to ensure that it responds to Canada within 5 working days. Wherever information provided by a reference differs from the information supplied by the Contractor, the information supplied by the reference will be the information assessed. Points will not be allocated or a mandatory criteria considered as met if the reference customer is not a customer of the Contractor itself (for example, the customer cannot be the customer of an affiliate of the Contractor). Nor will points be allocated or a mandatory criteria considered as met if the customer is itself an affiliate or other entity that does not deal at arm's length with the Contractor. Crown references will be accepted.

4. During the assessment of the resources proposed, should the references for two or more resources required under that TA either be unavailable or fail to substantiate the required qualifications of the proposed resources to perform the required services, the Contracting Authority may find the quotation to be non-responsive.

5. Only quotations that meet all of the mandatory criteria will be considered for assessment of the point rated criteria. Each resource proposed must attain the required minimum score for the point rated criteria for the applicable Resource Category. If the minimum score for any proposed resource is less than what is required, the Contractor's quotation will be found to be non-responsive.

6. Once the quotation has been accepted by the Technical Authority, the TA Form will be signed by Canada and provided to the Contractor for signature. The TA Form must be appropriately signed by Canada prior to commencement of any work. The Contractor must not commence work until a validly issued TA Form (the Task Authorization) has been received, and any work performed in its absence is done at the Contractor's own risk.

APPENDIX H TO ANNEX A
TASK AUTHORIZATION FORM

Attached hereto.

APPENDIX I TO ANNEX A

RESOURCES ASSESSMENT CRITERIA AND RESPONSE TABLE

To facilitate resource assessment, the Contractor must prepare and submit a response to a draft Task Authorization using the tables provided in this Appendix. When completing the resource grids, the specific information which demonstrates the requested criteria and reference to the page number of the résumé should be incorporated so that Canada can verify this information. The tables should not contain all the project information from the resume. Only the specific answer should be provided.

1.0 Mandatory Resource Assessment Criteria:

Criteria ID	Requirement	Contractor's Response
M1	**Project Manager** The Contractor must demonstrate that its proposed Project Manager has: (a) a minimum of 5 years of experience managing IT projects; and (b) one of the following project management certifications: (i) Project management professional PMP (Project Management Institute (PMI)) (ii) Certified associate in project management CAPM (PMI) (iii) CompTIA Project+ (iv) Master Project Manager MPM (American Academy of Project Management) (v) Certified Project Manager CPM (International Association of Project and Program Management) (vi) Project Management in IT Security PMITS (EC-Council) (vii) Associate in Project Management APM (Global Association for Quality Management (GAQM)) (viii) Professional in Project Management PPM (GAQM) (ix) Certified Project Director (GAQM) The Contractor must provide a copy of each certification.	
M2	**Technology Architect** The Contractor must demonstrate that its proposed Technology Architect has a minimum of 5 years of experience architecting solutions in the Help Desk and Support domain.	

M3	**Security Specialist** The Contractor must demonstrate that its proposed Security Specialist has a minimum of 5 years of experience performing the following tasks: (a) Conducting security threat and risk assessments; and (b) Developing and enforcing IT security policies, standards, guidelines and procedures on the security aspects of IT facilities and application systems. **Note to the Contractor:** the minimum 5 years of experience is a cumulative total of the experience performing all tasks (e.g. 2 years of experience performing (a) and 3 years of experience performing (b) meets the minimum 5 years of experience).	
M4	**Business Analyst** The Contractor must demonstrate that its proposed Business Analyst has a minimum of 5 years of experience analyzing business requirements in IT projects.	
M5	**On-Site Service Representative** The Contractor must demonstrate that its proposed On-Site Service Representative has a degree, diploma or certificate in a relevant field of study. The Contractor must provide a copy of each degree, diploma or certificate.	
M6	**On-Site Service Representative** The Contractor must certify that its proposed On-Site Service Representative has the following qualifications: (a) Fluent* in English and French; (b) Thorough knowledge of Help Desk and Support hardware (PC assembly, PC components) and Help Desk and Support software; and (c) Strong customer service and communication skills (both verbal and written). *To be considered fluent, the proposed resource must be able to communicate orally and in writing in English and in French without any assistance and with minimal errors.	

M7	**On-Site Service Team Lead** The Contractor must demonstrate that its proposed On-Site Service Team Lead has: (a) successfully completed a relevant training program from a recognized institution (e.g. relevant program at a community college); and (b) a minimum of 5 years of experience in a similar role. The Contractor must provide a copy of each degree, diploma or certificate.	
M8	**On-Site Service Team Lead** The Contractor must certify that its proposed On-Site Service Team Lead has the following qualifications: (i) Fluent* in English and French; and (ii) Strong customer service and communication skills (both verbal and written). *To be considered fluent, the proposed resource must be able to communicate orally and in writing in English and in French without any assistance and with minimal errors.	
M9	**Implementation Project Manager** The Contractor must demonstrate that its proposed Implementation Project Manager has: (a) a minimum of 5 years of experience managing IT projects; (b) one of the following project management certifications: (i) Project management professional PMP (Project Management Institute (PMI)) (ii) Certified associate in project management CAPM (PMI) (iii) CompTIA Project+ (iv) Master Project Manager MPM (American Academy of Project Management) (v) Certified Project Manager CPM (International Association of Project and Program Management) (vi) Project Management in IT Security PMITS (EC-Council) (vii) Associate in Project Management APM (Global Association for Quality Management (GAQM))	

	(viii) Professional in Project Management PPM (GAQM) (ix) Certified Project Director (GAQM) The Contractor must provide a copy of each certification.	
M10	**Solution Architect** The Contractor must demonstrate that its proposed Solution Architect has a minimum of 5 years of experience architecting solutions in the Help Desk and Support domain.	
M11	**Security Architect** The Contractor must demonstrate that its proposed Security Specialist has a minimum of 5 years of experience performing the following tasks: (a) Conducting security threat and risk assessments; and (b) Developing and enforcing IT security policies, standards, guidelines and procedures on the security aspects of IT facilities and application systems. **Note to the Contractor:** the minimum 5 years of experience is a cumulative total of the experience performing all tasks (e.g. 2 years of experience performing (a) and 3 years of experience performing (b) meets the minimum 5 years of experience).	
M12	**Security Architect** The Contractor must demonstrate that its proposed Security Architect has a certification from an internationally recognized security professionals organization (e.g. International Information Systems Security Certification Consortium (ISC)^2). The Contractor must provide a copy of each certification.	
M13	**Service Manager** The Contractor must demonstrate that its proposed Service Manager has a minimum of 5 years of experience in a similar role in the Help Desk and Support domain.	

2.0 Point Rated Resource Assessment Criteria:

(a) Implementation Project Manager

Criteria ID	Requirement	Point Allocation Scheme	Contractor's Response
R1	The Contractor should demonstrates that its proposed Implementation Project Manager has experience being the lead project manager on projects implementing Help Desk Support services. Each project referenced by the Contractor must have been in support of a minimum of 2,500 users and included one of the following services: (a) Service Desk Support; (b) On-Site and Break/Fix Support; or (c) Desktop Engineering Support. **Note to the Contractor:** internal projects within the Contractor's organization are accepted.	Points will be awarded in accordance with the following: a) 5 points per project, up to a maximum of 3 projects; b) 5 points if one of the projects included all services (i.e. Service Desk, On-Site and Break/Fix, and Desktop Engineering Support services); and c) 5 points if one of the projects was for a Canadian public sector organization. **Maximum Points = 25**	
		Required Minimum Score	**15**

(b) Solution Architect

R2	The Contractor should demonstrates that its proposed Solution Architect has experience being the lead solution architect on projects implementing Help Desk Support services. Each project referenced by the Contractor must have been in support of a minimum of 2,500 users and included one of the following services: (a) Service Desk Support; (b) On-Site and Break/Fix Support; or	Points will be awarded in accordance with the following: a) 5 points per project, up to a maximum of 3 projects; b) 5 points if one of the projects included all services (i.e. Service Desk, On-Site and Break/Fix, and Desktop Engineering Support services); and c) 5 points if one of the projects was for a Canadian public sector organization.	

	(c) Desktop Engineering Support. **Note to the Contractor:** internal projects within the Contractor's organization are accepted.	**Maximum Points = 25**	
		Required Minimum Score	**15**

(c) Security Architect

R3	The Contractor should demonstrates that its proposed Security Architect has experience being the lead security architect on projects implementing Help Desk Support services. Each project referenced by the Contractor must have been in support of a minimum of 2,500 users and included one of the following services: (a) Service Desk Support; (b) On-Site and Break/Fix Support; or (c) Desktop Engineering Support. **Note to the Contractor:** internal projects within the Contractor's organization are accepted.	Points will be awarded in accordance with the following: a) 5 points per project, up to a maximum of 3 projects; b) 5 points if one of the projects included all services (i.e. Service Desk, On-Site and Break/Fix, and Desktop Engineering Support services); and c) 5 points if one of the projects was for a Canadian public sector organization. **Maximum Points = 25**	
		Required Minimum Score	**15**

(d) Service Manager

Criteria ID	Requirement	Point Allocation Scheme	Contractor's Response

R4	The Contractor should demonstrates that its proposed Service Manager has experience being the lead service manager on projects implementing Help Desk Support services. Each project referenced by the Contractor must have been in support of a minimum of 2,500 users and included one of the following services: (a) Service Desk Support; (b) On-Site and Break/Fix Support; or (c) Desktop Engineering Support. **Note to the Contractor:** internal projects within the Contractor's organization are accepted.	Points will be awarded in accordance with the following: a) 5 points per project, up to a maximum of 3 projects; b) 5 points if one of the projects included all services (i.e. Service Desk, On-Site and Break/Fix, and Desktop Engineering Support services); and c) 5 points if one of the projects was for a Canadian public sector organization. **Maximum Points = 25**	
		Required Minimum Score	**15**

APPENDIX J TO ANNEX A

CERTIFICATIONS AT THE TA STAGE

The following Certifications are to be used, as applicable. If they apply, they must be signed and attached to the Contractor's quotation when it is submitted to Canada.

1. CERTIFICATION OF EDUCATION AND EXPERIENCE

The Contractor certifies that all the information provided in the résumés and supporting material proposed for completing the subject work, particularly the information pertaining to education, achievements, experience and work history, has been verified by the Contractor to be true and accurate. Furthermore, the Contractor warrants that every individual proposed by the Contractor for the requirement is capable of performing the Work described in the Task Authorization.

_____ _____

Print name of authorized individual & sign above Date

2. CERTIFICATION OF AVAILABILITY OF PERSONNEL

The Contractor certifies that, should it be authorized to provide services under this Task Authorization, the persons proposed in the quotation will be available to commence performance of the work within a reasonable time from the date of issuance of the valid Task Authorization, or within the time specified in the TA Form, and will remain available to perform the work in relation to the fulfillment of the requirement.

_____ _____

Print name of authorized individual & sign above Date

3. CERTIFICATION OF STATUS OF PERSONNEL

If the Contractor has proposed any individual who is not an employee of the Contractor, the Contractor certifies that it has permission from that individual to propose his/her services in relation to the Work to be performed under this TA and to submit his/her résumé to Canada. At any time during the Contract Period the Contractor must, upon request from the Contracting Authority, provide the written confirmation, signed by the individual, of the permission that was given to the Contractor of his/her availability. Failure to comply with the request may result in a default under the Contract in accordance with the General Conditions.

_____ _____

Print name of authorized individual & sign above Date

ANNEX B

BASIS OF PAYMENT

1. Service Desk Services

	Service Desk Services - Core Service for Justice Canada (SCI:SDS-Base) Per user price for up to 7,499 users	**Service Desk Services - Core Service for Justice Canada (SCI:SDS-7500)** Per user price for 7,500 to 9,999 users
Firm Per User Monthly Price – Initial Contract Period (4 years)	$	$
Firm Per User Monthly Price – Option Period 1 (1 year)	$	$
Firm Per User Monthly Price – Option Period 2 (1 year)	$	$

2. On-Site Support and Break/Fix Services

	On-site Support and Break/Fix Services - Core Service for Justice Canada in the National Capital Region (SCI:OSS-Base) Price includes support for all devices (audio-visual devices, laptops, desktops, tablets, printers, and peripherals)
Firm Per User Monthly Price – Initial Contract Period (4 years)	$
Firm Per User Monthly Price – Option Period 1 (1 year)	$
Firm Per User Monthly Price – Option Period 2 (1 year)	$

3. Engineering Support Services

	Engineering and Support Services - Core Service for Justice Canada (SCI:WES) For all Justice Canada users, End User Devices and Printers. Cost includes overall systems integrator role.
Firm Monthly Price – Initial Contract Period (4 years)	$
Firm Monthly Price – Option Period 1 (1 year)	$
Firm Monthly Price – Option Period 2 (1 year)	$

4. Professional Services

Task Authorization Portion - Labour Rates (for additional work on an as and when requested basis)

	Project Manager	Solution Architect	Security Architect	Business Analyst	On-Site Services Team Leader	On-Site Services Representative
Firm Per Diem Rate – Initial Contract Period (4 years)	$	$	$	$	$	$
Firm Per Diem Rate – Option Period 1 (1 year)	$	$	$	$	$	$
Firm Per Diem Rate – Option Period 2 (1 year)	$	$	$	$	$	$

5. Replacement Parts

The Contractor will be paid the Laid Down Cost* plus the following firm mark-up rate.

	The firm percentage (%) mark-up for replacement parts directly associated with the provision of Hardware Break/Fix Services (SCI:PartsHandling)
Firm Percentage Mark-up for Replacement Parts – Initial Contract Period (4 years)	$
Firm Percentage Mark-up for Replacement Parts – Option Period 1 (1 year)	$
Firm Percentage Mark-up for Replacement Parts – Option Period 2 (1 years)	$

*Laid Down Cost is defined as the cost incurred by the Contractor to acquire the parts for resale to Canada. This includes the supplier invoice price less trade discount plus any applicable charges for transportation, foreign exchange, customs duties and brokerage charges, but exclude Applicable Taxes.

ANNEX C

SECURITY REQUIREMENTS CHECK LIST

Attached hereto.

ATTACHMENT 1
CURRENT STATE INFORMATION

Attached hereto.

ATTACHMENT 2

BID SUBMISSION FORM

BID SUBMISSION FORM		
Bidder's full legal name		
Authorized Representative of Bidder for evaluation purposes (e.g., clarifications)	Name	
	Title	
	Address	
	Telephone #	
	Fax #	
	Email	
Bidder's Procurement Business Number (PBN) [see the Standard Instructions 2003] **[Note to Bidders: Please ensure that the PBN you provide matches the legal name under which you have submitted your bid. If it does not, the Bidder will be determined based on the legal name provided, not based on the PBN, and the Bidder will be required to submit the PBN that matches the legal name of the Bidder.]**		
Jurisdiction of Contract: Province or territory in Canada the Bidder wishes to be the legal jurisdiction applicable to any resulting contract (if other than as specified in solicitation)		
Bidder's Proposed Site(s) or Premises Requiring Safeguard Measures. See Part 3 for instructions.	Address of proposed site or premise: _____ City: _____ Province: _____ Postal Code: _____ Country: _____	
Former Public Servants See the Article in Part 2 of the bid solicitation entitled Former Public Servant for a definition of "Former Public Servant".	Is the Bidder a FPS in receipt of a pension as defined in the bid solicitation? Yes ____ No ____ If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	
	Is the Bidder a FPS who received a lump sum payment under the terms of the Work Force Adjustment Directive? Yes ____ No ____	

	If yes, provide the information required by the Article in Part 2 entitled "Former Public Servant"	
Security Clearance Level of Bidder [include both the level and the date it was granted] **[Note to Bidders: Please ensure that the security clearance matches the legal name of the Bidder. If it does not, the security clearance is not valid for the Bidder.]**		
On behalf of the Bidder, by signing below, I confirm that I have read the entire bid solicitation including the documents incorporated by reference into the bid solicitation and I certify that: 1. The Bidder considers itself and its proposed resources able to meet all the mandatory requirements described in the bid solicitation; 2. This bid is valid for the period requested in the bid solicitation; 3. All the information provided in the bid is complete, true and accurate; and 4. If the Bidder is awarded a contract, it will accept all the terms and conditions set out in the resulting contract clauses included in the bid solicitation.		
Signature of Authorized Representative of Bidder		

ATTACHMENT 3
MANDATORY BID EVALUATION CRITERIA

Attached hereto.

ATTACHMENT 4
POINT-RATED BID EVALUATION CRITERIA

Attached hereto.

ATTACHMENT 5

PRICING SCHEDULE

In respect of the "Estimated" data listed below (rows D, E, M, N, U, BB, CC, KK and LL), the estimated information is for evaluation purposes only during the solicitation process and does not represent a commitment of the future usage.

1. Service Desk Services

	Service Desk Services - Core Service for Justice Canada (SCI:SDS-Base) Per user price for up to 7,499 users	**Service Desk Services- Core Service for Justice Canada (SCI:SDS-7500)** Per user price for 7,500 to 9,999 users
Firm Per User Monthly Price (A) – Initial Contract Period (4 years)	$	$
Firm Per User Monthly Price (B) – Option Period 1 (1 year)	$	$
Firm Per User Monthly Price (C) – Option Period 2 (1 year)	$	$
Estimated Number of users (D)	4,000	7,500
Estimated Number of Months (E)	60	60
Extended Amount (F) = ((A)+(B)+(C)) X (D) x (E)	$	$
Weighting Factor (G)	0.20	0.05
Evaluated Price (H) = (F) x (G)	(1)$	(2)$
Total Evaluated Price for Service Desk Services (I) = ((1)$ + (2)$)	$	

2. On-Site Support and Break/Fix Services

	On-site Support and Break/Fix Services - Core Service for Justice Canada in the National Capital Region (SCI:OSS-Base) Cost includes support for all devices (audio-visual devices, laptops, desktops, tablets, printers, and peripherals)
Firm Per User Monthly Price (J) – Initial Contract Period (4 years)	$
Firm Per User Monthly Price (K) – Option Period 1 (1 year)	$
Firm Per User Monthly Price (L) – Option Period 2 (1 year)	$

Estimated Number of users (M)	2,200
Estimated Number of Months (N)	60
Extended Amount (O) = ((J)+(K)+(L)) X (M) x (N)	$
Weighting Factor (P)	0.20
Total Evaluated Price for On-Site Support and Break/Fix Services (Q) = (O) x (P)	$

3. Engineering Support Services

	Engineering and Support Services - Core Service for Justice Canada (SCI:WES) For all Justice Canada users, End User Devices and Printers. Price includes overall systems integrator role.
Firm Monthly Price (R) – Initial Contract Period (4 years)	$
Firm Monthly Price (S) – Option Period 1 (1 year)	$
Firm Monthly Price (T) – Option Period 2 (1 year)	$
Estimated Number of Months (U)	60
Extended Amount (V) = ((R)+(S)+(T)) X (U)	$
Weighting Factor (W)	0.14
Total Evaluated Price for Engineering Support Services (X) = (V) x (W)	$

4. Professional Services

Task Authorization Portion - Labour Rates (for additional work on an as and when requested basis)

	Project Manager	Solution Architect	Security Architect	Business Analyst	On-Site Services Team Leader	On-Site Services Representative
Firm Per Diem Rate (Y) – Initial Contract Period (4 years)	$	$	$	$	$	$
Firm Per Diem Rate (Z) –	$	$	$	$	$	$

Option Period 1 (1 year)						
Firm Per Diem Rate (AA) – Option Period 2 (1 year)	$	$	$	$	$	$
Estimated Level of Effort Per Year in Days (BB)	100	50	100	50	100	100
Estimated Number of Years (CC)	5	5	5	5	5	5
Extended Amount (DD) = ((Y)+(Z)+(AA)) X (BB) x (CC)	$	$	$	$	$	$
Weighting Factor (EE)	0.01	0.005	0.01	0.005	0.01	0.01
Evaluated Price (FF) = (DD) x (EE)	(3)$	(4)$	(5)$	(6)$	(7)$	(8)$
Total Evaluated Price for Professional Services (GG) = (3)$+(4)$ +(5)$ +(6)$ +(7)$ +(8)$	$					

5. Replacement Parts

	The firm percentage (%) mark-up for replacement parts directly associated with the provision of Hardware Break/Fix Services (SCI:PartsHandling)
Firm Percentage Mark-up for Replacement Parts (HH) – Initial Contract Period (4 years)	$
Firm Percentage Mark-up for Replacement Parts (II) – Option Period 1 (1 year)	$
Firm Percentage Mark-up for Replacement Parts (JJ) – Option Period 2 (1 years)	$

Estimated Annual Cost of Replacement Parts (KK)	$25,000.00
Estimated Number of Years (LL)	5
Extended Amount (MM) = ((HH)+(II)+(JJ)) x (KK) x (LL)	$
Weighting Factor (NN)	0.01
Total Evaluated Price for Replacement Parts (OO) = (MM) x (NN)	$

6. Total Bid Price

Total Evaluated Price for Service Desk Services (I)	$
Total Evaluated Price for On-Site Support and Break/Fix Services (Q)	$
Total Evaluated Price for Engineering Support Services (X)	$
Total Evaluated Price for Professional Services (GG)	$
Total Evaluated Price for Replacement Parts (OO)	$
Bidder's Total Bid Price	$

ATTACHMENT 6

FEDERAL CONTRACTORS PROGRAM FOR EMPLOYMENT EQUITY - CERTIFICATION

I, the Bidder, by submitting the present information to the Contracting Authority, certify that the information provided is true as of the date indicated below. The certifications provided to Canada are subject to verification at all times. I understand that Canada will declare a bid non-responsive, or will declare a contractor in default, if a certification is found to be untrue, whether during the bid evaluation period or during the contract period. Canada will have the right to ask for additional information to verify the Bidder's certifications. Failure to comply with any request or requirement imposed by Canada may render the bid non-responsive or constitute a default under the Contract.

For further information on the Federal Contractors Program for Employment Equity visit Employment and Social Development Canada (ESDC) - Labour's website.

Date:_____ (YYYY/MM/DD) (If left blank, the date will be deemed to be the bid solicitation closing date.)

Complete both A and B.

A. Check only one of the following:

( ) A1. The Bidder certifies having no work force in Canada.

( ) A2. The Bidder certifies being a public sector employer.

( ) A3. The Bidder certifies being a federally regulated employer being subject to the Employment Equity Act.

( ) A4. The Bidder certifies having a combined work force in Canada of less than 100 employees (combined work force includes: permanent full-time, permanent part-time and temporary employees [temporary employees only includes those who have worked 12 weeks or more during a calendar year and who are not full-time students]).

A5. The Bidder has a combined workforce in Canada of 100 or more employees; and

( ) A5.1 The Bidder certifies already having a valid and current Agreement to Implement Employment Equity (AIEE) in place with ESDC-Labour.

OR

( ) A5.2 The Bidder certifies having submitted the Agreement to Implement Employment Equity (LAB1168) to ESDC-Labour. As this is a condition to contract award, proceed to completing the form Agreement to Implement Employment Equity (LAB1168), duly signing it, and transmit it to ESDC-Labour.

B. Check only one of the following:

( ) B1. The Bidder is not a Joint Venture.

OR

( ) B2. The Bidder is a Joint venture and each member of the Joint Venture must provide the Contracting Authority with a completed annex Federal Contractors Program for Employment Equity - Certification. (Refer to the Joint Venture section of the Standard Instructions).

Department of Justice Canada
Help Desk and Support Services

Annex A: Statement of Work General

Table of Contents

INDEX OF TABLES

Index of Figures

1 INTRODUCTION

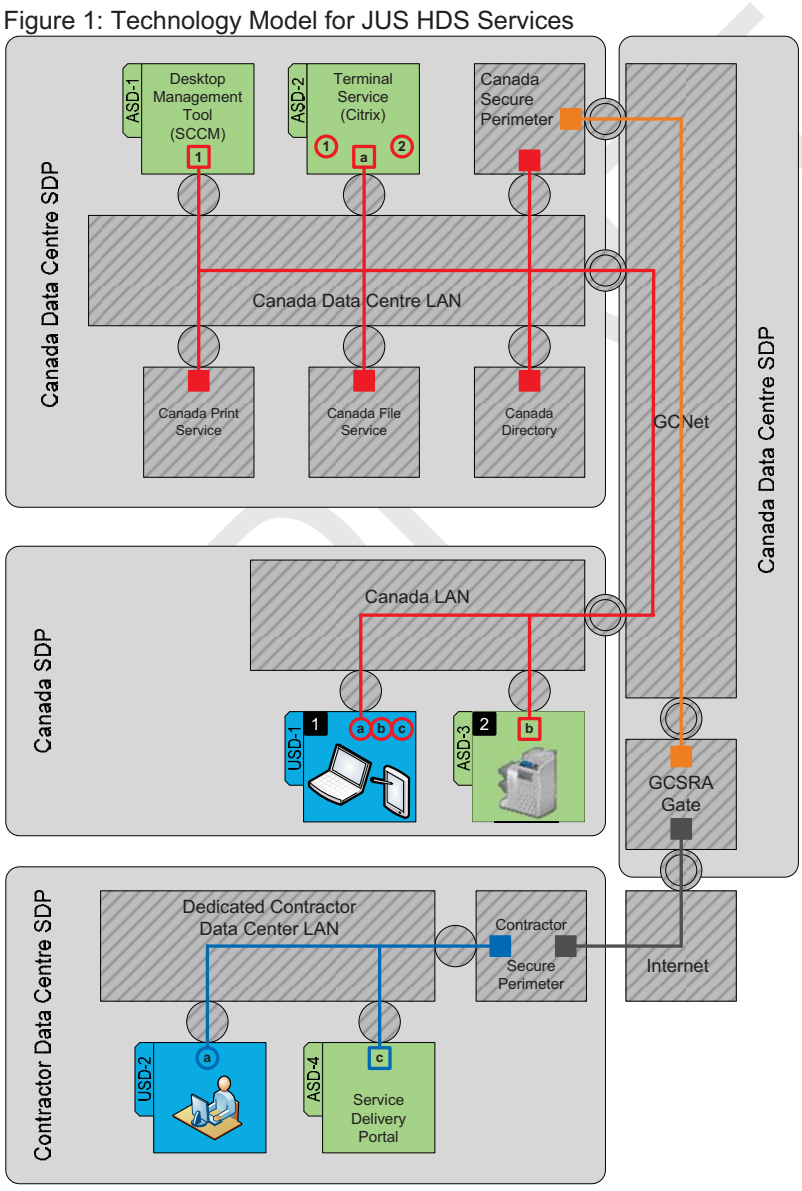
(1) This section is provided for information only.

1.1 Technology Model

(2) The Contractor is directed to review the Department of Justice Canada (JUS) Help Desk and Support (HDS) Services Annex A - Appendix A: Definitions for the definitions of commonly used terms in the Request for Proposal (RFP).

(3) The technology model for JUS HDS Services is illustrated in Figure 1. The technology model provides a high level technology perspective of the JUS HDS Services. The objective is to show the type of capabilities required for the service, where these capabilities will be implemented and how they will be networked together.

Figure 1: Technology Model for JUS HDS Services



(4) The use of the technology model should not be construed as limiting the design of JUS HDS Services.

(5) The key elements of the technology model are:

a) Service Delivery Points (SDP) that represent physical locations in a building where JUS HDS Services components are implemented;

b) Application Service Domains (ASD) that represent the grouping of 1 or more service objects capable of offering a service for consumption;

c) User Service Domains (USD) that represent the grouping of 1 or more access devices capable of consuming 1 or more Services; and

d) non-JUS HDS Services Domains, that have been included to allow Canada to describe existing Canada systems and services that will integrate with the JUS HDS Services.

1.1.1 Service Delivery Points

(1) SDPs are represented by a non-hatched grey boxes in Figure 1 which depict the following SDPs:

a) Canada Data Centre SDP: a Government of Canada (GC) data centre;

b) Contractor Data Centre SDP: a Contractor data centre where JUS HDS Services infrastructure is implemented; and

c) Canada SDP: a GC location.

(2) The infrastructure components in Canada Data Centre SDPs or Canada SDPs are provided by Canada.

1.1.2 Application Service Domains

(1) ASDs are represented by non-hatched green boxes in Figure 1 which depict the ASDs described in Table 1.

Table 1 - Application Service Domains

Label	Application Service Domain	Services offered	Services consumed
ASD-1	Desktop Management Tool (Microsoft System Centre Configuration Manager (SCCM))	1 Remote assistance The Terminal Service invokes the Remote Assistance Tool that mediates the session with the End User Device.	1 Remote control agent
		1 Software distribution The Terminal Service invokes the Software Distribution Tool to configure software distribution. The Software Distribution Tool interacts with the End User Device to push software	1 Software distribution agent

Label	Application Service Domain	Services offered	Services consumed
		components.	
ASD-2	Terminal Service (Citrix)	a Terminal Service session This is the interface for the Terminal Service session to be presented on the End User Device.	
ASD-3	Network Printer or Multi-Functional Device Printer	2 Printing device management agent. This is the management interface for printing device remote configuration. b Printing of digital content onto paper, faxing of digital content over a telephone line, scanning of paper into digital content, emailing of digital content.	
ASD-4	Service Delivery Portal	c Providing self-service requests, providing web content, exposing IT Service Management tool functions.	

1.1.3 User Service Domains

(1) USDs are represented by non-hatched blue boxes in Figure 1 which depict the USDs described in Table 2.

Table 2 - User Service Domains

Label	User Service Domain	Services offered	Services consumed
USD-1	End User Device	1 Remote control agent 1 Software distribution agent	1 Desktop Management Tool - Remote control 1 Desktop Management Tool -

Label	User Service Domain	Services offered	Services consumed
			Software distribution [a] Terminal Service (Citrix) using a thin client application [b] Printing using a print agent [c] Service Delivery Portal using a web browser
USD-2	Service Desk Agent Device	GC Secure Remote Access client	GC Secure Remote Access

1.1.4 Non-JUS HDS Services Domains

(1) The non-JUS HDS Services Domains, described below in Table 3 in order of appearance in Figure 1 (left to right, top to bottom), are represented by hatched grey box in Figure 1.

Table 3: Non-JUS HDS Services Domains

NON-JUS HDS SERVICES DOMAIN
Canada Secure Perimeter
GC Network (GCNet)
Canada Data Centre LAN
Canada Print Service
Canada File Service
Canada Directory
Canada LAN
GC Secure Remote Access (GCSRA) Gate
Dedicated Contractor Data Centre LAN
Contractor Secure Perimeter

1.1.5 JUS HDS Services Domains

(1) JUS HDS Services Domains, described below in Table 4, are used as the identifier of each Statement of Work (SOW) Annex where the requirements for the JUS HDS Services that is part

of the Domain can be found.

Table 4: Summary of JUS HDS Services Domains

JUS HDS SERVICES DOMAIN	DESCRIPTION
JUS Service Desk Service	The JUS Service Desk Service established by the Contractor will be the single contact point for End Users to report Incidents or submit Service Requests, and will be responsible for maintaining all information relating to the Incidents and Service Requests reported.
JUS On-Site Support Service	The JUS On-Site Support Service established by the Contractor will complete work activities that require hands-on access to the End User Device for the purpose of resolving Incidents or performing Service Requests.
JUS Desktop Engineering Service	The JUS Desktop Engineering Service established by the Contractor will respond to Incidents that require highly specialized technical skills and will also create and maintain OS Images, Software Packages, Software Patches and Upgrades as well as support documentation. The JUS Desktop Engineering Service will also manage the desktop management tool.

1.2 Canada Services

(2) This section defines the services that Canada will be responsible for in relation to the JUS HDS Services.

1.2.1 Hardware and Software Asset Procurement

(1) Canada will create hardware and software procurement vehicles for the JUS HDS Services. Canada will manage the demand and process orders with the vendor, and ensure delivery of the assets to the applicable pre-staging or distribution site. Canada will manage all hardware and software vendors.

1.2.2 On-Site Support Outside the National Capital Region

(1) Canada will provide on-site support human resources for all locations outside of the National Capital Region (NCR). These resources will leverage the tools and processes put in place by the Contractor. They will be assigned Incidents and Services Requests by the JUS Service Desk Service.

1.2.3 Canada File Service Management

(1) Canada will provide the underlying network file storage infrastructure. The Contractor will manage all End User access and privileges to shared and network file storage.

1.2.4 Canada LAN Management

(1) Canada will configure and support the LAN and provide all underlying LAN infrastructure. The Contractor will manage all network access accounts, and related user IDs, passwords, and resource privileges.

1.2.5 Canada Print Service Management

(1) Canada will provide a means for End Users to connect to network printers. The Contractor will create and manage all print queues for all networked printers. The Contractor will be expected to provide support to End Users trying to connect and use these printers. The Contractor will be responsible to provide fleet maintenance services for the printers.

1.2.6 Security Services

(1) Canada will provide security design, configuration, implementation and support services related to Public Key Infrastructure (PKI) keys, encryption, malware protection, and personal firewalls. The Contractor will be required to deliver updates to these services, as requested by Canada (e.g. distribute the latest versions of software).

1.2.7 Server Hosting Services

(1) Canada will provide server hosting services for the desktop management tool (SCCM).

1.2.8 Remote Access Services

(1) Canada will provide all Secure Remote Access (SRA) Services.

1.2.9 Network Services

(1) Canada will provide network connectivity, monitoring and management services for connectivity from the Canada data centre(s) and all End Users in scope.

1.2.10 Other Infrastructure and Application Support Services

(1) Canada will provide Level 2 and Level 3 Support for supported business applications, and for other infrastructure services (e.g. data centre and network).

1.2.11 Computers and Smart Phones

(1) Canada will provide computing devices and smart phones to the Contractor resources that need to connect to Canada's network for the delivery of on-premise JUS HDS Services. Contractor resources will not be allowed to connect their own equipment to Canada's network.

(2) Canada will provide computing devices to the Contractor personnel that need to connect to Canada network using Canada's SRA Service for the delivery of JUS Service Desk service.

2 OPERATIONAL READINESS PHASE

2.1 Requirements for Project Schedules

(1) For all project schedules required in this SOW, the Contractor must:

a) provide the schedule in Microsoft Project 2013 format;

b) identify the phases, gates, deliverables and milestones of the Work as distinct tasks where each task has a start and end date, a duration, is assigned to a resource group, and has the dependencies identified, such that the start and end date of the tasks are driven by the dependencies and duration;

c) identify each Contract deliverable as a milestone;

d) clearly describe the dependencies on Canada including:

i) identifying Canada's reviews as tasks;

ii) identifying Canada's approvals as milestones;

iii) identifying Canada's deliverables as milestones;

e) comply with dependencies identified in this SOW;

f) not create unnecessary dependencies on Canada's review and approval;

g) limit dependencies to the maximum extent possible;

h) schedule tasks in parallel to the maximum extent possible; and

i) progressively submit deliverables (i.e. not all at once).

(2) For all project schedules required in this SOW, the Contractor must provide as an annex to the project schedule:

a) a Canada resource plan identifying:

i) the task id and task name from the schedule where Canada input is required;

ii) what information is expected from Canada;

iii) what subject matter expertise is required to provide input to the task;

iv) what is the estimated duration of the interactions with the Contractor for the task;

v) attenuation measures to limit Canada resource overloading across schedules;

b) a list of planning assumptions;

c) a list of schedule risks including, but not limited to:

i) categorization of each risk;

ii) probability of each risk;

iii) impact if the risk materializes;

iv) mitigation measures;

v) monitoring measures; and

vi) risk assignment.

(3) Unless otherwise specified, for each Contract deliverable in a project schedule:

a) Canada will review the deliverable within 10 Federal Government Working Days (FGWDs) and provide its first round of formal comments to the Contractor, in writing;

b) the Contractor must provide an updated deliverable that addresses comments received from Canada within 5 FGWDs after receiving Canada first round of comments;

c) Canada will review the updated deliverable within 5 FGWDs after receiving the Contractor's updated deliverable and provide its second round of formal comments to the Contractor, in writing;

d) the Contractor must provide the final deliverable that addresses comments received from Canada within 5 FGWDs after receiving Canada second round of comments; and

e) Canada will approve or reject the deliverable within 5 FGWDs after receiving the

Contractor's final deliverable and provide a formal answer to the Contractor, in writing.

2.2 Deliverable Dependencies

(1) The Contractor must schedule SOW deliverables in compliance with the dependencies identified in Table 5.

Table 5 - Deliverable Dependencies

ID	Deliverable Name	Predecessors
1	Operational Readiness Schedule	
2	Program Management Plan	1
3	Service Management Plan	2
4	Privacy Management Plan	2
5	Privacy Impact Assessment	4
6	Configuration Management Plan	3
7	Service Continuity Plan	2
8	Transition Plan	2
M1	**Security Assessment and Authorization - Gate 1**	
9	High Level Design	2
10	Security Requirements Traceability Matrix Traced To High-Level Design	9
M2	**Security Assessment and Authorization - Gate 2**	M1
11	Detailed Design	10
12	Security Requirements Traceability Matrix Traced To Detailed Design	11
13	Change and Configuration Management Process	11
14	Operational Security Procedures	11
15	Security Installation Procedures	11
M3	**Security Assessment and Authorization - Gate 3**	M2
16	Implementation of JUS HDS Services	12,13,14,15
17	Security Installation Verification Plan	12,13,14,15
18	Integration Security Test Plan	12,13,14,15

19	Vulnerability Assessment Plan	12,13,14,15
20	Security Installation Verification Report	16,17
21	Integration Security Test Report	16,18
22	Vulnerability Assessment Report	16,19

2.3 Operational Readiness Schedule

(1) The Contractor must submit to Canada Contract's Technical Authority an operational readiness schedule, within 20 FGWD after Canada announces the Service Go Live Date, for approval by Canada to complete the following Work (further detailed in sections 2.4 through 2.13):

a) Program Management Plan;
b) Service Management Plan;
c) Privacy Management Plan;
d) Privacy Impact Assessment;
e) Configuration Management Plan;
f) Service Continuity Plan;
g) Transition Plan;
h) Security Assessment and Authorization of the High-Level Design (Gate 1):
    i) High-Level Design;
    ii) Security Requirements Traceability Matrix traced to High-Level Design;
i) Security Assessment and Authorization of the Detailed Design (Gate 2):
    i) Detailed Design;
    ii) Security Requirements Traceability Matrix Traced to Detailed Design;
    iii) Change and Configuration Management Process;
    iv) Operational Security Procedures;
    v) Security Installation Procedures;
j) Security Assessment and Authorization of the Installation (Gate 3):
    i) Implementation of JUS HDS Services;
    ii) Security Installation Verification Plan;
    iii) Integration Security Test Plan;
    iv) Vulnerability Assessment Plan;
    v) Security Installation Verification Report;
    vi) Integration Security Test Report; and
    vii) Vulnerability Assessment Report.

(2) The Work identified in the operational readiness schedule must be completed before Transition-In commences (see Transition-In subsection 2.10.1), including days required by Canada for review and approval of the Work, according to the operational readiness schedule.

(3) The completion of any Contract deliverable in the operational readiness schedule is not conditional on the completion of any other Work identified in this RFP.

(4) The Work identified in the operational readiness schedule is subject to review and approval by Canada.

2.4 Program Management Plan

(1) The Contractor must provide a program management plan to Canada Contract's Technical Authority which must address the following topics according to the PMBOK® Guide — Fifth Edition or any other project management method approved by Canada:

a) executive summary description of JUS HDS Services;

b) organizational plan that includes management structure, organizations, and roles and responsibilities of key personnel and subject matter experts;

c) resource plan that includes a methodology for determining resource levels required to complete the Work under the Contract and for assessing the skills and competencies of the resources to perform the required function;

d) quality assurance plan that includes an approach to formulating and enforcing work and quality standards, and reviewing work in progress;

e) communications plan that includes an approach for communicating individual task requirements, resolving issues (technical, service and personnel) and risks between the Contractor and Canada, and managing communications between the Contractor and Canada. The approach must include the use of secure electronic communications tools and applications, approved by Canada, to share information with program stakeholders identified by Canada;

f) risk management plan that includes the approach for identifying and tracking risks, isolating the event triggers for risks, assessing probability and impact, as well as identifying a mitigation plan; and

g) issue management plan that includes the approach for identifying and managing service management issues, isolating the issues, assessing the impacts, identifying responsible parties, assessment of a severity and priorities, and processes for determining a resolution.

2.5 Service Management Plan

(1) The Contractor must provide a service management Plan for JUS HDS Services to Canada Contract's Technical Authority that includes:

a) management and operational structure, organizations, roles and responsibilities of each function performing work under this Contract and key personnel and subject matter experts;

b) operational and management escalation process that includes:

i) identification of the designated Canada and Contractor personnel authorized to invoke the escalation procedure;

ii) escalation contact names, titles, email addresses and phone numbers; and

iii) escalation time frames based on the length of time an Incident remains unresolved and priority level of the Incident;

c) privacy breach process;

d) security breach process;

e) Service Desk processes;

f) Service Request processes for Contractor request fulfilment;

g) Change Management processes including how they are integrated with other Management Service processes;

h) Incident Management processes including how they are integrated with other Management Service processes and definition of Incident priority levels;

i) Configuration Management processes including how they are integrated with other Management Service processes;

j) Problem Management processes including how they are integrated with other

Management Service processes;

k) Release Management processes including how they are integrated with other Management Service processes;

l) detailed description of processes for each Management Service, and

m) detailed description of administration, operational and management support systems and tools.

2.6 Privacy Management Plan

(1) The Privacy Management Plan (PMP) demonstrates that the Contractor can meet the requirements of the Contract and provides assurance of their ability to manage Personal Information and Records in accordance with the statutory obligations.

(2) Within 60 FGWDs of the Service Go Live Date being announced, the Contractor must provide a draft PMP. Canada reserves the right to request changes to the PMP in order to ensure that privacy is being properly managed by the Contractor.

(3) Within 20 FGWDs following a request by Canada, the Contractor must provide Canada with an update to its PMP.

(4) The PMP must specifically describe the following items in great detail:

a) Contractor's privacy protection strategies and detail exactly how the Personal Information will be treated over its life cycle;

b) how the Personal Information will be collected, used, retained, and disclosed only for the purposes of the Work specified in the Contract;

c) how the Personal Information and Records will be accessible only to authorized individuals (on a need-to-know basis) for the purposes of the Work specified in the Contract;

d) the privacy breach protocol, and provide details on how any privacy breaches will be handled;

e) how the Contractor intends to ensure that Canadian Privacy requirements, as outlined in the Privacy Act , the Access to Information Act and Library and Archives of Canada Act, will be met throughout the performance of the Work and for the duration of the Contract Period;

f) any new measures the Contractor intends to implement in order to safeguard the Personal Information and the Records in accordance with their security classification;

g) how the Contractor intends to ensure that any reports containing Personal Information are securely stored or transmitted in accordance with their security classification; and

h) describe how the Contractor intends to ensure that their staff is trained on privacy and privacy related principals.

2.7 Privacy Impact Assessment

(1) The Contractor must identify the requirements for a Privacy Impact Assessment (PIA) in accordance with the TBS Directive on PIA's (http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=18308&section=text#cha1) by providing the following information within 20 FGWDs of a request by Canada:

a) business processes, data flows and procedures for the collection, transmission, processing, storage, disposal and access to information including Personal Information;

b) a list of the Personal Information used by the Contractor in connection with the Work and the purpose of each Personal Information item;

c) how the Personal Information is shared and with whom;

d) a list of all locations where hard copies of Personal Information are stored;

e) a list of all locations where Personal Information in machine-readable format is stored (for example, the location where any server housing a database including any Personal

Information is located), including back-ups;

f) a list of all measures being taken by the Contractor to secure the Personal Information and the Records beyond those required by this agreement;

g) any privacy-specific security requirements or recommendations that need to be addressed;

h) a detailed explanation of any potential or actual threats to the Personal Information or any Record, together with an assessment of the risks created by these threats and the adequacy of existing safeguards to prevent these risks; and

i) results of consultations (if any) from a PIA review by the Office of the Privacy Commissioner of Canada (OPCC) with signoff by OPCC.

(2) The Contractor must assist Canada during the development of the PIA and must implement recommendations from the PIA based on a schedule approved by Canada at no cost to Canada.

(3) If changes to the JUS HDS Services are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by the Canada, the Contractor must provide Canada with sufficient detail on the changes to support an update to the PIA, and obtain approval from Canada for the anticipated change.

(4) The Contractor must provide a privacy awareness communications kit to its resources involved in the JUS HDS Services that provides an overview on the use of Personal Information.

2.8 Configuration Management Plan

(1) The Contractor's configuration management plan must be developed to address both the Contractor provided infrastructure and the Canada provided infrastructure that the Contractor is responsible to manage as part of the JUS HDS Services.

(2) The Contractor must provide a configuration management plan that:TRACEFROMx>SR-73</TRACEFROMx>

a) addresses roles, responsibilities, and configuration management processes and procedures;

b) defines the configuration items for JUS HDS Services and when the configuration items are placed under configuration management;

c) establishes the means for identifying configuration items throughout the system development life cycle and a process for managing the configuration of the configuration items;

d) defines the processes for Software Patch management on custom software utilized within the JUS HDS Services Infrastructure that includes:<TRACEFROMx>SR-157</TRACEFROMx>

i) identifying, reporting, and correcting flaws in custom software;

ii) testing software updates related to flaw remediation for effectiveness and potential side effects on the JUS HDS Services before installation;

iii) incorporating flaw remediation into the JUS HDS Services configuration management process;

e) defines the processes for Software Patch management of the JUS HDS Services Infrastructure components that includes: TRACEFROMx>SR-158</TRACEFROMx>

i) ensuring the latest version of applications and operating systems are used;

ii) ensuring that vulnerabilities are evaluated and vendor-supplied security Software Patches are applied in a timely manner;

iii) prioritizing critical Software Patches using a risk-based approach;

iv) taking applications offline and bringing them back online;

v) aligning criticality levels for Software Patches as specified by Canada;

vi) rating of vulnerabilities against Common Vulnerabilities Scoring System (CVSS) v2;

vii) testing and verification methodology to ensure that Software Patches have been implemented properly; and

viii) notifying Canada of configuration vulnerabilities that would allow an unauthorized individual to compromise the confidentiality, integrity, or availability of JUS HDS Services.

2.9 Service Continuity Plan

(1) The Contractor must provide a Service Continuity Plan (SCP) to Canada Contract's Technical Authority that includes: <TRACEFROMx>SR-74</TRACEFROMx>

a) detailed and documented processes for restoring JUS HDS Services;

b) detailed the communications plan with Canada and its suppliers;

c) detailed plan and processes for transferring operational, management and administration functionality to a backup operations centre;

d) back up strategies for data centre facilities, network facilities, operational support systems and data, and key service components;

e) how the Contractor will ensure that its suppliers have in place SCP;

f) description of the process for testing the SCP;

g) steps the Contractor will take if any of its key suppliers go out of business, and

h) steps the Contractor will take if any of its manufacturers or Original Equipment Manufacturers (OEM) is no longer considered a trusted manufacturer or OEM by Canada.

(2) The Contractor must provide a final version of the SCP within 15 FGWDs after receiving comments from Canada on the draft SCP. <TRACEFROMx>SR-88</TRACEFROMx>

(3) The Contractor must implement the SCP (all processes, procedures, roles, responsibilities, etc.), and any subsequent annual updates, within 60 FGWDs following acceptance by Canada. <TRACEFROMx>SR-88</TRACEFROMx>

(4) The Contractor must provide to Canada within 40 FGWDs of a request, evidence not greater than 12 months old, (e.g. test results, evaluations, and audits, etc.) that the SCP has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Canada's service continuity requirements. <TRACEFROMx>SR-88</TRACEFROMx>

(5) If the Contractor determines that it will take more than 40 FGWDs to provide the requested evidence for the SCP, the Contractor must notify Canada within five (5) FGWDs of the original request for evidence, and request an extension, in writing, with appropriate justification. Granting an extension is within Canada's sole discretion. <TRACEFROMx>SR-88</TRACEFROMx>

2.10 Transition Plan

(1) The Contractor must submit a transition plan for coordinating all activities related to JUS HDS Services Transition, for approval by Canada that includes a plan and a schedule in Microsoft Project format to complete the following by the Service Go Live Date:

a) a transition-in methodology to take over responsibility for JUS HDS Services;

b) service transition strategy and approach to reduce transition risks;

c) a strategy to prevent service disruptions;

d) a communications strategy;

e) a management of change strategy;

f) a training strategy;

g) roles and responsibilities of key stakeholders;

h) success criteria;

i) integration with existing Canada processes;

j) integration of all JUS HDS Services;

k) creation of Service Delivery Portal Accounts;
l) an accommodation requirements for the resident JUS HDS Services personnel;
m) progress reporting;
n) an issue escalation process;
o) detailed schedule for the migration of End Users and Canada SDPs to the new service;
p) checklist of pre-transition and post transition activities for personnel involved in the transition (e.g. End Users, Canada Operations, Service Managers, Level 2 or Level 3 Support representatives);
q) transition reporting;
r) issue escalation process; and

2.10.1 Transition In

(1) The Service Go Live Date will be the latest of April 1st 2017 or 90 calendar days after Contract Award.

(2) The Contractor must execute the approved Transition Plan.

(3) The Contractor must begin providing the Help Desk and Support Services to Canada by the Service Go Live Date.

(4) The completion of any Work deliverable in the Transition Plan is not conditional on the completion of any other Work identified in this Contract.

(5) The Contractor must manage, track and coordinate the overall implementation of all deliverables and activities related to Transition In.

(6) Canada recognizes that considerable effort will be required by the new Contractor during the "Transition In" period in order to affect a smooth start-up of the new service. During this period, Canada intends to place a "freeze" (to the extent possible) on changes to the infrastructure. Canada also intends to assist the new Contractor in its "Transition-In" efforts by providing knowledge transfer.

(7) Canada expects that there will be a maximum of four (4) weeks "overlap" period immediately prior to the Service Go Live Date in which the previous Contractor will continue to deliver services while representatives of the new Contractor are on site.

(8) It is essential that the transition from the previous Contractor to the new Help Desk and Support Services present as little disruption to the End User community as possible. Accordingly, the new Contractor must work collaboratively with Canada in planning the transition from the previous Contractor to the new service.

(9) The legacy Service Management data will be made available for import into the Contractor's Service Delivery Portal, if desired. The data will be available in an "open" SQL database file format. Other data will also be made available for import (e.g. asset management data, user directory data, etc.).

(10) The HDS Service Desk Service must ensure that all "open" Service Management data is migrated into the Service Delivery Portal. This includes Incidents, Problems, Changes, Releases, and Service Requests.

2.10.2 Transition Out

(1) Canada wants to ensure that at the end of the contractual arrangement with the Contractor, an "end of term" or "hand over" transition effort is conducted by which Canada regains possession of all of the equipment and data belonging to Canada, and it learns, (e.g. through knowledge transfer and/or other means) any and all information necessary for Canada or another Contractor to assume responsibility for delivering IT services to its user community.

(2) At the end of the contract, the Contractor must return all information, Help Desk and Support Services Data and equipment that are owned by Canada. The Contractor agrees that, in addition to other data not specifically identified here, Canada owns all information pertaining to Canada's

processes, knowledge, FAQs, Incidents, and Service Requests that will be received and resolved by the Contractor over the term of the contract.

(3) At the end of the contract, the Contractor must conduct an "end of term" or “hand over” transition effort to facilitate the accomplishment of a seamless transition and to identify how it will coordinate with the incoming contractor and/or Canada’s personnel that includes, as a minimum delivering the following:

a) A complete extract of the Service Delivery Portal data, in a COTS file format (e.g. in SQL format) as specified by Canada, that includes but is not limited to:
   i) Incident Tickets;
   ii) Service Requests;
   iii) Problem Tickets;
   iv) Change records;
   v) Release Records;
   vi) Knowledge Repository;
   vii) Troubleshooting Scripts;
   viii) Frequently Asked Questions;
   ix) End User List;
   x) Resolver Queues; and
   xi) Resolver Group Membership.
   xii) Points of contact
   xiii) Location of technical and project management documentation
   xiv) Transition of key personnel
   xv) Actions required of Canada

b) A report of the Incidents and Problems currently outstanding; and

c) Knowledge transfer concerning the status of ongoing technical initiatives and the current status of IT service delivery.

(4) The Contractor must verify that all Software Packages and OS Images are properly saved in the Definitive Software Library.

(5) The Contractor must return to Canada all Government Furnished Equipment that Canada provided to the Contractor.

(6) The Contractor must provide a debriefing to Canada to confirm the Transition Out is completed and transfer any remaining knowledge to Canada.

2.11 Security Assessment and Authorization of the High-Level Design (Gate 1)

(7) The Contractor must provide Canada with the following deliverables for approval by Canada:

a) high-level design (see High-Level Design subsection), and

b) security requirements traceability matrix (see Security Requirements Traceability Matrix Traced to High-Level Design subsection).

(8) The Contractor must wait for Gate 1 approval by Canada before proceeding with the next gate of the security assessment and authorization.

2.11.1 High-Level Design

(1) This subsection defines the high-level design requirements for JUS HDS Services.

(2) The high-level design for the JUS HDS Services must conform to the requirements in JUS HDS Services Annex A - Appendix B: Security Requirements.

(3) The high-level design must contain the following information:

a) an architecture and design of the various JUS HDS Services components with particular

emphasis on the component interfaces;

b) design specifications for all system interfaces between JUS HDS Services Domains and non-JUS HDS Services Domains.

c) a deployment architecture that describes the allocation of logical service components to virtual or physical computing nodes and highlights the redundancy, scalability and security features of the architecture that support the achievement of all required service levels;

d) a network architecture including logical and physical connectivity diagrams that illustrate the implementation of perimeter security controls as well as the placement of services in network security zones and highlights the redundancy, scalability and security features of the architecture that support the achievement of all required service levels.

e) a description of the architectural layers (e.g., communications layer, virtualization layer, platform/OS layer, data management layer, middleware layer, business application layer);

f) a high-level component diagram that clearly shows the allocation of services and components to network security zones and identifies all data flows;

g) a description of the network zone perimeter defences;

h) a description of the use of virtualization technologies, where applicable;

i) descriptions of the allocation of all technical security requirements to high-level design elements at all architectural layers;

j) descriptions of the allocation of all non-technical security requirements to high-level organizational or operational elements;

k) a description of the approach for Remote Management;

l) a description of the approach for access control;

m) a description of the approach for security management and audit;

n) a description of the approach for Configuration Management; and

o) a description of the approach for Software Patch management.

(4) The high-level design must explicitly document justification for key security design decisions as they relate to:

a) network security zoning;

b) network and network zone perimeter defence; and

c) use of virtualization technology.

(5) The high-level design must contain the following information for the Service Delivery Portal:

a) a user interface concept describing the look and feel of the Service Delivery Portal web pages; and

b) a description of all web-page flows that illustrates how the User self-service and Administrator self-service functions will be performed using the Service Delivery Portal.

(6) The high-level design for JUS HDS Services must ensure the implementation of Internet Protocol Version (IPV) 6 coexists with IPV 4 and provides all the functionality for JUS HDS Services as provided with IPV 4, including any transition mechanisms that may be necessary between IPV 4 and IPV 6 at the Contractor's SDPs.

2.11.1.1 Network Connectivity

(1) Canada will provide GCSRA to the Contractor to allow the Contractor to connect to Canada's Network to access the Desktop Management Tools.

(2) The Contractor must use GCSRA to connect its resources to Canada's Network to access the Desktop Management Tools.

(3) The Contractor must provide the telecommunication lines to connect its SDPs to the Canada GCSRA gate on the Internet at no additional cost to Canada.

2.11.2 Security Requirements Traceability Matrix Traced to High-Level Design

(1) The Contractor must provide Canada with a Security Requirements Traceability Matrix (SRTM) that provides for each security requirement in the JUS HDS Services Annex A - Appendix B: Security Requirements, documentation references within the high-level design that describe the high-level system design elements to be implemented. The SRTM establishes assurance that the JUS Help Desk and Support High-level design fully satisfies its security requirements.

(2) All service documentation referenced in the STRM must be provided to Canada with the SRTM and must describe the security safeguards in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements in the JUS HDS Services Annex A - Appendix B: Security Requirements.

(3) At a minimum, the SRTM must contain, for each security requirement, the following information:

a) the security requirement identifier (SEC ID) from the JUS HDS Services Annex A - Appendix B: Security Requirements;

b) an identifier that maps the security requirement to the corresponding statement in the SOW (e.g., heading or line ID);

c) a description of how the security requirement is addressed in the high-level design;

d) the security requirement statement from the JUS HDS Services Annex A - Appendix B: Security Requirements; and

e) tracing (a reference to an identifiable element) to high-level design specifications.

2.12 Security Assessment and Authorization of the Detailed Design (Gate 2)

(1) The Contractor must provide Canada with a draft version of the following deliverables for approval by Canada:

a) detailed design security specification (see Detailed Design subsection);

b) updated SRTM traced to detailed design (see Security Requirements Traceability Matrix Traced To Detailed Design subsection); and

c) Change and configuration management process.

(2) The Contractor must wait for Gate 2 approval by Canada before proceeding with the next gate of the security assessment and authorization.

2.12.1 Detailed Design

(1) The Contractor must provide Canada with a detailed design that includes:

a) a detailed component diagram (this should be a refinement of the high-level component diagram);

b) descriptions of the allocation of technical security mechanisms to detailed design elements;

c) descriptions of the allocation of non-technical security mechanisms to high-level organizational or operational elements; and

d) justification for key design decisions.

(2) The detailed design must be compliant with the high-level design (see High-Level Design subsection). The detailed design must evolve the high-level design from a solution and technology agnostic design to a technology/product/solution specific design. It must be consistent with the approaches and decisions of the high-level design.

2.12.2 Security Requirements Traceability Matrix Traced to Detailed Design

(1) The Contractor must provide Canada with an updated SRTM that provides for each security requirement in the JUS HDS Services Annex A - Appendix B: Security Requirements, documentation references within the service detailed design security specification that describe the security safeguards to be implemented. The security requirements traceability matrix

establishes assurance that the JUS HDS Services detailed design fully satisfies its security requirements.

(2) All service documentation referenced in the SRTM must be provided to Canada with the SRTM and must describe the security safeguards in sufficient detail to allow Canada to confirm that the security safeguards satisfy the security requirements in the JUS HDS Services Annex A - Appendix B: Security Requirements.

(3) At a minimum, the SRTM must contain, for each security requirement, the following information:

a) the SEC ID from the JUS HDS Services Annex A - Appendix B: Security Requirements;

b) an identifier that maps the security requirement to the corresponding statement in the SOW (e.g., heading or line ID);

c) the security requirement statement from the JUS HDS Services Annex A - Appendix B: Security Requirements;

d) tracing (a reference to an identifiable element) to high-level design specifications, and

e) tracing (a reference to an identifiable element) to detailed design specifications.

2.12.3 Change and Configuration Management Process

(1) The Contractor must provide Canada with a change management process that includes:

a) Contractor's change management authorities;

b) Contractor resource roles and responsibilities for change management;

c) how the Contractor will use the change management process to support the development of the JUS HDS Services (e.g., a concept of operation);

d) method used to uniquely identify Configuration Items;

e) configuration item identification method;

f) description of the change management process, including the change review and approval process;

g) means for identifying Configuration Items throughout the system development life cycle and a process for managing the configuration of the Configuration Items;

h) measures used to enforce only authorized changes; and

i) procedures that the Contractor will use to accept modified or newly created configuration items.

2.12.4 Operational Security Procedures

(1) The Contractor must provide Canada with the operational security procedures that includes:

a) for each Operator role:

i) schedule of security-relevant actions to be performed in order to maintain the security posture of the JUS HDS Services;

ii) how to use available operational interfaces; and

iii) each scheduled action and how the End User is expected to perform it.

b) operational roles and responsibilities for:

i) interaction requirements with Canada representatives;

ii) reporting schedule and procedures;

iii) access control;

iv) audit and accountability;

v) identification and authentication;

vi) system and communications protection;

vii) awareness and training;

viii) configuration management;

ix) contingency planning;
x) Incident response;
xi) maintenance;
xii) media protection;
xiii) physical and environment protection;
xiv) personnel security; and
xv) system and information integrity.

2.12.5 Security Installation Procedures

(1) The Contractor must provide Canada with the security installation procedures that includes:
a) steps necessary for the secure installation and configuration of JUS HDS Services and for the secure preparation of the operational environment;
b) installation and configuration of all technical security solutions;
c) security configuration of hardware products; and
d) security configuration of software products (Commercial-Off-The-Shelf (COTS) and open source)

2.13 Security Assessment and Authorization of the Installation (Gate 3)

2.13.1 Implementation of JUS HDS Services

(1) The Contractor must implement the Service Delivery Portal in compliance with the approved predecessor deliverables (see Deliverable Dependencies subsection).
(2) The Contractor must provide Canada with the following deliverables for approval by Canada:
a) security installation verification plan (see Security Installation Verification Plan subsection);
b) integration security test plan (see Integration Security Test Plan subsection);
c) vulnerability assessment plan (see Vulnerability Assessment Plan subsection);
d) security installation verification report (see Security Installation Verification Report subsection);
e) integration security test report (see Integration Security Test Report subsection); and
f) vulnerability assessment report (see Vulnerability Assessment Report subsection).
(3) The Contractor must wait for Gate 3 approval by Canada before beginning the Transition-In.

2.13.2 Security Installation Verification Plan

(1) The Contractor must develop a Security Installation Verification Plan to conduct a comprehensive verification of the installation of security solutions and the security configuration of the JUS HDS Services' production environment.
(2) The Security Installation Verification Plan must identify the verifications to be performed and describe the scenario for performing each verification.
(3) The Contractor must include in the Security Installation Verification Plan provisions for Canada representatives to witness security installation verification.
(4) The Contractor must provide Canada with a Security Installation Verification Plan that contains, at minimum, the following information:
a) the security verification approach;
b) Canada witnessing arrangements;
c) an outline of the security verification items;
d) for each security verification item:

i) a description of the verification scenario;
ii) ordering dependencies; and
iii) expected results (i.e., pass/fail criteria).

(5) The Contractor must provide Canada with an updated SRTM that contains, for each security requirement to be tested by the security installation verification plan, the following information:

a) tracing (a reference to an identifiable element) to security installation verification test cases.

2.13.3 Integration Security Test Plan

(1) The Contractor must develop an Integration Security Test Plan that addresses integrated security functions (e.g., Kerberos authentication to Email server) as opposed to standalone security functions (e.g., local user login to operating system).

(2) The Integration Security Test Plan must identify the tests to be performed and describe the scenarios for performing each test. Test scenarios must include any ordering dependencies on the results of other tests.

(3) The Contractor must include in the Integration Security Test Plan provisions for Canada representatives to witness the integration security testing.

(4) The Contractor must provide Canada with an Integration Security Test Plan that contains, at minimum, the following information:

a) the security functions to be tested;
b) Canada witnessing arrangements;
c) for each security function or sets of security functions, the items to be tested including:
i) a description of the test case, procedure, or scenario;
ii) environmental requirements;
iii) ordering dependencies; and
iv) expected results (i.e., pass/fail criteria)

(5) The Contractor must provide Canada with an updated SRTM that contains, for each security requirement to be tested by the integration security test plan, the following information:

a) tracing (a reference to an identifiable element) to integration security testing test cases.

2.13.4 Vulnerability Assessment Plan

(1) The Contractor must provide Canada with a Vulnerability Assessment Plan that contains, at minimum, the following information:

a) a description of the scope of the vulnerability assessment;
b) necessary arrangements for Canada's representatives to witness the assessment;
c) a description of the vulnerability assessment process; and
d) a description of the vulnerability assessment tools that will be used, including any software versions.

2.13.5 Security Installation Verification Report

(1) The Contractor must conduct security installation verification in accordance with the Security Installation Verification Plan.

(2) The Contractor must correct installation and configuration errors and omissions that are detected as a result of the security installation verification.

(3) The Contractor must provide Canada with a security installation verification report that contains, at minimum, the following information for each of the test items in the security installation verification plan:

a) the expected results (i.e., pass/fail criteria);

b) the actual results; and

c) a description of deviations and how each was resolved.

2.13.6 Integration Security Test Report

(1) The Contractor must conduct integration security testing in accordance with the Integration Security Test Plan.

(2) The Contractor must provide Canada with an Integration Security Test Report that contains, at minimum, the following information for each of the test items in the Integration Security Test Plan:

a) the expected results (i.e., pass/fail criteria);

b) the actual results; and

c) a description of deviations and how each was resolved.

2.13.7 Vulnerability Assessment Report

(1) The Contractor must conduct a vulnerability assessment in accordance with the Vulnerability Assessment Plan.

(2) The Contractor must implement Software Patches and corrective measures as part of this activity. Where this is not feasible (e.g., time to test the Software Patch or determine and test corrective measures would seriously delay the project), the Contractor must create change management tickets for any required Software Patch or corrective measure that cannot be implemented as part of the vulnerability assessment activity. These tickets are to be created in the change management system for the production environment for implementation during the in-service phase of the Contract.

(3) The Contractor must provide Canada with a Vulnerability Assessment Report that contains, at minimum, the following information:

a) a listing of the vulnerability assessment tests that were conducted; and

b) for each vulnerability assessment test:

i) whether a known vulnerability was detected;

ii) a description of the vulnerability;

iii) a description of the Software Patch or corrective measure that was implemented to resolve the vulnerability; and

c) for any unresolved vulnerability:

i) an assessment of the significance of the vulnerability in the context of the JUS HDS Services;

ii) the problem ticket number for the outstanding Software Patch or corrective measure; or

iii) the rationale for not implementing a Software Patch or a corrective measure.

3 ACCEPTANCE OF THE WORK

3.1 Acceptance of Operational Readiness Phase

(1) The Contractor must execute the Work for the Operational Readiness Phase (ORP), according to the Operational Readiness Schedule (ORS) before submitting the Work defined in the ORP for acceptance by Canada. Once the Contractor has successfully completed the Work defined in the ORP, the Contractor must issue an Operational Readiness Completion Notice (ORCN) for the ORP to the Technical Authority by email and provide to Canada an acceptance test report (refer to subsection Acceptance Test Report).

(2) The ORCN must state that the Work has been fully inspected and tested in accordance with the approved ORP.

(3) The Contractor must perform the acceptance of Work for each JUS HDS Service as described in subsection Acceptance of a JUS HDS Service.

(4) The Contractor must only submit the ORCN for the ORP when a Work Completion Notice (WCN) has been submitted by the Contractor and Canada has accepted the Work for the ORP (refer to subsection Operational Readiness Phase) that includes:

a) all identified deliverables (reports, strategies, plans etc.);

b) JUS HDS Services; and

c) Service Delivery Portal (refer to subsection Service Delivery Portal).

3.2 Acceptance of a JUS HDS Service

(1) The Contractor must execute an acceptance test before delivering the Work for acceptance to Canada Contract's Technical Authority. Once the Contractor has successfully completed the acceptance test plan (refer to subsection Acceptance Test Plan), the Contractor must issue a WCN and an acceptance test report to the Technical Authority.

(2) The WCN must state that the Work has been fully inspected and tested in accordance with the approved acceptance test plan.

(3) The Contractor must ensure that the JUS HDS Services is fully functional in accordance with all specifications provided.

3.3 Acceptance Test Plan

(1) The Acceptance Test Plan provided by the Contractor must address:

a) requirements outlined in the SOW;

b) end-to-end functional, usability, accessibility, error, exception and compliance, interoperability and integration testing;

c) Canada witnessing arrangements;

d) tests cases to be performed and for each test case:

i) description, objective, procedure, or scenario;

ii) ordering dependencies on the results of other tests;

iii) environmental requirements;

iv) expected results (i.e., pass/fail criteria);

v) data metrics to be collected and reported; and

vi) how failures will be reported.

3.4 Acceptance Test Report

(1) The Acceptance Test Report provided by the Contractor must contain the following information for each of the test items in the associated acceptance test plan within 5 FGWDs of successfully completing the acceptance testing:

a) the expected results (i.e., pass/fail criteria);
b) the actual results;
c) a description of deviations and how each was resolved;
d) a traceability matrix that describes how each requirement (including reports, data, service levels and documentation) of the Work in the acceptance test plan was tested and validated (i.e. demonstration, documentation, etc); and
e) the Service Level Target testing results.

(2) The Contractor must conduct acceptance testing using a method approved by Canada.

(3) The Contractor must assist Canada with the analysis, isolation and correction of problems detected during Canada's acceptance testing.

3.5 Canada's acceptance process for ORP and a JUS HDS Service

(1) In addition to General Conditions 2035 section 11, Canada's acceptance procedures for a JUS HDS Service also includes the following:

a) Once Canada has received the Work Completion Notice (WCN) for a JUS HDS Services and the acceptance test report Canada will have 15 calendar days to perform its acceptance procedures (the "Acceptance Period"), and if Canada provides notice of any deficiency during the Acceptance Period, the Contractor must address the deficiency at no cost to Canada as soon as possible and notify Canada in writing once the Work is complete, at which time Canada will be entitled to re-inspect the Work and the Acceptance Period will start again from the time that the deficiency is corrected.

4 SERVICE DELIVERY IN STEADY STATE

(1) The requirements in this section are for the delivery of JUS HDS Services following the completion of the ORP.

4.1 Service Operations

4.1.1 Service Manager

(1) The Contractor must provide a Service Manager to meet with Canada's representatives during FGWDs from 08:00 to 17:00 ET and be reachable within 15 minutes of a request using communication methods as approved by Canada, 24 hours per day, 7 days per week, 365 days per year, for:

a) Management Services escalation (Incidents, Change Requests);
b) critical and high priority and Security Incidents;
c) Service Level reviews;
d) release implementation activities;
e) release maintenance and release window scheduling;
f) service quality; and
g) service reporting.

4.1.2 Operations Centre

(1) The Contractor must provide a primary Operations Centre, prior to the completion of the ORP, with the infrastructure and resources required for the centralized management and operation (24 hours per day, 7 days per week, 365 days) of JUS HDS Services.

(2) The Contractor must provide a backup Operations Centre, prior to the completion of operational readiness phase, which is not physically located with the primary Operations Centre (i.e. same building), that provides all operational and management functionality supported by the primary Operations Centre where the transition from the primary Operations Centre to the backup Operations Centre must be transparent to Canada and not impact the operations of JUS HDS Services.

4.1.3 Service Delivery Portal

(1) The Contractor must provide Canada with a Service Delivery Portal that allows:

a) Service Order entry;
b) Service Request entry;
c) Incident entry;
d) access to reports and documents; and
e) other IT service management functions (change, problem, release, configuration, asset and software license management).

(2) The Contractor must allow Canada to create, modify, suspend, terminate, prioritize, search, sort, view and download Service Orders (using a file naming convention specified by Canada and COTS file format).

(3) The format and content of all SDP forms must be approved by Canada.

(4) The Service Delivery Portal must provide an English and a French user interface and must allow the User to select the English or the French user interface at logon to the Service Delivery Portal.

(5) The Service Delivery Portal must include:

a) user interface web page design and layout as approved by Canada;
b) orientation/introduction page, as specified by Canada, with Contractor contact information;

c) online help;

d) assisted data entry where input fields with pre-defined values are populated using lists, drop-down lists, checkboxes and radio buttons in plain language;<TRACEFROMx>SR-169</TRACEFROMx>

e) assisted data entry where input fields with embedded meaning (i.e. multiple data elements concatenated within the same input field) are populated using a combination of lists, drop-down lists, checkboxes and radio buttons in plain language for predefined values and textboxes for User-provided values;<TRACEFROMx>SR-169</TRACEFROMx>

f) error verification where input fields are verified for format and validity, including cross-field validation, with detailed error messages in plain language that indicate to the User what is incorrect and what is the rule(s) that failed;<TRACEFROMx>SR-169</TRACEFROMx>

g) pre-defined fields (e.g. service, Service Delivery Point, work type, contact name, unit pricing, item number, quantities, etc.) approved by Canada, with assisted data entry (where applicable) to minimize error entries;<TRACEFROMx>SR-169</TRACEFROMx>

h) configurable, static and dynamic role-based and policy-based access controls for all functions, objects and data attributes, including but not limited to:

   i) creation;

   ii) modification;

   iii) suspension, where an item is temporarily made unavailable;

   iv) termination, where an item is permanently made unavailable yet retained in the system;

   v) deletion, where an item is removed from the system; and

   vi) view;

i) a least privilege policy for all Accounts as follows:

   i) the access control mechanisms must be configured to implement least privilege, allowing only authorized accesses for Users (and processes acting on their behalf) that are necessary to accomplish assigned tasks;

   ii) non-privileged Accounts must be created for read only access; and

   iii) authorization to privileged Accounts must be restricted to designated Administrators;

j) configurable Account Group settings that allow for:

   i) grouping of Accounts;

   ii) assignment of access controls to the Account Groups; and

   iii) nesting of Account Groups within a larger Account Group;

k) support for the delegation of Administrators and sub-delegation by existing Administrators;

l) secure access as follows:

   i) secure access connection (e.g. Transport Layer Security (TLS));

   ii) minimize the requirement for additional account logins to the various services;

   iii) request the JUS HDS Services unique User ID and password for access;

   iv) enforce a configurable idle session timeout period, as specified by Canada;

m) one-way daily selected Account attribute synchronization from a directory specified by Canada, including but not limited to, the following attributes:

   i) User ID;

   ii) name (first, middle, last);

   iii) address (all address attributes);

   iv) title;

   v) organization (including hierarchy);

   vi) telephone number (all types); and

vii) email address;

n) batch creation of Accounts from a file provided by Canada in COTS file format within 5 FGWDs of a request by Canada;

o) the ability for End Users to perform the following functions:

i) complete registration for a credential, including registering their challenge/response questions;

ii) see a checklist that presents the rules the password must comply with and check these rules positively as they are satisfied as the User chooses or changes their password;

iii) reset their Service Delivery Portal password;

iv) view service history on their Account; and

v) view last logon date and time to the JUS HDS Services;

p) a view for each Client, specified by Canada, that is accessible only by User and Administrator Accounts of the Client, and restricts access to:

i) Client orientation page; and

ii) JUS HDS Services information (e.g.; reports, data, and documents) and administration actions associated with the Client. For example, a Client must only be able to view the Incidents, reports, etc., applicable to the Client;

q) a view of all Clients, that is only accessible by Administrator Accounts (e.g-., the ability to view reports for the entire service);

r) the ability for Administrators to access all JUS HDS Services information (e.g., data, reports, documents) for the last 30 calendar days;

s) the ability for Administrators to schedule the automated email of reports:

i) to configurable distribution lists, as specified by Canada; and

ii) at a date and time, as specified by Canada;

t) the ability for Administrators to create tabular reports that include:

i) selecting available data sources;

ii) specifying selection criteria for the selected fields;

iii) selecting fields to appear on the report;

iv) allowing the User to save the report design with a report name specified by the User; and

v) allowing the User to retrieve the report design by report name;

u) the ability for Administrators to sort tabular report results by any field or multiple fields;

v) the ability for Administrators to download reports with a file naming convention and COTS file format specified by Canada;

w) the ability for Administrators to search and sort documents based on any date range, status (e.g., new, authorized, in progress, completed), and type; and

x) the ability for Administrators to download document search results in compressed format, and file naming convention and COTS file format specified by Canada.

(6) The Contractor must create access profiles (e.g., roles) as requested by Canada within five FGWDs of a request by Canada.

(7) The Contractor must create one or more Service Delivery Portal Accounts and assign a Service Delivery Portal Administrator access profile to the Accounts within five FGWDs of a request by Canada.

(8) The Contractor must transfer JUS HDS Services Management Data throughout the Contract Period electronically (method to be approved by Canada) at a frequency specified by Canada using COTS file format specified by Canada.

(9) The Service Delivery Portal must log all access to the Service Delivery Portal and provide an electronic file of the access log records for the previous 12 months to Canada, on request, in a

file naming convention and COTS file format specified by Canada.

4.2 IT Service Management

(1) The requirements in this section are applicable to all JUS HDS Services, for Contractor provided infrastructure and for Canada provided infrastructure managed by the Contractor as part of a JUS HDS Service, and must be provided prior to the completion of the ORP.

(2) The Contractor must provide Management Services for a JUS HDS Services at no additional cost to Canada.

(3) The Contractor must work co-operatively with Canada and any other third parties (e.g. Shared Services Canada, Network Service Providers, etc.) as requested by Canada to provide Management Services.

4.2.1 Change Management

(1) All Change Requests to the JUS HDS Services Infrastructure must be approved by Canada. <TRACEFROMx>SR-58</TRACEFROMx>

(2) The Contractor must only implement Change Requests from authorized approvers specified by Canada. A Change Request submitted by Canada from an authorized approver is considered approved by Canada. The Contractor must create at least one Change Ticket for each Change Request submitted by Canada within one FGWD of receiving the Change Request.

(3) The Contractor must allow Canada to submit Change Requests 7 days per week, 24 hours per day, 365 days per year (7X24X365):

a) to an email address specified by the Contractor (with an auto reply to confirm receipt of the email); and

b) electronically (with predefined forms and fields approved by Canada) using the Service Delivery Portal.

(4) The Contractor must acknowledge a Change Request to Canada within two) hours of the receipt of a Change Request from Canada.

(5) The Contractor must implement Change Requests, excluding Emergency Changes, during maintenance windows specified by Canada.

(6) The Contractor must categorize and assign Change Requests with a priority level in accordance with a scale specified by Canada. Change Request categorization and priority levels will be determined after contract award.

(7) The Contractor must revise the priority level in a Change Ticket when requested to do so by Canada within one hour of a request from Canada.

(8) The Contractor must escalate Change Requests based on the Change Request categorization (e.g. type, priority level, impact to Canada) and the length of time that the Change Request has remained open. Change Request escalation will be determined after contract award.

(9) The Contractor must escalate Change Requests as requested by Canada.

(10) A Change Ticket must include and maintain at least the following information:

a) Contractor Change Ticket number;

b) Change Request description;

c) related Change Tickets;

d) date and time stamp when Change Request initiated;

e) date and time stamp when Change Request closed;

f) location of change;

g) Change Request category;

h) security category;

i) reason for the change;

j) impact of the change;

k) risks associated with the change;
l) change type;
m) priority level of change;
n) status of change (e.g. open, closed, in progress, suspended, cancelled, etc.);
o) Canada Change Ticket number (if applicable);
p) affected SDPs;
q) Contractor contact (name, telephone number and email address);
r) name of the Contractor resource(s) performing the change;<TRACEFROMx>SR-113</TRACEFROMx>
s) name of the escorts, if applicable;<TRACEFROMx>SR-113</TRACEFROMx>
t) Canada identifier;
u) Canada contact information (name, telephone number and email address);
v) activity log including all actions taken by the Contractor and third parties for the change;
w) related Service Order number, if applicable;
x) scheduled date and time of change;
y) completion date and time of change;
z) originator of the Change Request;
aa) expected outage time (if applicable);
bb) Change Request approver's name; and
cc) back-out procedures and contingency plans.

(11) The Contractor must add, delete and modify Change Ticket information fields as requested by Canada.

(12) The values of the following Change Ticket information fields must be approved by Canada:
a) Change Request category;
b) security category;
c) change type;
d) impact of change;
e) risks associated with the change;
f) priority level of change; and
g) status of change.

(13) The Contractor must minimize the use of incomplete words, sentences and grammar and acronyms in Change Tickets.

(14) The Contractor must automatically update the status of a Change Ticket within 30 minutes of a change in status of the Change Ticket as evidenced by the Change Ticket timestamp.

(15) The Contractor must automatically provide Change Ticket information by email to a pre-defined distribution list for each JUS HDS Services for Change Requests where Canada specifies:
a) Information from the Change Ticket;
b) frequency of email updates;
c) distribution lists; and
d) criteria for selecting Change Requests (e.g. priority level, content of Change Ticket, Emergency Changes).

(16) The Contractor must continue to automatically send email upon updates of Change Requests until the Change Request is closed or Canada cancels the automatic update reporting for the change.

(17) The Contractor must back-out changes, when requested by Canada, using the back-out procedures specified in the Change Ticket that includes:
a) the tasks and activities to return the JUS HDS Services back to its pre-change state;

b) the expected operational results after the back-out has been executed;
c) the criteria to verify that the back-out was successful; and
d) reporting the back-out results in the activity log of the Change Ticket.

(18) The Contractor must provide a Change Request implementation notice to Canada, no later than 48 hours in advance of the implementation of the Change Request.

(19) The Contractor must provide a Change Request cancellation notice to Canada via email, within 24 hours of cancellation of the Change Request by the Contractor.

(20) The Contractor must close the Change Ticket(s) for a Change Request after the Change Request has been accepted by Canada.

(21) The Contractor must provide a Change Request completion notice to Canada within two FGWDs of the completion of any Change Request.

(22) The Contractor must update all relevant documentation and data repositories within 10 FGWDs of the completion of any Change Request.

4.2.2 Incident Management

(1) The Contractor must monitor JUS HDS Services for Incidents.

(2) The Contractor must use other Canada's Service Desk Services or other Service Delivery Portals in order to perform incident notification, incident troubleshooting and/or incident updates/resolutions.

(3) The Contractor must co-operatively work with Canada and any other third parties (e.g. Shared Services Canada, Service Providers, other Federal Government Departments, etc.) as requested by Canada to resolve Incidents.

(4) The Contractor must create one or more Incident Tickets for each Incident detected by the Contractor or reported by Canada.

(5) The Contractor must not include sensitive information in Incident Tickets for Security Incidents as mutually agreed to between Canada and the Contractor.

(6) The Contractor must allow Canada to submit information for an Incident 7 days per week, 24 hours per day, 365 days per year (7X24X365) electronically (with predefined forms and fields approved by Canada) using the Service Delivery Portal.

(7) The Contractor must categorize, assign and escalate Incidents for Incident resolution based on priority level (see Table 6) as specified by Canada.

(8) The Incident escalation will be determined after contract award.

(9) The Contractor must revise the priority level of an Incident when requested to do so by Canada within 15 minutes of the request.

(10) The Contractor must automatically escalate Incidents according to escalation levels and time periods specified by Canada.

(11) The Contractor must provide Canada with an operational escalation matrix and a management escalation matrix that defines the personnel, with alternates (of equal authority) and contains clear contact instructions.

(12) The Contractor must provide Canada with notification of Incidents according to the operational and management escalation matrices.

(13) The Contractor must automatically provide Incident Ticket information by email to a pre-defined distribution list for each JUS HDS Services for Incidents where Canada specifies:<TRACEFROMx>SR-101</TRACEFROMx>

a) information from Incident Ticket;
b) frequency of email updates;
c) distribution lists; and
d) criteria for selecting Incidents.

(14) The Contractor must continue to automatically send email upon updates of Incidents until the

Incident is closed or Canada cancels the automatic update reporting for the Incident.

(15) The Contractor's Incident Tickets must include and maintain, but not be limited to, the following information for all Incidents: <TRACEFROMx>SR-102</TRACEFROMx>

a) Contractor's Incident Number;
b) Incident description;
c) Incident originator contact information (name, telephone number and email address);
d) Incident originator language;
e) related Incident Tickets;
f) date and time stamp when Incident Tickets initiated;
g) date and time stamp when Incident Ticket closed;
h) Incident Ticket type as specified by Canada;
i) Incident priority level;
j) Incident status;
k) Incident escalations;
l) Canada Incident Number (if applicable);
m) Service functions impacted;
n) affected SDPs;
o) Contractor contact (name, telephone number and email address);
p) Client identifier (If applicable);
q) interactions with third parties;
r) activity log;
s) root cause (if available);
t) estimated time for resolution (must be updated every 15 minutes for Critical priority and High priority);
u) resolution description; and
v) outage time (for closed tickets only).

(16) The Contractor must open an Incident Ticket within five minutes of notification for both Contractor-determined and Canada-reported Incidents.<TRACEFROMx>SR-97</TRACEFROMx>

(17) The Contractor must update the Incident within five minutes of a change in status for Critical priority or High priority Incidents and within 15 minutes of a change in status of all other Incident statuses.

(18) The Contractor must document all management and technical escalations for Incidents in the Incident Ticket activity log.

(19) The Contractor must document all interactions with third parties for Incidents in the Incident Ticket activity log.

(20) The Contractor must document all investigation, troubleshooting & analysis details, resolution activities and communications for Incidents in the Incident Ticket activity log.

(21) The Contractor must track and report the outage time of each Incident in the associated Incident Tickets.

(22) The outage time for an Incident must start at the time (start time) that the Incident is detected by the Contractor, or reported to the Contractor by Canada.

(23) The outage time for an Incident must stop at the time that the JUS HDS Services is fully restored for that Incident and Canada has approved the closure of the associated Incident Tickets.

(24) The Contractor must suspend outage time for an Incident at Canada's request or where the Contractor has requested:

a) access to a Service Delivery Point necessary to resolving an Incident and Canada is unable to provide access;

b) information necessary to resolving an Incident and Canada is unable to provide the information, or

c) closure of an Incident Ticket pending Canada's approval, and Canada is not available to consider the request.

(25) The Contractor must request access to a Canada Service Delivery Point when such access is required for an Incident.

(26) The Contractor must restart the outage time for an Incident where the outage time has been suspended, when requested by Canada or when:

a) Service Delivery Point access was required by the Contractor and Canada grants access to the Service Delivery Point;

b) the request for information is provided by Canada to the Contractor; or

c) Canada is available to review the request to close an Incident and has determined that the Incident must remain open.

(27) The Contractor must update the Incident Ticket activity log for an Incident every 30 minutes and within five minutes of a request by Canada.

(28) The Contractor must notify Canada within 15 minutes of the occurrence of an Incident with priority levels as specified by Canada.

(29) If an Incident does not require Service Delivery Point access, where Service Delivery Point access was requested by the Contractor and the outage time for the Incident was suspended, the Contractor must include the suspended outage time in the total outage time for the Incident.

(30) If an Incident Ticket is closed and a subsequent Incident occurs within 24 hours for the same Incident, the Contractor must re-open the original Incident Ticket or open a new Incident Ticket with a cross reference to the previous Incident Ticket and calculate the outage time for the new Incident using the combined outage time of both Incidents.

(31) The Contractor must identify and document the causal factors (root causes) of all Incidents when available.

(32) The Contractor must develop work-arounds to address Incident resolution for Incidents with unidentified root causes. The Contractor must review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing/exercises.

(33) The Contractor must assign a priority level for an Incident as summarized in Table 6.

Table 6: Priority Level Assignment for Incidents

INCIDENT PRIORITY LEVELS		INCIDENT URGENCY LEVEL (Table 8)			
		Critical	High	Medium	Low
INCIDENT IMPACT LEVEL (Table 7)	Extensive	Critical	Critical	High	Low
	Significant	Critical	High	Medium	Low
	Moderate	High	Medium	Medium	Low
	Minor	Medium	Medium	Low	Low

Table 7 - Incident Impact Levels

Incident Impact Levels	
Extensive	Critical business applications & services of Canada are fully affected or reputation is potentially at stake. The business or businesses are unable to achieve their objectives such as satisfying the needs of their clients. The risk to public confidence and/or safety is severe. Several applications are unable to deliver their normal business functionality.
Significant	Critical business applications & services of Canada are partially affected. There is considerable disruption to business activities. The risk to public confidence and/or safety is considerable. An entire application is unable to deliver its normal business functionality.
Moderate	Limited or no impact on the critical business applications & services of Canada. There is some disruption to the business' non-core activities and therefore a reduced productivity of users. There is limited or no actual risk to public confidence and/or safety. The operation of an application is degraded – i.e. not all End Users or End User groups are able to conduct their normal business functions.
Minor	There is no disruption to the critical business applications & services of Canada. There is however minimal to no disruption to non-core business activities. End Users are inconvenienced but can still carry-out the business activity or other business activities. A single or small number of End Users are prevented from conducting their normal business functions.

Table 8 - Incident Urgency Levels

Incident Urgency Levels	
Critical	Severe effect on Canada timely delivery of its services. Extremely time sensitive, harmful to the business or its reputation. The End Users requiring the affected applications are unable to perform their jobs. Many affected End Users are entitled to the Premium Service Level Plan.
High	Considerable effect on Canada timely delivery of its services. Highly time sensitive as the harm to the business or its reputation is likely to occur in a short timeframe. The End Users requiring the affected applications are unable to perform their jobs. One or some affected End Users are entitled to the Premium Service Level Plan.
Medium	Some effect on Canada timely delivery of its services. Sufficient time to allow a response without unreasonably effecting business productivity. Partial loss of critical business functions during normal business hours.
Low	Little or no effect on Canada timely delivery of its services. Normal work can continue until responding.

4.2.3 Problem Management

(1) Problem Management for JUS HDS Services must include integration with the Contractor's Incident Management, Change Management and Configuration Management processes.

(2) The Contractor must pro-actively identify, investigate, diagnose, analyze (trend) and correlate

Incidents for the determination of Problems and Known Errors.

(3) The Contractor must provide resolutions and targeted preventative actions for Problems and Known Errors including, but not limited to:

a) training;

b) recommending procedural or process changes; and

c) creating support documentation.

(4) The Contractor must designate three or more Incidents with the same root cause within a rolling 90 calendar day window as a Problem and open a Problem Ticket within five FGGWDs of the third Incident.

(5) The Contractor must obtain Canada approval to close a Problem Ticket.

(6) The Contractor must not suspend a Problem Ticket.

(7) The Contractor must assign an impact, urgency and priority level to a Problem Ticket as specified by Canada.

(8) The Contractor must link Incidents to existing or new Problems as requested by Canada.

(9) The Contractor must manage Problems through to resolution, ensuring that root cause is established, preventive measures are implemented, and appropriate “clean-up” is done as a result of the Problem.

(10) The Contractor’s Problem Tickets must include and maintain, but not be limited to, the following dedicated information fields for all Problems:

a) Problem Ticket number;

b) Problem description/details;

c) Date and time stamp when Problem Ticket was logged;

d) Problem status;

e) Problem urgency level;

f) Problem impact level;

g) Problem priority level;

h) Related Incidents;

i) End User details;

j) Service details;

k) Equipment details;

l) Details of all diagnostic or attempted recovery actions taken;

m) Problem trend analysis; and

n) Resolution description and root cause.

(11) The Contractor must identify and investigate Known Errors until they are eliminated by the successful implementation of one or more Change Requests.

(12) The Contractor must provide online access to a database of Known Errors in the Service Delivery Portal.

4.2.4 Release Management

(1) The Contractor must integrate its Release Management processes with its Change Management and Configuration Management processes.

(2) The Contractor must implement the software release utilized for a JUS HDS Services as approved by Canada.

(3) The Contractor must implement changes to a release of software (e.g. minor release upgrade, service packs) utilized for a JUS HDS Services within six months of the general commercial availability and as requested by Canada.

(4) The Contractor must not use the production environment of the JUS HDS Services to plan, test the implementation of new and changed software, hardware and documentation for a JUS HDS

Services release not using the production environment of the JUS HDS Services.<TRACEFROMx>SR-64</TRACEFROMx>

(5) The Contractor must implement new and changed software, hardware and documentation for a JUS HDS Services release as approved by Canada.<TRACEFROMx>SR-64</TRACEFROMx>

(6) The Contractor must develop and implement procedures for the distribution, installation, and rollback of changes implemented for a JUS HDS Services release.<TRACEFROMx>SR-64</TRACEFROMx>

(7) The Contractor must coordinate the communications for a JUS HDS Services release to affected Clients and End Users as specified by Canada.

(8) The Contractor must obtain Canada approval for any JUS HDS Services release that may impact the End Users of the JUS HDS Services.

(9) The Contractor must provide Canada with notification of a JUS HDS Services release or upgrade that may impact the End Users of the JUS HDS Services. The notification must be provided a minimum of 30 FGWDs prior to the release or upgrade, and detail the reason for the release or upgrade and summarize the changes.

(10) The Contractor must use Change Requests for all changes implemented by a JUS HDS Services release.

(11) The Contractor must provide JUS HDS Services release information updates by email, to a pre-defined distribution list specified by Canada, until such time as all associated Change Tickets for the Release are closed.

(12) The Contractor must provide a 12-month release plan, within 20 FGWDs of a Canada request that includes the schedule, functionality, and technical characteristics of any planned releases to JUS HDS Services.

(13) The Contractor must implement JUS HDS Services releases during maintenance windows approved by Canada where the timeframe for release activity cannot exceed the pre-approved maintenance windows.

(14) The Contractor must participate in Release Management review meetings conducted by Canada.

(15) The Contractor must ensure that all changes for a JUS HDS Services release are fully tested and staged prior to being implemented.

(16) The Contractor must not use JUS HDS Services in production to test changes for a JUS HDS Services release prior to the release.

(17) The Contractor must ensure that a JUS HDS Services release includes a back-out plan that includes the method of implementation (MOP), how it will be conducted, and the length of time to complete.

(18) The Contractor must update all relevant documentation and data repositories after the implementation of a JUS HDS Services release within 10 FGWDs of the completion of a release.

(19) The Contractor must provide a Post Implementation Report to Canada after each JUS HDS Services release that includes a summary of the release activities and lessons learned.

(20) The Contractor must provide, based on the priority level, an acceptance test plan for a Change Request in the Change Ticket that includes:

a) description of what is to be tested;

b) tasks and activities to verify functional and operational integrity following the change;

c) impacts to the current environment and on the functionality and operation of a JUS HDS Services after the change is implemented;

d) acceptance test schedule, procedures, and expected results;

e) backout procedures to remove the change and restore a JUS HDS Services to its pre-change state if the implementation of the change fails; and

f) acceptance criteria, expected and actual results.

4.2.5 Configuration Management, Asset Management and Software License Management

(1) Configuration Management performed by the Contractor for JUS HDS Services must include the identification, configuration, tracking, programming and implementing of all configuration items, their attributes and their relationships to meet the on-going operational requirements of the JUS HDS Services in accordance with Canada's requirements.

(2) The Configuration Management performed by the Contractor for JUS HDS Services must include processes for:<TRACEFROMx>SR-61</TRACEFROMx>

a) determining the types of changes that are configuration controlled;

b) approving configuration-controlled changes with explicit consideration for security impact analyses;

c) documenting approved configuration-controlled changes;

d) retaining and reviewing records of configuration-controlled changes; and

e) auditing activities associated with configuration-controlled changes.

(3) The Contractor must provide a Configuration Management Database (CMDB) that includes the configuration information and status on all hardware and software Configuration Items for JUS HDS Services.

(4) The Contractor must provide a Definitive Software Library (DSL) to store all authorized software in a location that is protected from unauthorized access, modification and use and allows the performance of software audits.

(5) The Contractor must ensure that only authorized Configuration Items are released and implemented in JUS HDS Services Infrastructure.

(6) The Contractor must ensure that the Change Management process is used for any additions, removals or modifications to Configuration Items of JUS HDS Services.

(7) The Contractor must ensure that the information contained within the CMDB must be automatically synchronized with the Contractor's provisioning process such that any additions, removals or modifications to Configuration Items for JUS HDS Services are reflected in the CMDB within one FGWD of completing any additions, removals or modifications.

(8) The Contractor must ensure that configuration files associated with network configuration for the JUS HDS Services Infrastructure be encrypted in the CMDB.

(9) The Contractor must maintain a distinct and separate configuration baseline for each JUS HDS Services environment (i.e. production, test, etc.).

(10) The Contractor must develop, document, and maintain under configuration control, a current baseline configuration of the JUS HDS Services Infrastructure components and the two previous versions.

(11) The Contractor must log each Configuration Item addition, removal or modification where each log entry in a configuration log file must include:

a) date and time of Configuration Item addition, removal or change; and

b) the unique user identifier of the resource making the addition, removal or change.

(12) The Contractor must provide Canada online access to configuration log files for the previous three years that includes:

a) viewing a configuration log files based on time and date specified by Canada; and

b) downloading configuration log files in a file naming convention as specified by Canada and COTS file format.

(13) The Contractor must archive configuration log data for the Contract Period and provide the archived configuration log data within five FGWDs of a request by Canada, for a specified time period using a file naming convention and COTS format as specified by Canada.

(14) The Contractor must conduct periodic audits of the CMDB against the actual JUS HDS Services and report any discrepancies to Canada, investigate the causes for the discrepancies and provide recommendations to prevent recurrence of the discrepancies within 10 FGWDs of completing the audit.

(15) The Contractor must assist Canada in conducting its own configuration audit of JUS HDS Services. Where Canada configuration audits identify discrepancies between information in the CMDB and actual configuration of the JUS HDS Services, the Contractor must correct those discrepancies, within a timeframe agreed to with Canada, investigate the causes for the discrepancies and provide recommendations to prevent recurrence of the discrepancies within 10 FGWDs of a request by Canada.

(16) The Contractor must manage configuration settings for JUS HDS Services Infrastructure that includes:<TRACEFROMx>SR-67</TRACEFROMx>

a) specifying configuration settings to implement least privilege/functionality;

b) documenting exceptions to configuration settings; and

c) monitoring and controlling changes to the configuration settings in accordance with the Change Management and Configuration Management processes.

(17) The Contractor must develop, document, and maintain an inventory of the JUS HDS Services Infrastructure components that:<TRACEFROMx>SR-71</TRACEFROMx>

a) accurately reflects their current configuration;

b) is at the level of granularity deemed necessary for tracking and reporting;

c) includes enough information to achieve effective property accountability;

d) is available for review and audit by Canada; and

e) is updated as an integral part of component installations, removals, and JUS HDS Services updates.

(18) The Contractor must track and maintain the following IT asset information for assets they are supporting:

a) asset tag number;

b) asset type

c) assignee name (first name, last name, telephone number and email address);

d) location;

e) organization;

f) asset status (e.g. active, on loan, decommissioned, etc.);

g) date of installation;

h) date decommissioned;

i) host name;

j) make;

k) model; and

l) warrantee expiry date.

(19) The Contractor must track and maintain the following Software License information for JUS Supported Software:

a) software title;

b) software version;

c) publisher;

d) number of licenses provided by Canada (purchased software licenses);

e) licence serial numbers

f) number of licenses installed;

g) assets that have the license installed; and

h) maintenance expiry date.

4.3 Meetings

(1) Meetings must be conducted during business hours of 08:00 ET to 17:00 ET on FGWDs in the

National Capital Region.

(2) Meetings will be held in person unless otherwise indicated in the SOW or specified by Canada.

(3) For all meetings unless otherwise indicated in the SOW or specified by Canada, the Contractor will be responsible to develop the agenda, chair the meeting, and record the minutes and action items.

4.3.1 Service Operations Management Meetings - Monthly

(1) Service Operations Management Meetings will be held on a monthly basis with representatives from Canada and the Contractor. The meeting agenda must include:

a) Performance Review: review of the previous month's Service Level Performance Report (refer to subsection Service Level Performance Report);

b) Critical priority Incidents and Problems Review: review of the Root Cause Analysis for any Critical priority Incidents and Problems;

c) Service Request Review: review of the volume and backlog of Service Requests;

d) Change Request Review: review of Change Requests recently completed, and occurring in the upcoming period;

e) Release Review: review of Releases recently completed, and occurring in the upcoming period;

f) Complaints and Issues Review: discussion on any outstanding End User complaints and issues;

g) Accolades Review: review of accolades and recent accomplishments;

h) Service Orders, Task Authorizations, and Contract Amendments Review: review of any current Services Orders, Task Authorizations and Contract Amendments that may be in progress; and

i) Continual Service Improvement Opportunities: discussion on current service delivery and service support processes and possible improvements.

4.3.2 Service Review and Business Planning Meetings - Quarterly

(1) Canada may organize and conduct an executive-level Service Review and Business Planning Meeting on a quarterly basis. The Contractor must attend this meeting at Canada's request. The meeting will include a review of the following elements in relation to the JUS HDS Services:

a) service delivery and service support performance for the preceding quarter;

b) major accomplishments for the preceding quarter;

c) major service delivery and service support issues in the preceding quarter;

d) planned improvements to service delivery and service support in the upcoming quarter; and

e) risks, opportunities, and objectives in the upcoming quarter.

4.3.3 High / Critical / Security Incident Meeting – When Requested

(1) The Contractor must participate in a High, Critical or Security-related Incident Meeting on an "as and when required" basis with Canada. The meeting agenda must cover, at minimum:

a) Date and time of attack, Incident or event;

b) estimated injury level, if applicable;

c) estimated impact level;

d) attack, Incident or event duration;

e) type and description of attack, Incident or event;

f) whether attack appears to have been successful and impact, if applicable;

g) attack scope, if applicable;

h) apparent source/origin of attack, Incident or event;
i) estimated number of systems affected;
j) list of systems affected;
k) chain of events and timeline;
l) actions taken;
m) status of mitigations;
n) references to applicable logs or evidence data; and
o) lessons learned.

4.4 Reporting

(1) The Contractor must define the content and format of reports and documentation in consultation with Canada and is subject to Canada's approval and acceptance before acceptance of the JUS HDS Services.

(2) Unless indicated otherwise, the Contractor must provide reports in English.

(3) All JUS HDS Services reports and documentation produced by the Contractor must be accessible from the Service Delivery Portal unless otherwise indicated by Canada.

4.4.1 Service Level Performance Report – Monthly

(1) The Contractor must provide a Service Level Performance Report which is to be made available to Canada on a monthly basis within five FGWDs of the end of the previous month.

(2) The Contractor must report on the monthly Service Levels achieved for each Service Level Target they are responsible for, including the following information:

a) Service Level Metrics measured for the previous month (an aggregate for the month based for all measurements taken during that month); and
b) Service Level Metric Trends of the monthly aggregated Service Level data for the past 13 months.

(3) The Contractor must report on any missed Service Level Targets, including the information below:

a) date of the missed Service Level Target;
b) description of the missed Service Level Target;
c) calculated Service Level;
d) contracted Service Level; and
e) applicable Service Credits.

4.4.2 Service Operations Status Report – Monthly

(1) The Contractor must provide a monthly Service Operations Status Report to Canada within five FGWDs of the end of the previous month that includes the following:

a) executive summary of Incident activity;
b) executive summary of the Service Request activity;
c) executive summary of Problems, steps taken to resolve, Root Cause Analysis, and recommendations as how to avoid similar Problems in the future;
d) executive summary of Change Request activity;
e) executive summary of Release activity;
f) status and updates of projects;
g) technical accomplishments and plans for the upcoming period;
h) risks including probability and impact, and mitigating actions;
i) recommendations for capacity changes;

j) Service Level and other issues requiring resolution; and

(2) The Contractor must report the details of any Critical priority Incidents that were assigned to them during the period, including:

a) Incident Number;
b) End User name and location;
c) Incident type;
d) Incident description;
e) Incident priority level;
f) hardware and / or software affected;
g) Contractor's Service Representative name;
h) Incident reported date and time;
i) Incident resolution date and time; and
j) Incident resolution.

4.4.3 Billing Report – Monthly

(1) The Contractor must provide a monthly Billing Report to Canada within ten FGWDs of the end of the previous month that includes for the previous 12 months the following:

a) total billing activity, broken down by service and cost centres (primary and secondary) for approved Service Orders; and
b) total billed charges for all approved Service Orders or any other billable event or service.
c) billing disputes requiring resolution.

4.4.4 Professional Services Utilization Report – Monthly

(1) The Contractor must provide a monthly Professional Services Utilization Report to Canada within ten FGWDs of the end of the previous month that includes the following:

a) list of projects involving the use of Professional Services during the period;
b) names and categories of each Professional Services resource that performed work during the period;
c) quantity of the Professional Services days and spending per resource per project;
d) summary of the total amount spent on Professional Services since the start of the contract; and
e) summary of estimated Professional Services days and spending required during the next reporting period.

4.4.5 Service Review and Business Planning Report – Quarterly

(1) When requested, the Contractor must provide a Service Review and Business Planning Report which is to be made available to Canada on an quarterly basis within ten FGWDs of the end of the previous quarter that includes the following:

a) executive summary of the service delivery and service support performance for the preceding quarter;
b) major accomplishments for the preceding quarter;
c) major service delivery and service support issues in the preceding quarter;
d) planned improvements to service delivery and service support in the upcoming quarter; and
e) risks, opportunities, and objectives in the upcoming quarter.

4.4.6 Engineering and Planning Analysis Report - Annually

(1) The Contractor must provide an Engineering and Planning Analysis Report which is to be made available to Canada on an annual basis within 20 FGWDs of the end of the previous 12month period of a fiscal year (April to March) that includes the following for the next 12 months:

a) upcoming Canada requirements;
b) engineering and planning activities;
c) capacity baselines and trends;
d) recommendations on technology innovation and improvements;
e) projected costs; and
f) recommendations for maintaining, improving and optimizing the service.

4.4.7 Security Breach Report – When Requested

(1) When requested by Canada, the Contractor must provide a Security Breach Report, within five FGWDs of a request by Canada, by reporting period specified by Canada, that includes:

a) number of Security Incidents;
b) number of Security Investigations completed;
c) average and highest response time to Security Incidents; and
d) average and highest Security Investigation completion time.

4.4.8 High / Critical / Security Incident Post-Mortem Report – When Requested

(1) The Contractor must provide an Incident Post-Mortem Report for a Security Incident, or a High or Critical priority Incident within 72 hours of a request by Canada, that includes, but is not limited to:

a) Incident number;
b) Incident description;
c) Incident reported date and time;
d) Incident resolution date and time;
e) Incident resolution;
f) chain of events and timeline;
g) actions taken by Contractor;
h) lessons learned;
i) limitations/issues with JUS HDS Services; and
j) recommendations to improve JUS HDS Services.

4.4.9 Change Request Post-Mortem Report – When Requested

(1) The Contractor must provide a Change Request Post-Mortem Report to Canada, within five FGWDs of a request by Canada, for a Change Request that it does not successfully complete that includes the results of the acceptance testing and any recommendations. The report must provide a Root Cause Analysis for the failed Change Request and recommend the actions that are required to avoid re-occurrences.

4.4.10 Asset Management Summary Report –On Demand

(1) The Contractor must provide real time access to an Asset Management Summary Report of the current IT Assets under management by the Contractor. At minimum, the report must include the following:

a) asset tag;
b) asset type;

c) assignee name;
d) location;
e) organization;
f) asset status (e.g. active, on loan, decommissioned, etc.);
g) date of installation;
h) date decommissioned;
i) host name;
j) make;
k) model; and
l) warrantee expiry date.

4.4.11 Software License Management Summary Report – On Demand

(1) The Contractor must provide real time access to a Software License Management Summary Report of the current IT Software licenses under management of the Contractor, within five FGWDs of a request by Canada. At minimum, the report must include the following:

a) software title;
b) software type;
c) software version;
d) publisher;
e) number of licenses provided by Canada (purchased software licenses);
f) number of licenses installed;
g) assets that have the license installed; and
h) maintenance expiry date.

5 CONTINUAL SERVICE IMPROVEMENT

(1) The Contractor must provide continual service improvement processes to maintain the value of the JUS HDS Services for Canada through the continual evaluation and improvement of the quality of JUS HDS Services and the overall maturity of the IT service management lifecycle and underlying processes.

(2) The Contractor's continual service improvement processes must include:

a) the review and analysis of Service Level Agreement (SLA) achievements and results;

b) the review and analysis of data it collects as part of service delivery and transform it in information to identify service gaps, trends and the impact on JUS HDS Services;

c) the review, analysis and recommendation of changes to JUS HDS Services to better align with Canada business objectives which are:

i) reduce costs;

ii) improve service; and

iii) improve security.

d) the review, analysis and recommendation of changes to JUS HDS Services where service improvement opportunities are identified throughout the complete service lifecycle;

e) the review, analysis and recommendation of changes to processes to better harmonize interactions between JUS HDS Services and Canada-provided services;

f) the implementation of individual activities and responsibilities that support improvements in the quality, efficiency and effectiveness of JUS HDS Services;

g) regular scrutiny and review of current JUS HDS Services and processes to drive continual service improvement; and

h) best use of quality management to enable and support continual service improvement.

6 SECURITY AND PRIVACY

6.1 Implementation of Privacy Management Plan

(1) The Contractor must implement the privacy management plan (all processes, procedures, roles, responsibilities, etc.), and any subsequent annual updates, within 60 FGWDs following service acceptance by Canada.

(2) The Contractor must provide to Canada within 40 FGWDs of a request, evidence not older than 12 months (e.g. test results, evaluations, and audits) that the privacy management plan has been implemented correctly, operating as intended, and producing the desired outcomes in meeting Canada's privacy requirements.

(3) If the Contractor determines that it will take more than 40 FGWDs to provide the requested evidence for the privacy management plan, the Contractor must notify Canada within five FGWDs of the original request for evidence, and request an extension, in writing with appropriate justification. Granting an extension is within Canada's sole discretion.

(4) If changes to the JUS HDS Services are anticipated that affect the use, collection, processing, transmission, storage or disposal of Personal Information, or at any time if requested by Canada, the Contractor must provide Canada with sufficient detail to support an update to the privacy impact assessment, and obtain approval from Canada for the anticipated change.

(5) Before the Service Go Live Date, the Contractor agrees to provide one-page awareness training package instructing its employees and consultants regarding the use of the Personal Information provided by Canada about the End Users.

6.2 Implementation of Service Continuity Plan

(1) The Contractor must work in conjunction with Canada to establish national restoration priorities for JUS HDS Services in an order of precedence as specified by Canada.

(2) The Contractor must notify Canada by phone and e-mail within 15 minutes of determining that a disaster or other emergency situation has occurred that affects JUS HDS Services that includes: a brief description, date and time, whicht services are impacted, estimated restore time, and impacted End Users.

(3) The Contractor must restore the JUS HDS Services to a known state after a disruption, compromise, or failure.

(4) The Contractor must implement and test the SCP (all processes, procedures, roles, responsibilities etc) on an annual basis, and provide the test results to Canada within ten FGWDs of completion of the SCPtesting.<TRACEFROMx>SR-88</TRACEFROMx>

(5) The Contractor must correct any problems identified during the testing of the SCP within 60 FGWDs after the test results have been provided to Canada. <TRACEFROMx>SR-88</TRACEFROMx>

(6) The Contractor must provide to Canada within 40 FGWDs of a request, evidence not greater than 12 months old, (e.g. test results, evaluations, and audits, etc.) that the SCPhas been implemented correctly, operating as intended, and producing the desired outcomes in meeting the service continuity requirements for JUS HDS Services. <TRACEFROMx>SR-88</TRACEFROMx>

(7) The Contractor must coordinate the development and testing of the SCPwith the organizational groups, within the Contractor and Canada, responsible for related plans.

(8) The Contractor must conduct capacity planning so that necessary capacity for processing, telecommunications, and environmental support exists during contingency operations.

(9) The Contractor must train its personnel in their contingency roles and responsibilities with respect to the JUS HDS Services, including simulated events to facilitate effective response in crisis situations, and provide refresher training at least annually.

(10) The Contractor must identify potential accessibility problems to the alternate storage site in the event of an area-wide disruption or disaster and outline explicit mitigation actions in the

Contingency Plan.

(11) The Contractor must test the backup data for JUS HDS Services monthly to verify media reliability and data integrity.

(12) The Contractor must use a sample of backup data for JUS HDS Services in the restoration of selected JUS HDS Services functions as part of SCPtesting.

(13) The Contractor must store backup copies of operating system software, critical system software, and component inventory in a separate facility or fire-rated container that is not collocated with the JUS HDS Services Infrastructure.

(14) The Contractor must transfer any backup data within 24 hours of the backup being done to an alternate storage site.

(15) The Contractor must refresh the disk images of JUS HDS Services Infrastructure components from configuration-controlled and integrity-protected disk images.

6.3 Ongoing Security Assessment and Monitoring

(1) The Contractor must maintain the Security Authorization state of the JUS HDS Services through continuous monitoring and annual audit of the implemented security requirements within the JUS HDS Services to determine if the security requirements in the information system continue to be effective over time in light of changes that occur in the JUS HDS Services and its operational environment.<TRACEFROMx>SR-53</TRACEFROMx>

(2) The Contractor must update its Operational Security Procedures as part of authorization maintenance activities within 30 calendar days of a request by Canada. <TRACEFROMx>SR-54</TRACEFROMx>

(3) The Contractor must provide evidence to support authorization maintenance activities, within 30 calendar days of a request by Canada, following all changes to the JUS HDS Services Infrastructure within the Contractor's control. <TRACEFROMx>SR-53</TRACEFROMx>

(4) The Contractor must ensure that the Security Posture of the JUS HDS Services is maintained by continuously: <TRACEFROMx>SR-56</TRACEFROMx>

a) monitoring threats and vulnerabilities;

b) monitoring for malicious activities and unauthorized access; and

c) where required, taking proactive countermeasures, including taking both pre-emptive and response actions to mitigate threats.

(5) The Contractor must run automated vulnerability scanning tools against all JUS HDS Services Infrastructure components on a monthly basis, or as specified by Canada. <TRACEFROMx>SR-140</TRACEFROMx>

(6) The Contractor must allow Canada, or its representatives, to conduct a vulnerability assessment on an annual basis against the JUS HDS Services, within three FGWDs of a request by Canada, that includes: <TRACEFROMx> SR-138</TRACEFROMx>

a) physical access to the JUS HDS Services facilities (i.e. Contractor's facilities where the JUS HDS Services Infrastructure is located);

b) network access(es) to the JUS HDS Services Infrastructure to allow for authenticated and unauthenticated scanning of network components and security appliances, using Canada operated equipment, and Canada specified tools; and

c) assistance for the duration of any on-site portion of the vulnerability assessment of at least one technical resource that is familiar with the technical aspects of the JUS HDS Services Infrastructure (i.e., the hardware, software, and network components, security appliances, and their configuration).

(7) Canada will limit its vulnerability assessment to discovery and scanning activities to JUS HDS Services Infrastructure and will not engage in disruptive or destructive activities.<TRACEFROMx>SR-138</TRACEFROMx>

(8) The Contractor must mitigate all security deficiencies found, at no additional cost to Canada, during:

a) Canada security audits and vulnerability assessments; and

b) the Contractor's own continuous security monitoring and vulnerability assessment activities.

(9) The Contractor must develop a vulnerability mitigation plan approved by Canada within five FGWDs of completion of a vulnerability assessment (conducted by Canada or the Contractor) that includes proposed protection measures to mitigate the identified risks resulting from the vulnerability assessment.

(10) The Contractor must:

a) report any JUS HDS Services security issues to Canada immediately upon learning of their existence;

b) track identified security issues in the JUS HDS Services; and

c) report progress to Canada until each security issue is fixed or mitigated.

(11) The Contractor must produce a vulnerability mitigation report after completion of remediation activities that includes:

a) a description of the corrective measures implemented; and

b) proof that associated system documentation has been updated to reflect the changes.

(12) The Contractor must define and execute the processes for Software Patch management for the JUS HDS Services Infrastructure components that includes:

a) ensuring the latest version of applications and operating systems are used;

b) ensuring that vulnerabilities are evaluated and vendor-supplied security Software Patches are applied in a timely manner;

c) prioritizing critical Software Patches using a risk-based approach;

d) taking applications offline and bringing them back online;

e) aligning criticality levels for Software Patches as specified by Canada;

f) rating of vulnerabilities against CVSS v2; and

g) testing and verification methodology to ensure that the Software Patches have been implemented properly.

6.4 Investigation of Complaints and Access to Information Requests

(1) The Contractor must exercise, during the entire Contract Period, processes and controls that preserve the integrity, privacy and accuracy of all information and data and metadata, irrespective of format and in their possession or under their care or control which information and data is generated by, acquired pursuant to or in any other way arises out of their responsibilities and obligations under the Contract in order to ensure that the information and data can be used as persuasive evidence in a court of law.

(2) The Contractor must, to the extent it is permitted by law, fully cooperate with Canada and assist Canada in the investigation of complaints, regulatory or criminal investigations and prosecutions both regulatory and criminal and access to information requests that includes allowing security audits/inspections and furnishing requested information (e.g. documentation, data protection description, data architecture and security descriptions) as may be required by Canada within five (5) FGWDs of a request by Canada.

7 SERVICE LEVEL TARGETS

(1) The Contractor must meet or exceed the Service Levels Target (SLT requirements in this section for JUS HDS Services following acceptance of the JUS HDS Services by Canada.

(2) The Contractor must provide the hardware andr software for monitoring and measuring SLTs.

(3) The Contractor must count omitted SLT performance measurements as failed measurements.

7.1 Service Delivery Portal - Maximum Service Outage Time

7.1.1 Definition

(1) The Service Level Target Service Delivery Portal Maximum Service Outage Time (SLT-SDP-MSOT) is the SLT for the maximum accumulated outage time for the Service Delivery Portal allowed in any calendar month (can be used to calculate service availability).

7.1.2 Value

(1) The SLT-SDP-MSOT must have an accumulated outage time in any calendar month less than or equal to 45 minutes (equates to approximately 99.50% availability).

7.1.3 Method

(1) The SLT-SDP-MSOT Service Credit Period is 7 days per week, 24 hours per day and 365 days per year.

(2) The Contractor must calculate SLT-SDP-MSOT for the Service Delivery Portal by summing the outage time for all Critical Priority and High Priority Incidents (refer to subsection Incident Management) related to the Service Delivery Portal for that calendar month.

(3) The outage time from the following events must be excluded from the calculation of the SLT-SDP-MSOT:

a) failure of a service or system that is not provided by the Contractor.

7.2 Service Delivery Portal - Maximum Time to Restore Service

7.2.1 Definition

(1) The Service Level Target Service Delivery Portal Maximum Time to Restore Service (SLT-SDP-MTRS) is the SLT for the maximum continuous time period to restore the Service Delivery Portal to complete operational status following an Incident for which SLT-SDP-MTRS is calculated (service outage).

7.2.2 Value

(1) The SLT-SDP-MTRS must have a maximum restore time of 4.0 continuous hours.

7.2.3 Method

(1) The SLT-SDP-MTRS Service Credit Period is 7 days per week, 24 hours per day and 365 days per year.

(2) The calculation of SLT-SDP-MTRS begins from the time at which a Critical Priority or a High Priority Incident for the Service Delivery Portal is reported by Canada, or is detected by the Contractor, until the time that the Incident is closed.

7.3 JUS Service Desk Service - Maximum Time to Answer

7.3.1 Definition

(1) The Service Level Target Service Desk Maximum Time to Answer (SLT-SD-MTA) is the SLT for the maximum amount of time for the Service Desk Service to answer telephone calls.

7.3.2 Value

(1) The SLT-SD-MTA must be less than or equal to 45 seconds, 95% of the time.

7.3.3 Method

(1) The SLT-SD-MTA Service Credit Period is 6:00 ET to 21:00 ET during FGWDs.

(2) The SLT-SD-MTA must meet or exceed 95% of all telephone calls received by the JUS Service Desk Service in a calendar month.

(3) The SLT-SD-MTA must be calculated as follows:

(number of calls answered within service level seconds + number of calls abandoned) / (total number of calls answered + total number of abandoned calls) * 100

(4) The calculation of the time to answer a call starts from the time the telephone call is connected to the Contractor's telephone system and ends when the Contractor's JUS Service Desk Agent answers the call.

7.4 JUS Service Desk Service - Maximum Time on Hold

7.4.1 Definition

(1) The Service Level Target Service Desk Maximum Time on Hold (SLT-SD-MTOH) is the SLT for the maximum amount of time for the JUS Service Desk Service to put a telephone call from an End User on hold or to respond to an End User Web-Chat communication.

7.4.2 Value

(1) The SLT-SD-MTOH must be less than or equal to 2 minutes, 95% of the time.

7.4.3 Method

(1) The SLT-SD-MTOH Service Credit Period is 6:00 ET to 21:00 ET during FGWDs.

(2) The SLT-SD-MTOH must meet or exceed 95% of all telephone calls and all Web-Chat communications received by the JUS Service Desk Service from an End User in a calendar month.

(3) The SLT-SD- MTOH must be calculated as follows:

(number of calls on hold from End Users within service level minutes + calls from End Users without hold time + calls abandoned + number of Web-Chat communications responded to within service level minutes) / (total calls + total number of Web-Chat communications received) * 100

(4) The calculation of the time on hold for telephone calls starts from the time the telephone call is put on hold and ends when the Contractor's JUS Service Desk Agent takes the call off hold.

(5) The calculation of the time on hold for Web-Chat communications starts from the time a Web-Chat communication is received from an End User and ends when the Contractor's JUS Service Desk Agent responds to the End User.

7.5 JUS Service Desk Service - Maximum Time to Escalate - Standard

7.5.1 Definition

(1) The Service Level Target Service Desk Maximum Time to Escalate (Standard) (SLT-SD-MTTE-1) is the SLT for the maximum amount of time that the JUS Service Desk Service can work on an Low or Medium Priority Incident Ticket before escalating to a Level 2 or Level 3 Support representative for an End User assigned to the Standard Service Level Plan.

7.5.2 Value

(1) The SLT-SD-MTTE-1 must be less than or equal to 30 minutes, 95% of the time.

7.5.3 Method

(1) The SLT-SD-MTTE-1 Service Credit Period is 6:00 ET to 21:00 ET during FGWDs.

(2) The SLT-SD-MTTE-1 must meet or exceed 95% of all telephone calls received by the JUS Service Desk Service from an End User assigned to the Standard Service Level Plan in a calendar month.

(3) The SLT-SD-MTTE-1 must be calculated as follows:

(number of Low or Medium Priority calls from Standard Service Level Plan End Users escalated within service level minutes + number of calls from Standard Service Level Plan End Users resolved by Level 1 within service level minutes) / (total calls from Standard Service Level Plan End Users) * 100

(4) The calculation of the time to escalate a call starts from the time the telephone call is answered by the Contractor's JUS Service Desk Agent and ends when the Incident Ticket is either resolved, or escalated to a Level 2 or Level 3 Support representative.

7.6 JUS Service Desk Service - Maximum Time to Escalate - Premium

7.6.1 Definition

(1) The Service Level Target Service Desk Maximum Time to Escalate (Premium) (SLT-SD-MTTE-2) is the SLT for the maximum amount of time that the JUS Service Desk Service can work on an High or Critical Priority Incident Ticket for an End User assigned to the Standard Service Level Plan or on an Incident Ticket for an End User assigned to the Premium Service Level Plan before escalating to a Level 2 or Level 3 Support Representative.

7.6.2 Value

(1) The SLT-SD-MTTE-2 must be less than or equal to 15 minutes, 95% of the time.

7.6.3 Method

(1) The SLT-SD-MTTE-2 Service Credit Period is 6:00 ET to 21:00 ET during FGWDs.

(2) The SLT-SD-MTTE-2 must meet or exceed 95% of all telephone calls received by the JUS Service Desk Service from an End User assigned to the Premium Service Level Plan in a calendar month.

(3) The SLT-SD-MTTE-2 must be calculated as follows:

(number of calls from Standard Service Level Plan End Users with High or Critical Priority escalated within service level minutes + number of calls from Premium Service Level Plan End Users escalated within service level minutes + number of calls from Premium Service Level Plan End Users resolved by Level 1 within service level minutes) / (number of calls from Standard Service Level Plan End Users with High or Critical Priority + total calls from Premium Service Level Plan End Users) * 100

(4) The calculation of the time to escalate a call starts from the time the telephone call is answered by the Contractor's JUS Service Desk Agent and ends when the Incident Ticket is either closed, or escalated to a Level 2 or Level 3 Support representative.

7.7 JUS Service Desk Service - Maximum Time to Respond to Alternate Service Channel Incidents

7.7.1 Definition

(1) The Service Level Target Service Desk Maximum Time to Respond to Alternate Service Channel Incidents (SLT-SD-MTRASCI) is the SLT for the maximum amount of time for the JUS Service Desk Service to respond to voice-mail, email and Service Delivery Portal Self Service Incidents from an End User.

7.7.2 Value

(1) The SLT-SD-MTRASCI must be less than or equal to 30 minutes, 95% of the time.

7.7.3 Method

(1) The SLT-SD-MTRASCI Service Credit Period is:

a) 6:00 ET to 21:00 ET during FGWDs for emails and Self Service Incidents; and

b) 7 days per week, 24 hours per day and 365 days per year for voice-mail Incidents.

(2) The SLT-SD-MTRASCI must meet or exceed 95% of all voice-mail, emails and Self Service Incidents from an End User received by the JUS Service Desk Service in a calendar month.

(3) The SLT-SD-MTRASCI must be calculated as follows:

(number of voice-mail, emails and Self Service Incidents from End Users responded to within service level minutes) / (total number of voice-mail, emails and Self Service Incidents from End Users) * 100

(4) The calculation of the time to respond to the Alternate Service Channel starts from the time the voice-mail or email is received by the Contractor or the time the Self Service Incident is created and ends when the JUS Service Desk Service calls the End User.

7.8 JUS Service Desk Service – Minimum Level 1 Resolution Rate for Resolvable Incidents

7.8.1 Definition

(1) The Service Level Target Service Desk Minimum Level 1 Resolution Rate (SLT-SD-ML1RR) is the SLT for the minimum resolution rate for Incident Tickets to be resolved by the JUS Service Desk Service.

7.8.2 Value

(1) The SLT-SD-ML1RR must have a minimum resolution rate of 85% of all Resolvable Incidents.

7.8.3 Method

(1) A Resolvable Incident is an Incident that can be resolved using troubleshooting scripts or the desktop management tool (i.e. does not require physical access to the device).

(2) Canada and the Contractor must mutually agree upon the specific categorization of Incident Tickets and whether or not such tickets will be included within the Resolvable Incident definition for SLT-SD-ML1RR calculation.

(3) The SLT-SD-ML1RR must meet or exceed 85% of all Resolvable Incidents received by the JUS Service Desk Service in a calendar month.

(4) The SLT-SD-ML1RR must be calculated as follows:

(number of Resolvable Incidents that are resolved by JUS Service Desk Service) / (total number of Resolvable Incidents) * 100

7.9 JUS Service Desk Service – Minimum End User Satisfaction Rate

7.9.1 Definition

(1) The Service Level Target Minimum End User Satisfaction Rate (SLT-SD-MEUSR) is the SLT for the average score of Customer Satisfaction Measurement Surveys returned by End Users for Incident or Service Request they make with the JUS Service Desk Service, with the exception that any individual End User will not be surveyed if he/she has completed a Customer Satisfaction Measurement Survey for another contact within a 30 day period.

7.9.2 Value

(1) The SLT-SD-MEUSR must have a score value set in the table below according to the respective period.

(2) Table 9: End User Satisfaction Indicator

TIME PERIOD	SERVICE LEVEL
Months 1 – 4 following the Service Go Live Date	Average score not less than 3.0
Months 5 – 18 following the Service Go Live Date	Average score not less than 3.3
Month 19 following the Service Go Live Date and thereafter	Average score not less than 3.6
All times following the Service Go Live Date	Score of 1.0 or less must not be recorded on more than 3% of the surveys returned

7.9.3 Method

(1) The SLT-SD-MEUSR is based on an average score of Customer Satisfaction Measurement Surveys returned and on a scale of 1.0 to 5.0

(2) The average score is measured monthly based on all Incidents and Service Requests Tickets received by the JUS Service Desk Service in a calendar month.

(3) Customer Satisfaction Measurement Survey responses received after 30 calendar days will not be included in response measurement

7.10 Escalated Support - Maximum Time to Respond to Incident - Standard

7.10.1 Definition

(1) The Service Level Target Escalated Support Maximum Time to Respond to Incident (Standard) (SLT-ES-MTTRTI-1) is the SLT for the maximum amount of time for the JUS On-Site Support Service and the JUS Desktop Engineering Service to respond to a Low or Medium Priority Incident Ticket from a Standard Service Level Plan End User once it has been assigned to them.

7.10.2 Value

(1) The SLT-ES-MTTRTI-1 must be less than or equal to 4 hours from Incident Ticket assignment, 95% of the time.

7.10.3 Method

(1) The SLT-ES-MTTRTI-1 Service Credit Period is 7:00 ET to 18:00 ET during FGWDs for the JUS On-Site Support Service.

(2) The SLT-ES-MTTRTI-1 Service Credit Period is 8:00 ET to 17:00 ET during FGWDs for the JUS Desktop Engineering Service.

(3) The SLT-ES-MTTRTI-1 must meet or exceed the service level for 95% of all Low or Medium Priority Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from an End User assigned to the Standard Service Level Plan in a calendar month.

(4) The SLT-ES-MTTRTI-1 must be calculated as follows:

(number of Low or Medium Priority Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from Standard Service Level Plan End Users responded within the service level hours) / (total number of Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from Standard Service Level Plan End Users) * 100

(5) The calculation of the time starts when the Incident Ticket is assigned to the JUS On-Site Support Service and the JUS Desktop Engineering Service and ends at the time they start resolving the Incident Ticket with the End User.

7.11 Escalated Support - Maximum Time to Respond to Incident - Premium

7.11.1 Definition

(1) The Service Level Target On-Site Support Maximum Time to Respond to Incident (Premium) (SLT-ES-MTTRTI-2) is the service level target for the maximum amount of time for the JUS On-Site Support Service and the JUS Desktop Engineering Service to respond to a High or Critical Priority Incident Ticket from a Standard Service Level Plan End User or an Incident Ticket from a Premium Service Level Plan End User once it has been assigned to them.

7.11.2 Value

(1) The SLT-ES-MTTRTI-2 must be less than or equal to 2 hours from Incident Ticket assignment, 95% of the time.

7.11.3 Method

(1) The SLT-ES-MTTRTI-2 Service Credit Period is 7:00 ET to 18:00 ET during FGWDs for the JUS On-Site Support Service.

(2) The SLT-ES-MTTRTI-2 Service Credit Period is 8:00 ET to 17:00 ET during FGWDs for the JUS Desktop Engineering Service.

(3) The SLT-ES-MTTRTI-2 must meet or exceed the service level for 95% of all Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from an End User assigned to the Standard Service Level Plan with High or Critical Priority Incident Ticket and an End User assigned to the Premium Service Level Plan in a calendar month.

(4) The SLT-ES-MTTRTI-2 must be calculated as follows:

(number of Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from Standard Service Level Plan End User with High or Critical Priority Incident Ticket and Premium Service Level Plan End Users responded within the service level) / (total number of Incident Tickets received by the JUS On-Site Support Service and the JUS

Desktop Engineering Service from Standard Service Level Plan End User with High or Critical Priority Incident Ticket and Premium Service Level Plan End Users) * 100

(5) The calculation of the time starts when the Incident Ticket is assigned to the JUS On-Site Support Service and the JUS Desktop Engineering Service and ends at the time they start resolving the Incident Ticket with the End User.

7.12 Escalated Support - Maximum Time to Resolve from Incident - Standard

7.12.1 Definition

(1) The Service Level Target On-Site Support Maximum Time to Resolve from Incident (Standard) (SLT-ES-MTTRFI-1) is the SLT for the maximum amount of time for the JUS On-Site Support Service and the JUS Desktop Engineering Service to resolve an Incident Ticket from a Standard Service Level Plan End User once it has been assigned to them.

7.12.2 Value

(1) The SLT-ES-MTTRFI-1 must be less than or equal to 8 hours from Incident Ticket assignment, 95% of the time.

7.12.3 Method

(1) The SLT- ES-MTTRFI-1 Service Credit Period is 7:00 ET to 18:00 ET during FGWDs for the JUS On-Site Support Service.

(2) The SLT- ES-MTTRFI-1 Service Credit Period is 8:00 ET to 17:00 ET during FGWDs for the JUS Desktop Engineering Service.

(3) The SLT- ES-MTTRFI-1 must meet or exceed the service level for 95% of all Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from an End User assigned to the Standard Service Level Plan in a calendar month.

(4) The SLT- ES-MTTRFI-1 must be calculated as follows:

(number of Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from Standard Service Level Plan End Users resolved within the service level hours) / (total number of Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from Standard Service Level End Users) * 100

(5) The calculation of the time starts when the Incident Ticket is assigned to the JUS On-Site Support Service and the JUS Desktop Engineering Service and ends at the time they either resolve the Incident Ticket, or re-assign it to another JUS On-Site Support Service or JUS Desktop Engineering Service representative.

7.13 Escalated Support - Maximum Time to Resolve from Incident - Premium

7.13.1 Definition

(1) The Service Level Target On-Site Support Maximum Time to Resolve from Incident (Premium) (SLT-ES-MTTRFI-2) is the SLT for the maximum amount of time for the JUS On-Site Support Service and the JUS Desktop Engineering Service to resolve an Incident Ticket from a Premium Service Level Plan End User once it has been assigned to them.

7.13.2 Value

(1) The SLT-ES-MTTRFI-2 must be less than or equal to 4 hours from Incident Ticket assignment, 95% of the time.

7.13.3 Method

(1) The SLT- ES-MTTRFI-2 Service Credit Period is 7:00 ET to 18:00 ET during FGWDs for the JUS On-Site Support Service.

(2) The SLT- ES-MTTRFI-2 Service Credit Period is 8:00 ET to 17:00 ET during FGWDs for the JUS Desktop Engineering Service.

(3) The SLT-ES-MTTRFI-2 must meet or exceed the service level for 95% of all Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from an End User assigned to the Premium Service Level Plan in a calendar month.

(4) The SLT-ES-MTTRFI-2 must be calculated as follows:

(number of Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from Premium Service Level Plan End Users resolved within the service level hours) / (total number of Incident Tickets received by the JUS On-Site Support Service and the JUS Desktop Engineering Service from Premium Service Level Plan End Users) * 100

(5) The calculation of the time starts when the Incident Ticket is assigned to the JUS On-Site Support Service and the JUS Desktop Engineering Service and ends at the time they either resolve the Incident Ticket, or re-assign it to another JUS On-Site Support Service or JUS Desktop Engineering Service representative.

7.14 Escalated Support – Maximum Time to Deploy Critical Security Update

7.14.1 Definition

(1) The Service Level Target Engineering Support Maximum Time to Deploy Critical Security Update (SLT-ES-MTDCSU) is the SLT for the maximum amount of time for the JUS On-Site Support Service and / or the JUS Desktop Engineering Service to deploy a critical security update to all affected JUS supported Hardware and JUS supported Software.

7.14.2 Value

(2) The SLT-ES-MTDCSU must be less than or equal to five FGWDs.

7.14.3 Method

(1) The SLT-ES-MTDCSU Service Credit Period is 07:00 ET to 18:00 ET during FGWDs.

(2) The calculation of SLT-ES-MTDCSU begins from the time at which a Critical Security Update requirement has been identified by Canada or the Contractor, and ends when the Critical Security Update has been deployed to all affected JUS supported Hardware and JUS supported Software.

7.15 Service Request – Maximum Time to Fulfil

7.15.1 Definition

(1) The Service Level Target Service Request Fulfilment (SLT-SRF) is the SLT for the percentage of Service Requests that must be completed within their Maximum Fulfilment Time Target. The SLT-SRF must be calculated for each JUS HDS Services (e.g. JUS Service Desk Service, JUS On-Site Support Service and JUS Desktop Engineering Service).

7.15.2 Value

(1) The SLT-SRF is that 95% of the Service Requests for that Service must be completed within the Maximum Fulfilment Time Target. The Maximum Fulfilment Time Targets are specified in Table 10 below.

Table 10: Service Request Maximum Fulfillment Time Targets

JUS HDS SERVICES	SERVICE REQUEST TYPE	SERVICE LEVEL PLAN	MAXIMUM FULFILLMENT TIME TARGET
JUS Service Desk Service	End User account management (add, modify, remove, change permissions) for Active Directory accounts on Canada LAN using Active Directory native administration functions or another Active Directory administration tool that could be provided by Canada	Standard and Premium	1 FGWD
JUS Service Desk Service	Administrator Account management (add, modify, remove, change permissions) for the Service Delivery Portal	Standard and Premium	1 FGWD
JUS Service Desk Service	Print queue management (add, modify, remove, change permissions, change properties) on Canada LAN	Standard and Premium	1 FGWD
JUS Service Desk Service	Remote Installation/Removal of Software Packages	Standard	2 FGWDs
JUS Service Desk Service	Remote Installation/Removal of Software Packages	Premium	1 FGWD
JUS Service Desk Service	Add, modify, remove, change email distribution list	Standard and Premium	1 FGWD
JUS Service Desk Service	Network storage access management privileges (add, modify, remove, change) on Canada LAN	Standard and Premium	1 FGWD
JUS On-Site Support Service	a. Install, move, add, change or remove Hardware and Software as per Appendix C: Standard Hardware and Software (for 1 to 6 End Users) b. For moves, End Users must be moving in the same building (no need to go outside to move equipment).	Standard	5 FGWDs
JUS On-Site Support Service	a. Install, move, add, change or remove Hardware and Software as per Appendix C: Standard Hardware and Software (for 1 to 6 End	Premium	2 FGWDs

JUS HDS SERVICES	SERVICE REQUEST TYPE	SERVICE LEVEL PLAN	MAXIMUM FULFILLMENT TIME TARGET
	Users) b. For moves, End Users must be moving in the same building (no need to go outside to move equipment).		
JUS On-Site Support Service	a. Install, move, add, change or remove Hardware and Software as per Appendix C: Standard Hardware and Software (for 1 End User) b. Canada can request up to a maximum of 20 Rush Service Requests per month.	Rush	4 hours
JUS On-Site Support Service	a. Install or remove non-standard Hardware or Software as approved by Canada. b. Note: if possible, Software Service Request must be completed remotely by JUS Desktop Engineering Service.	Standard	5 FGWDs
JUS On-Site Support Service	a. Install or remove not-standard Hardware or Software as approved by Canada. b. Note: if possible, Software Service Request must be completed remotely by JUS Desktop Engineering Service.	Premium	1 FGWD
JUS On-Site Support Service	Set-up and Tear-down for multimedia requests for special events.	Standard and Premium	1 FGWD
JUS Desktop Engineering Service	Package Software for deployment	N/A	15 FGWDs
JUS Desktop Engineering Service	Package business application for deployment	N/A	15 FGWDs
JUS Desktop Engineering Service	Create new OS Image and package it for deployment	N/A	15 FGWDs

JUS HDS SERVICES	SERVICE REQUEST TYPE	SERVICE LEVEL PLAN	MAXIMUM FULFILLMENT TIME TARGET
JUS Desktop Engineering Service	Create new OS Image version and package it for deployment	N/A	30 FGWDs

7.15.3 Method

(1) The SLT-SRF Service Credit Period is 07:00 ET to 18:00 ET during FGWD within a calendar month.

(2) The SLT-SRF must be calculated for each Service Request as follows:

(number of Service Requests that were completed within the Maximum Fulfillment Time Target for the calendar month / (number of Service Requests that should have been completed within the Maximum Fulfillment Time Target for the calendar month or 700, whichever is lesser)) * 100

(3) The calculation of the time starts when the Service Request is assigned to the JUS HDS Services and ends at the time the Contractor fulfils the Service Request.

8 SUPPORTED HARDWARE AND SOFTWARE

(1) The JUS HDS Services must provide support for all future components added by Canada to Appendix C: Standard Hardware and Software.

(2) The Contractor must agree that:

a) Canada reserves the right to add, modify or remove the Hardware and Software listed in Appendix C: Standard Hardware and Software from time to time as Canada sees fit;

b) Canada will provide 10 calendar days notice to the Contractor of changes to Appendix C: Standard Hardware and Software; and

c) after expiry of the 10-day notice period, components acquired by Canada and added to the Appendix C: Standard Hardware and Software will be subject to all other provisions of this Contract.

9 STANDARDS

(1) All Work performed by the Contractor must conform to all applicable standards and codes as listed in this subsection and remain current with any revisions and/or changes.

(2) The Standards applicable to a JUS HDS Services are referenced in the applicable SOW section for the JUS HDS Services. In cases where a conflict or discrepancy exists between Standards, Canada will advise the Contractor as to which Standard applies.

9.1 Internet Protocol

(1) The following standards and functionality apply to the Internet Protocol (IP):

a) [RFC 791]: IPV4; and

b) [RFC 2460]: IPV6 where upon requested by Canada, the Contractor must implement Internet Protocol v6 (IPv6) for JUS HDS Services at no additional cost to Canada, within six months of a request by Canada.

9.2 Directory

(1) The following standards and functionality apply to Directory:

a) RFC4511: Lightweight Directory Access Protocol (LDAP); and

b) RFC4422: Simple Authentication and Security Layer (SASL).

9.3 Web Session Security

(1) The following standards apply to Web Session Security:

a) Transport Layer Security (TLS) Protocol Version 1.1; and

b) Transport Layer Security (TLS) Protocol Version 1.2.

9.4 Markup Language and Web Access

(1) The following standards and policies apply to markup language:

a) Extensible Markup Language (XML) (refer to: http://www.w3.org/XML/).

9.5 Accessibility

(1) The following guidelines, standards and policies apply to the accessibility of the Service Delivery Portal:

a) Section 508 of Industry Canada's "Accessible Procurement Toolkit", refer to:

http://www.apt.gc.ca/ap11120E.asp?pId=436

b) Treasury Board Secretariat's Standard on Web Accessibility, refer to:

http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=23601&section=text

c) w3c's Web Content Accessibility Guidelines 2.0 at a double A level of conformance, refer to:

http://www.w3.org/TR/WCAG/

d) Policy on the Duty to Accommodate Persons with Disabilities in the Federal Public Service, refer to: http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12541&section=text

e) Web Experience Toolkit Guideline (for Self Service portal) - http://www.tbs-sct.gc.ca/ws-nw/index-eng.asp

9.6 Security

(1) The following security policies must be adhered to:

a) Policy on Government Security:
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=16578&section=text

b) Policy on Management of Information Technology:
http://www.tbs-sct.gc.ca/pol/doc-eng.aspx?id=12755

10 PROFESSIONAL SERVICES

(1) The Contractor must provide resources to Canada, in any Canadian city, in accordance with a validly issued Task Authorization, in the following categories:

a) Project Manager;
b) Technology Architect;
c) Security Specialist;
d) Business Analyst;
e) On-Site Services Representative; and
f) On-Site Services Team Leader.

(2) Location of the Work, security clearance and language requirements for resources will be specified at the time the Task Authorization is completed.

10.1 Project Manager

(1) The Service Catalogue Item (SCI):Project Manager must:

a) manage projects initiated by Canada that require the tailoring of one or more JUS HDS Services, by ensuring that resources are made available for the required Work and that the service(s) is (are) fully operational within the required timeframe, budget, and performance parameters;
b) develop a project charter;
c) develop and maintain a comprehensive project schedule showing all Work Breakdown Structure (WBS) activities, dependencies, durations, milestones, deliverables, phases and the critical path;
d) determine budgetary requirements;
e) develop a resource plan;
f) develop a risk management plan;
g) meet in conference with stakeholders and other project managers to clearly identify issues impeding the progress of the project;
h) formulate statements of issues impeding the progress of the requested project, establish procedures for the development and implementation of significant, new or modified project elements to solve these issues, and obtain approval thereof;
i) prepare plans, charts, tables and diagrams to assist in analyzing or displaying problems; work with a variety of project management tools;
j) identify and propose mitigation of risks;
k) report progress of the project on an ongoing basis and at scheduled points in its life cycle;
l) produce appropriate reports and dashboards, and identify scheduling and/or dependency issues; and
m) conduct project briefings for Canada management.

10.2 Technology Architect

(1) The SCI:Technology Architect must :

a) provide advice, recommendations, and support as may be required concerning issues and new requirements related to JUS HDS Services, including solution integration, migration to a new O/S Platform, image engineering, Software distribution, and Software Patch management;
b) analyze existing capabilities and requirements of JUS components, develop redesigned frameworks and recommend areas for improved capability and integration;
c) develop specifications and technical designs for the tailored JUS HDS Services' architecture, based on the business and functional requirements of the TA and its

integration with existing GC solutions;

d) recommend, and incorporate into the statement of requirements, finalized specifications and technical designs that will deliver the functionality required by the TA;

e) with an implementation team, implement and integrate the developed technical JUS architecture; and

f) advise when upgrades of the JUS HDS Services platform should take place.

10.3 Security Specialist

(1) The SCI:Security Specialist must:

a) perform IT Security Assessments of IT systems;

b) conduct reviews of backup and recovery plans;

c) review existing security policies, standards, guidelines and procedures and providing advice as to their appropriateness and effectiveness;

d) develop a security design document with recommended security safeguards;

e) document security services processes;

f) conduct compliance audits of IT operations, application systems and infrastructure.

g) conduct security threat and risk assessments of IT facilities, application systems and communications;

h) design the security framework and implement the security components of the JUS HDS Services Infrastructure required to protect assets and to support application systems;

i) produce operational security requirements and traceability matrices as requested in the TA;

j) develop and/or enforce IT security policies, GC security standards (e.g. Management of Information Technology Security), guidelines and procedures on the security aspects of applicable IT services;

k) investigate Security Incidents and report the cause and related weaknesses of the JUS HDS Services, and recommend solutions; and

l) prepare other technical reports, such as a network vulnerability assessment, requirement analysis, and options analysis report.

10.4 Business Analyst

(1) The SCI:Business Analyst must:

a) document business process requirements;

b) perform analysis of business process requirements involving business service improvement, and identify functional requirements, procedures, and decision flows;

c) identify any risks that would impede the progress of implementing the functional requirements or affect existing business processes, and recommend strategies to mitigate them;

d) define and document interfaces of manual to automated operations within application subsystems, to external systems, and between new and existing systems;

e) identify business processes for re-design, prototype potential solutions, provide trade-off information and suggest a recommended course of action;

f) establish acceptance test criteria; and

g) brief Project Manager on the modified business architecture, as well as any emerging business and technology trends.

10.5 On-Site Services Representative

(1) The SCI: On-Site Services Representative must:

a) provide first and second level support for Incidents and complete Service Requests, including new Installations and Upgrades for a wide range of Hardware, Software, peripherals and applications;
b) provide advice on the operations and functionality of various applications, printers, and systems;
c) diagnose and resolve, desktop configuration and Software issues;
d) diagnose and resolve, Hardware issues;
e) escalation of problems where appropriate;
f) provide general maintenance of corporate printers; and
g) setup and configuration of videoconferencing equipment.

10.6 On-Site Services Team Leader

(1) The SCI:On-Site Services Team Leader must:

a) provide first and second level support for Incidents and complete Service Requests, including new Installations and Upgrades for a wide range of Hardware, Software, peripherals and applications;
b) diagnose and resolve, desktop configuration and Software issues;
c) provide direction and assistance to On-Site Service Representatives; and
d) lead a team to complete a technical assignment.

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat: 19335-16-0056

Security Classification / Classification de sécurité

Aug 26/16

SECURITY REQUIREMENTS CHECK LIST (SRCL)
LISTE DE VÉRIFICATION DES EXIGENCES RELATIVES À LA SÉCURITÉ (LVERS)

PART A - CONTRACT INFORMATION / PARTIE A - INFORMATION CONTRACTUELLE

1. Originating Government Department or Organization / Ministère ou organisme gouvernemental d'origine: Department of Justice Canada

2. Branch or Directorate / Direction générale ou Direction: Information Solution Branch

3. a) Subcontract Number / Numéro du contrat de sous-traitance: N/A

3. b) Name and Address of Subcontractor / Nom et adresse du sous-traitant: N/A

4. Brief Description of Work / Brève description du travail

The resulting contract will be used to provide Justice Canada for Level 1 Service Desk Services, Level 2 On-site and Break/Fix Support Services, Level 3 Engineering and Support Services, and professional services through a task authorization on an as and when requested basis for Project Manager, Solution Architect, Security Architect, Business Analyst, On-site Services Team Leader and On-site Services Representative. It is intended to result in the award of a contract for 4 years, plus 2 irrevocable 1-year options allowing Justice Canada to extend the term of the contract.

5. a) Will the supplier require access to Controlled Goods? Le fournisseur aura-t-il accès à des marchandises contrôlées?	✓ No Non	Yes Oui
5. b) Will the supplier require access to unclassified military technical data subject to the provisions of the Technical Data Control Regulations? Le fournisseur aura-t-il accès à des données techniques militaires non classifiées qui sont assujetties aux dispositions du Règlement sur le contrôle des données techniques?	✓ No Non	Yes Oui
6. Indicate the type of access required / Indiquer le type d'accès requis		
6. a) Will the supplier and its employees require access to PROTECTED and/or CLASSIFIED information or assets? Le fournisseur ainsi que les employés auront-ils accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS? (Specify the level of access using the chart in Question 7. c) (Préciser le niveau d'accès en utilisant le tableau qui se trouve à la question 7. c)	No Non	✓ Yes Oui
6. b) Will the supplier and its employees (e.g. cleaners, maintenance personnel) require access to restricted access areas? No access to PROTECTED and/or CLASSIFIED information or assets is permitted. Le fournisseur et ses employés (p. ex. nettoyeurs, personnel d'entretien) auront-ils accès à des zones d'accès restreintes? L'accès à des renseignements ou à des biens PROTÉGÉS et/ou CLASSIFIÉS n'est pas autorisé.	✓ No Non	Yes Oui
6. c) Is this a commercial courier or delivery requirement with no overnight storage? S'agit-il d'un contrat de messagerie ou de livraison commerciale sans entreposage de nuit?	✓ No Non	Yes Oui

7. a) Indicate the type of information that the supplier will be required to access / Indiquer le type d'information auquel le fournisseur devra avoir accès

Canada	NATO / OTAN	Foreign / Étranger
✓	☐	☐

7. b) Release restrictions / Restrictions relatives à la diffusion

Canada	NATO / OTAN	Foreign / Étranger
No release restrictions / Aucune restriction relative à la diffusion ✓	All NATO countries / Tous les pays de l'OTAN ☐	No release restrictions / Aucune restriction relative à la diffusion ☐
Not releasable / À ne pas diffuser ☐		
Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐	Restricted to: / Limité à : ☐
Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :	Specify country(ies): / Préciser le(s) pays :

7. c) Level of information / Niveau d'information

Canada	NATO	Foreign / Étranger
PROTECTED A / PROTÉGÉ A ✓	NATO UNCLASSIFIED / NATO NON CLASSIFIÉ ☐	PROTECTED A / PROTÉGÉ A ☐
PROTECTED B / PROTÉGÉ B ✓	NATO RESTRICTED / NATO DIFFUSION RESTREINTE ☐	PROTECTED B / PROTÉGÉ B ☐
PROTECTED C / PROTÉGÉ C ✓	NATO CONFIDENTIAL / NATO CONFIDENTIEL ☐	PROTECTED C / PROTÉGÉ C ☐
CONFIDENTIAL / CONFIDENTIEL ✓	NATO SECRET / NATO SECRET ☐	CONFIDENTIAL / CONFIDENTIEL ☐
SECRET / SECRET ✓	COSMIC TOP SECRET / COSMIC TRÈS SECRET ☐	SECRET / SECRET ☐
TOP SECRET / TRÈS SECRET ☐		TOP SECRET / TRÈS SECRET ☐
TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐		TOP SECRET (SIGINT) / TRÈS SECRET (SIGINT) ☐

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
19335-16-0056
Security Classification / Classification de sécurité

PART A (continued) / PARTIE A (suite)

8. Will the supplier require access to PROTECTED and/or CLASSIFIED COMSEC information or assets? — No ☑ / Yes ☐
Le fournisseur aura-t-il accès à des renseignements ou à des biens COMSEC désignés PROTÉGÉS et/ou CLASSIFIÉS? — Non ☑ / Oui ☐
If Yes, indicate the level of sensitivity:
Dans l'affirmative, indiquer le niveau de sensibilité :

9. Will the supplier require access to extremely sensitive INFOSEC information or assets? — No ☑ / Yes ☐
Le fournisseur aura-t-il accès à des renseignements ou à des biens INFOSEC de nature extrêmement délicate? — Non ☑ / Oui ☐

Short Title(s) of material / Titre(s) abrégé(s) du matériel :
Document Number / Numéro du document :

PART B - PERSONNEL (SUPPLIER) / PARTIE B - PERSONNEL (FOURNISSEUR)

10. a) Personnel security screening level required / Niveau de contrôle de la sécurité du personnel requis

☐ RELIABILITY STATUS / COTE DE FIABILITÉ	☐ CONFIDENTIAL / CONFIDENTIEL	☑ SECRET / SECRET	☐ TOP SECRET / TRÈS SECRET
☐ TOP SECRET – SIGINT / TRÈS SECRET – SIGINT	☐ NATO CONFIDENTIAL / NATO CONFIDENTIEL	☐ NATO SECRET / NATO SECRET	☐ COSMIC TOP SECRET / COSMIC TRÈS SECRET
☐ SITE ACCESS / ACCÈS AUX EMPLACEMENTS			

Special comments:
Commentaires spéciaux :

NOTE: If multiple levels of screening are identified, a Security Classification Guide must be provided.
REMARQUE : Si plusieurs niveaux de contrôle de sécurité sont requis, un guide de classification de la sécurité doit être fourni.

10. b) May unscreened personnel be used for portions of the work? — No ☑ / Yes ☐
Du personnel sans autorisation sécuritaire peut-il se voir confier des parties du travail? — Non ☑ / Oui ☐
If Yes, will unscreened personnel be escorted? — No ☐ / Yes ☐
Dans l'affirmative, le personnel en question sera-t-il escorté? — Non ☐ / Oui ☐

PART C - SAFEGUARDS (SUPPLIER) / PARTIE C - MESURES DE PROTECTION (FOURNISSEUR)

INFORMATION / ASSETS / RENSEIGNEMENTS / BIENS

11. a) Will the supplier be required to receive and store PROTECTED and/or CLASSIFIED information or assets on its site or premises? — No ☐ / Yes ☑
Le fournisseur sera-t-il tenu de recevoir et d'entreposer sur place des renseignements ou des biens PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ / Oui ☑

11. b) Will the supplier be required to safeguard COMSEC information or assets? — No ☑ / Yes ☐
Le fournisseur sera-t-il tenu de protéger des renseignements ou des biens COMSEC? — Non ☑ / Oui ☐

PRODUCTION

11. c) Will the production (manufacture, and/or repair and/or modification) of PROTECTED and/or CLASSIFIED material or equipment occur at the supplier's site or premises? — No ☑ / Yes ☐
Les installations du fournisseur serviront-elles à la production (fabrication et/ou réparation et/ou modification) de matériel PROTÉGÉ et/ou CLASSIFIÉ? — Non ☑ / Oui ☐

INFORMATION TECHNOLOGY (IT) MEDIA / SUPPORT RELATIF À LA TECHNOLOGIE DE L'INFORMATION (TI)

11. d) Will the supplier be required to use its IT systems to electronically process, produce or store PROTECTED and/or CLASSIFIED information or data? — No ☐ / Yes ☑
Le fournisseur sera-t-il tenu d'utiliser ses propres systèmes informatiques pour traiter, produire ou stocker électroniquement des renseignements ou des données PROTÉGÉS et/ou CLASSIFIÉS? — Non ☐ / Oui ☑

11. e) Will there be an electronic link between the supplier's IT systems and the government department or agency? — No ☐ / Yes ☑
Disposera-t-on d'un lien électronique entre le système informatique du fournisseur et celui du ministère ou de l'agence gouvernementale? — Non ☐ / Oui ☑

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat
19735-16-0056
Security Classification / Classification de sécurité

PART C - (continued) / PARTIE C - (suite)

For users completing the form manually use the summary chart below to indicate the category(ies) and level(s) of safeguarding required at the supplier's site(s) or premises.
Les utilisateurs qui remplissent le formulaire manuellement doivent utiliser le tableau récapitulatif ci-dessous pour indiquer, pour chaque catégorie, les niveaux de sauvegarde requis aux installations du fournisseur.

For users completing the form online (via the Internet), the summary chart is automatically populated by your responses to previous questions.
Dans le cas des utilisateurs qui remplissent le formulaire en ligne (par Internet), les réponses aux questions précédentes sont automatiquement saisies dans le tableau récapitulatif.

SUMMARY CHART / TABLEAU RÉCAPITULATIF

Category / Catégorie	PROTECTED / PROTÉGÉ			CLASSIFIED / CLASSIFIÉ			NATO				COMSEC					
	A	B	C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET	NATO RESTRICTED / NATO DIFFUSION RESTREINTE	NATO CONFIDENTIAL / NATO CONFIDENTIEL	NATO SECRET	COSMIC TOP SECRET / COSMIC TRÈS SECRET	PROTECTED / PROTÉGÉ A	PROTECTED / PROTÉGÉ B	PROTECTED / PROTÉGÉ C	CONFIDENTIAL / CONFIDENTIEL	SECRET	TOP SECRET / TRÈS SECRET
Information / Assets / Renseignements / Biens		✓		J.J. 2016-08-17	✓											
Production																
IT Media / Support TI		✓		2016-08-17	✓											
IT Link / Lien électronique		✓			✓											

12. a) Is the description of the work contained within this SRCL PROTECTED and/or CLASSIFIED?
La description du travail visé par la présente LVERS est-elle de nature PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☒ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification".
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire.

J.J. 2016-08-17

12. b) Will the documentation attached to this SRCL be PROTECTED and/or CLASSIFIED?
La documentation associée à la présente LVERS sera-t-elle PROTÉGÉE et/ou CLASSIFIÉE?

☑ No / Non ☒ Yes / Oui

If Yes, classify this form by annotating the top and bottom in the area entitled "Security Classification" and indicate with attachments (e.g. SECRET with Attachments).
Dans l'affirmative, classifier le présent formulaire en indiquant le niveau de sécurité dans la case intitulée « Classification de sécurité » au haut et au bas du formulaire et indiquer qu'il y a des pièces jointes (p. ex. SECRET avec des pièces jointes).

Government of Canada / Gouvernement du Canada

Contract Number / Numéro du contrat	
19335-16-0056	9TD. Aug 24/16
Security Classification / Classification de sécurité	

PART D - AUTHORIZATION / PARTIE D - AUTORISATION

13. Organization Project Authority / Chargé de projet de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
Nguyen, Truong-Vu	Project Manager	Tr-Vu Nguyen

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
(514) 283-6434	(514) 496-6757	truong.vu.nguyen@justice.gc.ca	2016-08-16

14. Organization Security Authority / Responsable de la sécurité de l'organisme

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
FRANÇOISE BEAUDOIN	DEPUTY DSO	F Beaudoin

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
(613) 957-8941	(613) 957-7868		AUG 17 2016

15. Are there additional instructions (e.g. Security Guide, Security Classification Guide) attached?
Des instructions supplémentaires (p. ex. Guide de sécurité, Guide de classification de la sécurité) sont-elles jointes? ☑ No / Non ☐ Yes / Oui

16. Procurement Officer / Agent d'approvisionnement

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
~~Lacroix, Mario~~ Jonah Dubé	~~Team Leader, Contracting Operations~~ Supply Specialist	

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
(613) 952-9830		mario.lacroix@justice.gc.ca	August 31, 2016

17. Contracting Security Authority / Autorité contractante en matière de sécurité

Name (print) - Nom (en lettres moulées)	Title - Titre	Signature
		Sherry Campbell

Telephone No. - N° de téléphone	Facsimile No. - N° de télécopieur	E-mail address - Adresse courriel	Date
			August 30, 2016

Sherry Campbell
Contract Security Officer, Contract Security Division
Sherry.Campbell@tpsgc-pwgsc.gc.ca
Tel/Tél - 613-948-1646 / Fax/Téléc - 613-948-1712

TBS/SCT 350-103(2004/12)

Security Classification / Classification de sécurité

Canada

Department of Justice Canada
Help Desk and Support Services

Appendix A to Annex A
Service Domain: JUS Service Desk Service

Table of Contents

1 INTRODUCTION

(1) This section is provided for information only.

(2) The JUS Service Desk Service established by the Contractor will be the primary contact point for End Users to report Incidents or submit Service Requests, and will be responsible for maintaining all information relating to the Incidents and Service Requests reported.

(3) The JUS Service Desk Service objectives are:

a) to act as the central point of contact between End Users and all IT Services, including applications and infrastructure;

b) to handle Incident Tickets and Service Requests, and to act as a focal point for information management relating to the delivery of IT Services;

c) to restore normal service operation as quickly as possible with minimum disruption to End Users, thus ensuring that the best achievable levels of service and availability are maintained; and

d) to help identify and lower the overall cost of ownership for IT Services as a whole.

(4) This appendix describes the requirements for the JUS Service Desk Service. The following is included in this document:

a) Requirements specific to the provisioning of the JUS Service Desk Service for Incidents and Service Requests for both applications and IT infrastructure.

b) Requirements specific to the Service Delivery Portal that Canada representatives would have access to as part of this Service. This appendix describes the requirements of the Service Delivery Portal, from the following perspectives:

i) End Users – e.g. for Self Service capabilities to create an Incident Ticket or Service Request;

ii) Canada service managers – e.g. to create or review an Incident Ticket or Service Request or to run a management report;

iii) Level 2 Support representatives (outside the NCR) - e.g. to create or update an Incident Ticket or Service Request; and

iv) Level 2 and Level 3 Support representatives for infrastructure and applications – e.g. to create or update an Incident Ticket or Service Request assigned to them. These user groups may use the Service Delivery Portal as their primary IT service management tool.

2 SERVICE DELIVERY REQUIREMENTS

2.1 Scope of JUS Service Desk Service

(1) The JUS Service Desk Service is one of the JUS HDS Services. When ordered by Canada by issuing a Service Order, the HDS Service Desk Service, as managed and implemented by the Contractor, must meet or exceed all of the requirements listed in this appendix of the SOW, in the balance of the SOW and elsewhere in the Contract prior to acceptance by Canada and during the entire period specified in each Service Order.

(2) The JUS Service Desk Service must provide Level 1 Support for Hardware and Software identified in the following tables in Appendix C: Standard Hardware and Software List:

a) Table 1 – Software List L1

b) Table 2 – Hardware List

c) Table 3 – OS Image

(3) The JUS Service Desk Service must provide Level 1 Support for all other IT infrastructure services including but not limited to directory, access management and Public Key Infrastructure (PKI) services, data centre services, networking and telecommunications services, and other distributed computing services including collaboration, Remote Access, enterprise storage, and terminal services.

(4) The JUS Service Desk Service must participate in Incident Management, Problem Management, Change Management, Release Management, Configuration Management, Asset Management, and Software License Management activities as specified in this appendix of the SOW.

2.2 Hardware, Software and Facilities

(1) The Contractor must supply all Hardware and Software, except Government Furnished Equipment (GFE), for the JUS Service Desk Service.

(2) The JUS Service Desk Service infrastructure must be located at Contractor SDPs.

2.3 Service Catalogue Items

(1) The Contractor must provide a SCI:SDS-User which allows an End User to be supported by the JUS Service Desk Service (one user per SCI) as specified by Canada in a Service Order.

(2) The following Feature Profile definitions pertain to the SCIs for the JUS Service Desk Service:

a) Premium Service Level Plan for up to 4% of the cumulative number of SCI:SDS-User ordered with Service Orders; and

b) Standard Service Level Plan for the remainder of the SCI:SDS-User.

(3) The Contractor must provide the Premium Service Level Plan to End Users identified by Canada. These End Users are for example:

a) high-level executives;

b) resources working on a high-profile file or project; and

c) resources responsible for mission-critical work.

2.4 Hours of Service

(1) The JUS Service Desk Service must be a point of contact 24 hours per day, 7 days per week, 365 days per year under the following operation modes:

a) attended mode support hours are from 6:00 ET to 21:00 ET on FGWDs, as follows:

i) live agents processing Service Requests and Incidents for the Telephone Support, Email Support, Web-Chat, and Self Service Service Channels; and

ii) live agents troubleshooting and escalating Incidents to the appropriate supporting group, as required.

b) unattended mode support, i.e. outside of attended mode support hours, as follows:

i) agent is on standby only;

ii) Telephone Support only (Email Support, Web-Chat and Self Service Service Channels are processed the following FGWD);

iii) calls are answered by the Voice-mail system;

iv) End Users leave a voice message and an agent calls back within SLTs;

v) best effort service levels for Incident resolution;

vi) escalate to an appropriate on-call Level 2 and Level 3 Support representative to resolve the Incident or provide the requested service, if available; and

vii) unresolved Incidents are dealt with the following FGWD.

2.5 Service Channels

(1) The JUS Service Desk Service must provide the following Service Channels to End Users:

a) Telephone Support - for Authorized End Users to access the JUS Service Desk Service using:

i) a unique and dedicated toll-free telephone number (for example, 1-800 number); the telephone number will be specified by Canada; and

ii) a unique and dedicated NCR local telephone number; the telephone number will be specified by Canada.

b) Self Service – a component of the Service Delivery Portal specific to End Users to be able to access the JUS Service Desk Service;

c) Voice-mail Support in unattended mode only – the ability to leave a Voice-mail message to the JUS Service Desk Service for support purposes;

d) Email Support – the ability to send an email to the JUS Service Desk Service for support purposes; and

e) Web-Chat Support – a Service Channel of the Service Delivery Portal that allows an End User to establish an online chat session with the JUS Service Desk Service.

(2) The JUS Service Desk Service must provide a method through which an End User can send information related to an Incident or a Service Request to the HDS Service Desk Service via email or Web-Chat, and the JUS Service Desk Service must enter the information as an Incident Ticket or a Service Request.

(3) The JUS Service Desk Service must provide Self Service access via the Service Delivery Portal to be able to view and update information to:

a) Canada on-site support representatives (e.g. outside the NCR), and

b) Canada Level 2 and Level 3 Support representatives for infrastructure and applications.

(4) The JUS Service Desk Service must provide Self Service access to Canada Service Managers to be able to be able to view and update information and run management reports.

(5) The JUS Service Desk Service must provide access to all Service Channels in the official language of choice (English or French) of any Canada representative.

2.6 HDS Service Desk Service Personnel Training

(1) The Contractor must provide at no additional cost to Canada all training the JUS Service Desk Service personnel requires to fulfil their duties with competence and effectiveness at all times during the Contract Period.

(2) The Contractor must ensure that JUS Service Desk Service personnel skills remain current with the evolving technical and application environment that the Contractor is responsible to support as part of the JUS Service Desk Service.

(3) The Contractor must ensure that JUS Service Desk Service personnel continuous training activities do not impact the Service Level Targets.

3 SERVICE REQUIREMENTS

3.1 Initial Contact Management Requirements

(1) The JUS Service Desk Service must be available as a primary point of contact to Authorized End Users to report Incidents or submit Service Requests. The secondary point of contact to the JUS Service Desk Service will be the Service Delivery Portal.

(2) The JUS Service Desk Service must track the initial contact with End Users for a new Incident or Service Request for all Service Channels. At minimum, the following End User information must be captured for every contact:

a) name;

b) telephone number;

c) location;

d) organization;

e) asset number;

f) time and date of the contact; and

g) purpose of the contact.

(3) The JUS Service Desk Service must provide the End User with an Incident Number or Service Request Number, and retain and update the information captured in the above requirement for future reference when the End User contacts the JUS Service Desk Service in the future.

(4) As a minimum, the JUS Service Desk Service must:

a) receive Incident Tickets and Service Requests from End Users from one of the Service Channels;

b) for Incidents submitted on an Alternate Service Channel, the JUS Service Desk Service must call the End User;

c) data enter and perform a quality assurance check on the Incident Ticket and the Service Request information provided by the End User to ensure it is correct;

d) begin efforts to resolve the Incident;

e) escalate to an appropriate Level 2 and Level 3 Support representative to resolve the Incident or provide the requested service, if required;

f) report Incidents or Service Requests to external service desks using one of the following methods as specified by Canada:

i) enter Incidents and Service Request information into a service delivery portal provided by the external service desk;

ii) forward (via email) Incidents and Service Request information to the external service desk email address; and

iii) provide Incidents and Service Request information to the external service desk by telephone;

g) maintain contact with the End User and all assigned support representatives throughout the entire process to confirm completion (for both Incident Tickets and Service Requests);

h) ensure all information relating to the Incident Tickets and Service Requests is captured in the Service Delivery Portal; and

i) issue bilingual communications to End Users, as approved by Canada, concerning issues and changes which affect the IT infrastructure (e.g. planned server downtime).

3.2 Incident Management

(1) The JUS Service Desk Service must address, as a minimum, the following Incident Management actions:

a) open (or update, as appropriate) an Incident Ticket and record information concerning the Incident, including, as a minimum, the information identified in the General SOW, Annex A, subsection Incident Management;

b) attempt to resolve Incidents using scripts and the desktop management tool (e.g. Remote Control);

c) report Prohibited Software to Canada when detected on an End User Device as part of ongoing support activities;

d) manage the support process from reporting through resolution, ensuring that all Incidents are given an appropriate level of attention, escalated to higher support resources when necessary, and are resolved in an efficient and timely manner;

e) report the resolution of the Incident back to the originating End User and ensure they are satisfied that the Incident has been resolved;

f) ensure that Incident Tickets are properly completed including Incident description, resolution efforts, and all contact information;

g) close the Incident Ticket;

h) update the Knowledge Repository with information related to Incident resolution when appropriate; and

i) review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing and exercises.

(2) For the support of Hardware, the JUS Service Desk Service must address, as a minimum, the following actions:

a) troubleshoot the usage and operation of the Hardware (how to questions);

b) track lost or stolen Hardware;

c) assist with basic instruction on the replacement of media for the Device; and

d) assist with the support of the migration of settings during equipment evergreening.

(3) For the support of Software, the JUS Service Desk Service must address, as a minimum, the following actions:

a) troubleshoot the usage and operation of the Software (how to questions);

b) assist with security updates and notifications;

c) assist with installation and de-installation of the Software, Software Patches and security updates; and

d) assist with the support of the migration of Software and settings, including shortcuts, during technology refresh.

(4) For the support of business applications, the JUS Service Desk Service must address, as a minimum, the following actions:

a) execute Canada-provided support scripts for resolving issues with the supported business applications; and

b) provide End User assistance with the installation and de-installation of the software and related patches, and security updates, as required.

(5) The JUS Service Desk Service must perform password resets for End User Accounts on Canada LAN using active directory native administration functions or another active directory administration tool that could be provided by Canada.

(6) The JUS Service Desk Service must perform password reset for End User Accounts on the Service Delivery Portal.

(7) The JUS Service Desk Service must perform Incident Management according to the JUS HDS Services Managed Service Incident Management process (refer to General SOW, Incident Management subsection).

3.3 Service Request Management

(1) The JUS Service Desk Service must address, as a minimum, the following actions related to Service Request management:

a) accept and update as appropriate a Service Request and record additional information concerning the Service Request, including, but not be limited to, the following information fields:

i) Service Request Number;
ii) Service Request type;
iii) date and time Service Request received;
iv) date and time Service Request assigned;
v) date and time Service Request closed;
vi) related Service Requests;
vii) End User details;
viii) Service Request details;
ix) equipment details;
x) actions taken; and
xi) Service Request assignee.

b) report the completion of the Service Request back to the originating End User and ensure they are satisfied with the completion of the Service Request;

c) ensure that Service Request records are properly completed including description and contact information; and

d) close the Service Request.

3.4 End User Assistance and Frequently Asked Questions

(1) The JUS Service Desk Service must provide End Users with tips or answers to Frequently Asked Questions (FAQs) as approved by Canada.

(2) The JUS Service Desk Service must maintain FAQs and publish training and education reference materials, as approved by Canada, on the Service Delivery Portal for End Users to access for Self Service support.

3.5 Other IT Service Management Activities

3.5.1 Problem Management

(1) The JUS Service Desk Service must link Incidents to existing or new Problems as requested by the Canada.

(2) The JUS Service Desk Service must participate in Problem Management in compliance with the Problems Management process (refer to General SOW, Problem Management subsection).

3.5.2 Change Management

(1) The HDS Service Desk Service must participate in Change Management in compliance with the Change Management process (refer to General SOW, Change Management subsection).

3.5.3 Release Management

(1) The HDS Service Desk Service must coordinate the communications for a Supported HDS Software release to affected End Users, as specified by Canada.

(2) The HDS Service Desk Service must participate in Release Management in compliance with the Release Management process (refer to General SOW, Release Management subsection).

3.5.4 Configuration Management, Asset Management and Software License Management

(1) The HDS Service Desk Service must ensure that updates to the Asset Management, Software License Management and Configuration Management Database (CMDB) repositories are completed as a result of IT Service Management processes.

3.6 Customer Satisfaction Management

3.6.1 Customer Satisfaction

(1) The JUS Service Desk Service must measure End User satisfaction levels with respect to the performance of the JUS HDS Services by requesting End Users to complete a Customer Satisfaction Measurement Survey for Incidents and Service Requests.

(2) The JUS Service Desk Service must make the Customer Satisfaction Measurement Survey available to End Users using the Service Delivery Portal.

(3) In addition to any End-User Customer Satisfaction Measurement Survey requirements set in 3.6.2, the Contractor must at Canada's request, but not more often than once quarterly, conduct End-User Satisfaction surveys. The Contractor's proposed Customer Satisfaction Measurement Surveys (including the underlying instrument(s), methodology and survey plan) is subject to Canada's review, comments and approval, and must cover a representative sample of the End-Users. Canada will provide reasonable assistance to the Contractor to:

a) identify the appropriate sample of End-Users;

b) distribute the Customer Satisfaction Measurement Surveys; and

c) encourage participation by such End-Users in order to obtain meaningful results.

(4) The Contractor must report the results of the Customer Satisfaction Measurement Surveys separately from each of the End-Users or groups of End-Users as may be specified by Canada, and the Contractor must conduct a review session of the results of each Customer Satisfaction Measurement Survey with Canada within 30 FGWDs following the mutually agreed deadline for completion and return of the Customer Satisfaction Measurement Survey.

(5) Not later than 30 FGWDs following each review session, the Contractor must provide to Canada an action plan for addressing any problem areas identified in the Customer Satisfaction Measurement Survey results.

3.6.2 Customer Satisfaction Measurement Plan

(1) The Contractor must submit a customer satisfaction measurement plan before the end of the Operational Readiness Phase (see Annex A General SOW, Operational Readiness Phase subsection) for approval by Canada that describes the method to perform the Customer Satisfaction Measurement Survey including:

a) defining measurable objectives to be achieved;

b) defining the different questionnaires and their purpose;

c) defining the questions that will be asked;

d) defining the rules for soliciting End Users (i.e. each Incident, random, periodic, etc.); and

e) defining the rules to interpret the results.

(2) The Contractor must review the customer satisfaction measurement plan on an annual basis, and provide an assessment for approval by Canada within 20 FGWDs of the contract anniversary including:

a) an assessment of the achieved objectives over the last year;

b) recommended changes to improve the value of the customer satisfaction measurement plan; and

c) an action plan to implement the recommended changes.

(3) The Contractor must implement changes approved by Canada to the Customer Satisfaction Measurement Plan within 20 FGWDs of receiving Canada's approval.

4 SERVICE DELIVERY PORTAL FUNCTIONALITY REQUIREMENTS

(1) The Contractor must deliver the Service Delivery Portal requirements below.

4.1 Solution Hardware, Software and Facilities

(1) The Contractor must supply all Hardware and Software, except Government Furnished Equipment (GFE), for the Service Delivery Portal.

(2) The Service Delivery Portal infrastructure must be located at Contractor SDPs.

4.2 Knowledge Management – Knowledge Repository

(1) The Contractor must provide a knowledge management solution that will capture and make available a Knowledge Repository documenting Incident resolution, Known Errors, procedural instructions, Frequently Asked Questions and other pertinent information.

(2) The Knowledge Repository must offers real, accurate, and context-aware content to the End User by using a probable context and associated knowledge (End-Users' profile information, recent searches, related Incidents, etc.) to inform the End User and to prioritize the correct answer for faster, individualized searching.

(3) The context-aware Knowledge Management Platform is based on data discovery analytics tool with the capability to automate knowledge additions where data can be streamlined, integrated, or leveraged to make the JUS Service Desk Service more efficient.

4.3 Service Delivery Portal – End User Functionality

(1) The Service Delivery Portal must allow an End User to create an Incident Ticket or a Service Request and submit it to the JUS Service Desk Service.

(2) The Service Delivery Portal must allow an End User to view the current status of an Incident Ticket or Service Request where they are the originator.

(3) The Service Delivery Portal must provide a means for an End User to look up Known Errors, procedural instructions, Frequently Asked Questions and other pertinent information in a Knowledge Repository in order to obtain their own support using a Self Service approach with the objective of reducing the number of Incidents reported to the JUS Service Desk Service.

(4) The Service Delivery Portal must provide a means for an End User to view important system notifications, service status and dashboard of happening Incidents as published by the JUS Service Desk Service.

4.4 Cognitive virtual service – Virtual Assistant

(1) The Service Delivery Portal must provide a virtual chat as a Self Service combining an interactive, intelligent virtual assistant with the Web-Chat support to interpret an End User's needs through intelligent analysis of Web-Chat, and to offer instant, precise and automated answers.

(2) The Service Delivery Portal virtual assistant must deliver answers from the Knowledge Repository or tap into a variety of data sources to respond intelligently to an End User query.

(3) Both open and closed Web-Chat sessions can automatically be converted to Incident Tickets or Service Requests with the entire Web-Chat history logged in the Incident Tickets.

(4) The Service Delivery Portal virtual assistant must offer a call back or other form of support to the End User if an answer or solution cannot be found. i.e. intelligently route chat sessions to live Level 1 Support agents when End Users need a more personal touch or create a conventional JUS Service Desk Service Incident Ticket through the same interface.

(5) The deployment plan and schedule will be determined after contract award and mutually agreed between Canada and the Contractor

4.5 Service Delivery Portal – Level 2 or Level 3 Support Representative Functionality

(1) The Service Delivery Portal must allow a Level 2 or Level 3 Support representative (e.g. Level 2 JUS On-Site Support Service or Application Support representative) to create an Incident Ticket or a Service Request and submit it to the JUS Service Desk Service.

(2) The Service Delivery Portal must allow a Level 2 or Level 3 Support representative to view the current status or update an Incident Ticket or Service Request that has been assigned to them.

(3) The Service Delivery Portal must provide a means for a Level 2 or Level 3 Support representative to look up Known Errors, procedural instructions, Frequently Asked Questions and other pertinent information in a Knowledge Repository.

(4) The Service Delivery Portal must allow a Level 2 or Level 3 Support representative to create and update a Change Request, a Problem Ticket, a Release Record, an Asset Management Record, a Software License Record, or a configuration item.

4.6 Service Delivery Portal – Service Manager Functionality

(1) The Service Delivery Portal must allow a Canada Service Manager to create an Incident Ticket or a Service Request and submit it to the JUS Service Desk Service.

(2) The Service Delivery Portal must allow a Canada Service Manager to view the current status of any Incident Ticket or Service Request.

(3) The Service Delivery Portal must allow a Canada Service Manager to change the priority of any Incident Ticket.

(4) The Service Delivery Portal must allow a Canada Service Manager to perform queries or access a report (as defined in the Statement of Work).

(5) The Service Delivery Portal must allow a Canada Service Manager to create and update a Change Request, a Problem Ticket, a Release Record, an Asset Management Record, a Software License Record, or a configuration item record.

5 TRAINING REQUIREMENTS

(1) The Contractor must provide on-line training in both English and French to familiarize Canada with the operation of the Service Delivery Portal. This includes End Users, Service Managers and Level 2 and Level 3 Support representatives.

(2) The Contractor must update the on-line training when there is a major release upgrade of the Service Delivery Portal within 30 FGWDs of obtaining approval to proceed with the release upgrade.

6 SERVICE LEVEL TARGETS

6.1 Service Level Targets for the Service Delivery Portal

(1) The JUS Service Desk Service must comply with the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for the JUS Service Desk Service requirements for the Service Delivery Portal:

a) SLT-SDP-MSOT (Service Delivery Portal Maximum Service Outage Time); and

b) SLT-SDP-MTTR (Service Delivery Portal Maximum Time to Restore Service).

6.2 Service Level Targets for Attended Mode

(1) The JUS Service Desk Service must comply with the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for all Standard Service Level Plan End Users during attended mode:

a) SLT-SD-MTA (Service Desk Maximum Time to Answer);

b) SLT-SD-MTOH (Service Desk Maximum Time on Hold);

c) SLT-SD-MTTE-1 (Service Desk maximum Time to Escalate - Standard);

d) SLT-SD-MTRASCI (Service Desk Maximum Time to Respond to Alternative Service Channel Incidents;

e) SLT-SD-MML1RR (Service Desk Minimum Level 1 Resolution Rate; and

f) SLT-SRF (Service Request Fulfilment).

(2) The JUS Service Desk Service must comply with the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for all Premium Service Level Plan End Users during Attended Mode:

a) SLT-SD-MTA (Service Desk Maximum Time to Answer;

b) SLT-SD-MTOH (Service Desk maximum Time on Hold;

c) SLT-SD-MTTE-2 (Service Desk Maximum Time to Escalate Premium);

d) SLT-SD-MTRASCI (Service Desk Maximum Time to Respond to Alternative Service Channel Incidents;

e) SLT-SD-MML1RR (Service Desk Minimum Level 1 Resolution Rate; and

f) SLT-SRF (Service Request Fulfilment).

6.3 Service Level Targets for Unattended Mode

(1) The HDS Service Desk Service must have the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for all End Users during Unattended Mode:

a) SLT-SD-MTRASCI (Service Desk Maximum Time to Respond to Alternative Service Channel Incidents.

6.4 Service Level Targets for End User Satisfaction

(1) The HDS Service Desk Service must have the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for the HDS Service Desk Service requirements for the End User Satisfaction:

a) SLT-SD-MEUSR (Service Desk Minimum End User Satisfaction Rate)

7 REPORTING AND DOCUMENTATION REQUIREMENTS

(1) The Contractor must define the content and format of reports and documentation in consultation with Canada and subject to Canada's approval and acceptance before acceptance of the JUS HDS Services.

(2) Unless indicated otherwise, the Contractor must provide reports in English in a format specified by Canada. All JUS HDS Services reports and documentation produced by the Contractor must be accessible from the Service Delivery Portal unless otherwise indicated by Canada.

7.1.1 Service Delivery Portal Documentation

(1) The Contractor must provide electronic copies of User Guides for the operation of the Service Delivery Portal in English and French. It must include the following:

a) structure, content and usage instructions; and

b) menu, data entry forms and report screen shots.

7.1.2 Service Desk Activity Report - Monthly

(1) The Contractor must provide a service desk activity report which is to be made available to Canada on a monthly basis within five FGWDs of the end of the previous month.

(2) The service desk activity report must include the following current monthly statistics, and the previous 12 months statistics:

a) number and percentage of Contacts, by region;

b) number and percentage of Contacts by Service Channel, by region

c) number and percentage of Contacts, by Incident, Service Request, and End User Assistance (FAQ), by region;

d) average number of Contacts per End User, by region (displayed as a bar chart graph);

e) number and percentage of Incidents, by priority, by level resolved (including application and other infrastructure support groups), by region;

f) number of Incidents open at the end of period, by priority, by region;

g) number and percentage of Service Requests, by level completed (including application and other infrastructure support groups), by region;

h) number of Service Requests open at the end of period, by region;

i) number of Customer Satisfaction Surveys taken, by region;

j) Customer Satisfaction Survey results, by region; and

k) number of queries against the Self-Service Knowledge Repository.

(3) The monthly Service Desk Activity Report must include the following current monthly statistics,:

a) number of Incidents by top 10 Incident category;

b) number of Service Requests by top 10 Service Request category; and

c) number of queries by the top 10 topics on the Self-Service Knowledge Repository.

Department of Justice Canada
Help Desk and Support Services

Appendix B to Annex A
Service Domain: JUS On-Site Support Service

Table of Contents

1 INTRODUCTION

(1) This section and is provided for information only.

(2) The JUS On-Site Support Service established by the Contractor will be responsible for accepting and resolving Incidents and Service Requests assigned to it from the JUS Service Desk Service. In conjunction with the JUS Service Desk Service, the JUS On-Site Support Service will act as the primary support group for the End User community and as such is expected to handle the vast majority of support requirements. The JUS On-Site Support Service will perform the duties of a Level 2 Support group.

(3) JUS On-Site Support Service Objectives:

a) To handle Incident Tickets and Service Requests that require physical access to the device;

b) To deliver warranty and post-warranty hardware repair and replacement;

c) To restore normal service operation as quickly as possible with minimum disruption to End Users, thus ensuring that the best achievable levels of service and availability are maintained;

d) To assist the Service Desk in managing information concerning the Incidents and Problems affecting the equipment, and be responsible for problem trend analysis; and

e) To help identify and lower the overall cost of ownership for Information Technology (IT)Services as a whole.

(4) This annex describes the requirements for the JUS On-Site Support Service.

2 JUS On-Site Support Service

(1) The JUS On-Site Support Service is one of the JUS HDS Services. When ordered by Canada, by issuing a Service Order, the JUS On-Site Support Service, as managed and implemented by the Contractor, must meet or exceed all of the requirements listed in this section of the Statement of Work (SOW), in the balance of the SOW and elsewhere in the Contract prior to acceptance by Canada and during the entire period specified in each Service Order.

(2) The Contractor must supply all hardware, software and tools, except Government Furnished Equipment, for the JUS On-Site Support Service.

(3) The JUS On-Site Support Service personnel can be located at Canada Service Delivery Points as agreed to with Canada.

2.1 Service Catalogue Items

(1) The Contractor must provide a SCI:OSS-User which allows an End User to be supported by the JUS On-Site Support Service (one user per SCI) as specified by Canada in a Service Order.

(2) The following Feature Profile definitions pertain to the Service Catalogue Items (SCIs) for the JUS On-Site Support Service:

a) Premium Service Level Plan for up to 4% of the cumulative number of SCI:OSS-User ordered with Service Orders; and

b) Standard Service Level Plan for the remainder of the SCI:OSS-User.

(3) The Contractor must provide the Premium Service Level Plan to End Users identified by Canada. These End Users are for example:

a) high-level executives;

b) resources working on a high-profile file or project; and

c) resources responsible for mission-critical work.

2.2 Coverage Area and Standard Hours of Service

(1) The Contractor must provide the JUS On-Site Support Service, within the National Capital Region, in Canada Service Delivery Points and in other locations as specified by Canada from time to time.

(2) The Contractor must provide the JUS On-Site Support Service from 7:00 ET to 18:00 ET on FGWDs.

2.3 Personnel

(1) The Contractor must staff the JUS On-Site Support Service with personnel with the right skills, in the right quantity, at the right time and at the right place to meet the Service Level Targets.

(2) The Contractor's JUS On-Site Support Service personnel must be bilingual, highly qualified technical professionals with exemplary client-service skills to interact directly with End Users.

2.3.1 Continuous Training

(1) The Contractor must provide at no additional cost to Canada all training that the JUS On-Site Support Service personnel require to fulfil their duties with competence and effectiveness at all times during the Contract period.

(2) The Contractor must ensure that JUS On-Site Support Service personnel skills remain in synch with the evolving technical environment the Contractor is responsible to support as part of the JUS On-Site Support Service.

(3) The Contractor must ensure that JUS On-Site Support Service personnel continuous training activities do not impact the Service Level Targets.

3 ON-SITE SUPPORT

(1) The JUS On-Site Support Service must provide services to End Users in the official language (English or French) of their choice 100% of the time.

(2) The JUS On-Site Support Service must provide Level 2 Support by resolving Incidents and performing Service Requests for hardware and software identified in the following tables in Appendix C: Standard Hardware and Software List:

a) Table 2 – Hardware list;

b) Table 3 – OS Image; and

c) Table 4 – Software list L2.

3.1 Service Remediation

(1) The JUS On-Site Support Service must accept and resolve Incidents.

(2) The JUS On-Site Support Service must exclusively work on Incident Tickets assigned by the JUS Service Desk Service or the Service Manager, with the exception of Premium Service Level Plan End Users for whom the Incident Ticket may be created after the fact.

(3) The JUS On-Site Support Service must prioritize its support according to the priority of the Incident Ticket (refer to General SOW, Incident Management subsection) where Incidents with the highest priority are resolved first.

(4) The JUS On-Site Support Service must re-prioritize its support when the Priority Code of an Incident Ticket is changed.

(5) Upon receiving an Incident, the JUS On-Site Support Service must:

a) assign the Incident Ticket to a JUS On-Site Support Service representative;

b) confirm acceptance of the Incident Ticket to the JUS Service Desk Service;

c) contact the appropriate End User and/or other Canada representative(s) to confirm the assignment;

d) visit the End User's location or other appropriate location from which to begin efforts to resolve the Incident;

e) provide on-site technical / functional assistance including coaching (e.g. "how to" questions) to End Users;

f) co-operatively work with Canada and any other third parties as requested by Canada to resolve Incidents;

g) involve other resolution groups as required, and supervise progress to ensure that resolution efforts respect applicable warranties, Service Level Targets, and industry best practices;

h) retain responsibility for resolving the Incident and updating the Incident Ticket unless otherwise directed or until assigned to another resolver group, regardless of the participation of any other support group or individual;

i) comply to prescribed escalation procedures for all Incident types;

j) notify the appropriate Canada representative(s) if and when a Service Level Target is about to be missed, or if Incident resolution efforts were not completed successfully within the same FGWD;

k) maintain contact with the affected End User, JUS Service Desk Service, all involved support resources, and other Canada representatives as necessary and act as the focal point for all information and coordination throughout resolution efforts;

l) provide alternatives to End Users, using available spare inventory devices provided by Canada, when their computers, printers, or other devices are expected to be unavailable for longer than one FGWD, or less for critical situations;

m) report the resolution of the Incident to the appropriate End User and/or other Canada representative(s) and ensure that the End User is satisfied with the resolution prior to

terminating efforts;

n) conduct appropriate testing to ensure that the work was completed properly;

o) update the Incident Ticket promptly according to the Service Level Targets; and

p) ensure that all applicable procedures, standards and quality controls have been adhered to.

3.2 Break/Fix

(1) The JUS On-Site Support Service must provide warranty hardware repair and replacement services for all devices covered by a warranty.

(2) The JUS On-Site Support Service must provide post-warranty hardware repair and replacement services for all devices not covered by a warranty.

(3) The JUS On-Site Support Service must provide replacement parts and Canada will reimburse the Contractor for the replacements of non-warranty parts as per SCI:PartsHandingFee.

(4) When directed by Canada, the JUS On-Site Support representative must return to a Canada representative a failed hard disk. The replacement hard disk will be considered a non-warranty part provided that by not returning the original hard disk constitutes a non compliance to the terms and conditions of the manufacturer's warranty.

(5) The JUS On-Site Support Service must perform appropriate troubleshooting (including running of diagnostics, if necessary) in order to ensure that the approach to resolve the Incident is the fastest method of allowing the affected End User(s) to return to work.

(6) When it is necessary to replace a faulty component while delivering warranty or non-warranty services:

a) all replacement equipment will conform to standards as specified by Canada; or

b) if it is not possible to replace the faulty component with a standard component, the Contractor will propose an alternative to Canada and obtain approval from an authorized Canada representative prior to completing the work.

(7) The JUS On-Site Support Service must conclude repairs with quality control steps to ensure that:

a) all applicable procedures and standards have been adhered to;

b) any and all software drivers required by the affected equipment have been properly installed;

c) the malfunctioning equipment has been fully tested;

d) hard disk to be returned to Canada are securely returned;

e) the equipment is returned to the Service Delivery Point contact person in an operational state;

f) any required form has been filled-in; and

g) the repair resolution is documented in the Incident Ticket.

(8) The Contractor must manage the warranty claims with the manufacturers of the equipment.

3.3 Service Requests

(1) The JUS On-Site Support Service must accept and execute Service Requests (refer to General SOW, subsection Service Request – Maximum Time to Fulfil) assigned to it from the JUS Service Desk Service.

(2) All Work performed as part of technology refreshes (see Technology Refresh subsection) must be provided by the Contractor at no additional cost to Canada and must not be included in the Service Request metrics.

3.4 Preventive Maintenance

(1) The JUS On-Site Support Service must visit printers semi-annually to perform preventative maintenance including:

a) inspecting ozone filters and static eliminator teeth, and cleaning the fuser unit;
b) inspecting paper pickup rollers for dust, glazing and cracks and replace rollers when they become shiny and appear "glazed";
c) inspecting separation pads for dust, glazing and cracks and replace rollers, together with pickup rollers, when they become shiny and appear "glazed";
d) cleaning dirty transfer rollers;
e) inspecting mirrors for dust build- up;
f) inspecting the fuser assembly rollers for marks and replace if marks are present;
g) ensuring printers are functioning as expected;
h) creating an Incident Ticket if the printer needs to be repaired; and
i) where applicable, applying Software upgrades, patches and / or firmware updates to printers.

(2) The JUS On-Site Support Service must visit boardrooms quarterly to perform preventative maintenance on multimedia equipments including:
a) inspecting, adjusting and cleaning equipment as required;
b) cleaning or replacing dust filters in equipment as required;
c) checking bulb life and recommending replacement as required;
d) checking image settings and adjusting as required;
e) changing batteries in remote controls, keyboards and mice;
f) ensuring appropriate signage regarding the equipment located in the boardroom;
g) ensuring equipment inventory for the boardroom is accurate and up to date;
h) ensuring equipment is functioning as expected; and
i) where applicable, applying Software upgrades, patches and / or firmware updates to multimedia boardroom equipment.

3.5 Technology Refresh (Evergreening)

(1) The JUS On-Site Support Service must, at no additional cost to Canada, perform technology refreshes according to the following schedule:
a) desktop and laptops every 4 years;
b) monitors every 6 years; and
c) printers every 6 years.

(2) The number of years is calculated from the in-service date of the device. However, Canada reserves the right to modify the life of an asset.

(3) The Contractor must prepare an annual report for approval by Canada, within 30 FGWDs of a request by Canada, identifying devices that need to be refreshed during the upcoming fiscal year.

(4) The JUS On-Site Support Service must prepare for Canada an annual refresh plan for the devices approved by Canada describing the monthly refresh schedule to be performed.

(5) The JUS On-Site Support Service must perform the Device Deployment for the devices as per the refresh plan approved by Canada (see section below).

3.6 Device Deployment

(1) The JUS On-Site Support Service must deploy devices based on a scheduled Technology Refresh approved by Canada.

3.6.1 Deployment Planning

(1) The JUS On-Site Support Service must confirm the deployment schedule with the End User and/or Canada coordinator.

3.6.2 Device Assembly

(1) The JUS On-Site Support Service must unpack, configure and test the device.

(2) For End User Devices, the JUS On-Site Support Service must:

a) install the base Operating System Image;

b) apply configuration settings;

c) install any required additional software packages; and

d) execute the disk encryption software, included in the base OS image, for portable devices and let it run unattended until completion of the full disk encryption.

(3) The JUS On-Site Support Service must dispose of all product containers and materials in the appropriate location as per the requirements of each Service Delivery Point, if applicable.

3.6.3 Device Installation

(1) The JUS On-Site Support Service must deliver and install the new device at the End User location or another location specified by Canada.

(2) The JUS On-Site Support Service must provide orientation information, approved by Canada, to newly activated End Users or when hardware is added to ensure that they have a comprehensive understanding, and expand upon the information as necessary.

(3) The JUS On-Site Support Service must ensure the new device performs as expected.

3.6.4 Data and Settings Migration

(1) In the case of a End User device replacement, the JUS On-Site Support Service must:

a) provide the End User with End User-specific information as to what installed software will be transferred from the old device to the new device; and

b) migrate all End User data and settings from the old device to the new device and record changes from the initial assessment with the End User.

(2) The JUS On-Site Support Service must obtain Canada approval for any deviation from Canada standards (Appendix C: Standard Hardware and Software List).

3.6.5 Device Disposal

(1) The JUS On-Site Support Service must promptly prepare retired devices including:

a) moving the retired devices from the End User location into a storage area identified by Canada at the Service Delivery Point and retain the retired devices for 2 weeks;

b) performing secure erasure of storage devices, using an RCMP-approved software application / process;

c) coordinating the return of equipment to Crown Assets or the Computer for Schools Program following the established Canada process where Canada pays shipping costs; and

d) aggregating surplus assets in a Service Delivery Point specified by Canada.

3.6.6 Completion

(1) The JUS On-Site Support Service must sign-off the work completion form with the End User or Canada representative, including the hardware disposal form, if applicable.

(2) The JUS On-Site Support Service must follow up with the End User or the Canada representative within 48 hours via e-mail or Service Delivery Portal to reconfirm the deployment was well performed and the device is running smoothly.

(3) The JUS On-Site Support Service must record the follow-up and close the Service Request.

3.7 Multimedia Support

(1) The JUS On-Site Support Service must resolve multimedia related Incidents and perform

multimedia Service Requests.

(2) The JUS On-Site Support Service is responsible for visiting each boardroom on a monthly basis to ensure that the equipment is operating properly. The frequency of visit must be adjusted as required to ensure the boardroom multimedia equipment is operating as required when Canada uses them, and any recurring issues must be reported to Canada so that they can be addressed.

(3) The JUS On-Site Support Service must facilitate all warranty repairs with the manufacturer including:

a) obtaining spare parts or a Return Merchandise Authorization (RMA);

b) shipping the defective product back to the manufacturer and obtaining replacements; and

c) facilitating on-site replacement or servicing of under-warranty defective equipment.

3.8 IT Service Management

(1) The JUS On-Site Support Service must participate in Incident Management, Problem Management, Configuration Management, Change Management, Release Management, Configuration Management, Asset Management and Software License Management when these processes require on-site contact.

3.8.1 Incident Management

(1) The JUS On-Site Support Service must perform Incident Management according to the HDS Managed Service Incident Management process (refer to General SOW, Incident Management subsection).

3.8.2 Problem Management

(1) The JUS On-Site Support Service must participate in Problem Management in compliance with the Problems Management process (refer to General SOW, Problem Management subsection).

3.8.3 Change Management

(1) The JUS On-Site Support Service must participate in Change Management in compliance with the Change Management process (refer to General SOW, Change Management subsection).

3.8.4 Release Management

(1) The JUS On-Site Support Service must participate in Release Management in compliance with the Release Management process (refer to General SOW, Release Management subsection).

3.8.5 Configuration Management, Asset Management and Software License Management

(1) The JUS On-Site Support Service must participate in Configuration Management in compliance with the Configuration Management process (refer to General SOW, Configuration Management subsection).

(2) The JUS On-Site Service must ensure that updates to the Asset Management, Software License Management and Configuration Management information in the Configuration Management Database (CMDB) repository are made as a result of IT Service Management processes.

(3) The JUS On-Site Support Service is responsible for supporting IT Asset Management and Software License Management by:

a) registering software licences in the CMDB when deploying new software components;

b) registering IT-related products in the CMDB when deploying new components;

c) maintaining the identification of registered workstations, monitors, printers, scanners, blackberries, etc;

d) managing asset disposal in accordance with Canada procedures, policies and regulations;

e) assisting Canada with a physical audit as required;

f) complying with Canada policies and guidelines for physical security of computer assets;

and

g) performing asset assignment for End Users by updating the CMDB.

4 TRAINING

(1) The Contractor must provide training on its JUS On-Site Support Service processes, procedures and tools to Canada Regional On-Site Support Personnel using web-based training technology.

(2) The Contractor must provide three (3) half day virtual interactive training sessions to regions in English and French every year.

(3) The Contractor must provide copies of the JUS On-Site Support Service processes, procedures and tool user guides on the Service Delivery Portal.

5 SERVICE LEVEL TARGETS

(1) The JUS On-Site Support Service must have the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for the Standard Service Level Plan:

a) SLT-OSSMTOS-1 (On-Site HDS Support Maximum Time On-Site Standard);

b) SLT-ESSMTR-1 (On-Site HDS Support Maximum Time to Restore Standard).

(2) The JUS On-Site Support Service must have the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for the Premium Service Level Plan:

a) SLT-OSSMTOS-2 (On-Site HDS Support Maximum Time On-Site Premium);

b) SLT-ESSMTR-2 (On-Site HDS Support Maximum Time to Restore Premium).

6 REPORTING

(1) The JUS On-Site Support Service must provide a monthly Device Deployment report to Canada in tabular and graphical format that includes :

a) the number of devices scheduled for refresh;

b) the number of devices refreshed; and

c) the number of new devices installed.

(2) The JUS On-Site Support Service must provide an adhoc Device Disposal report to Canada in tabular format that includes :

a) device asset tag;

b) device type;

c) disposal date;

d) disposal method; and

e) disposal destination.

(3) The JUS On-Site Support Service must provide a monthly Preventive Maintenance report to Canada in tabular format that includes :

a) the asset number of the maintained device;

b) the device type;

c) the maintenance date;

d) the asset location;

e) resulting Incident Tickets if any; and

f) the preventive maintenance performed.

(4) The JUS On-Site Support Service must provide a monthly Multimedia Incident report to Canada in tabular format that includes :

a) the Incident Ticket number;

b) the Incident date;

c) the affected boardroom;

d) the affected equipment;

e) the description of the Incident; and

f) the Incident resolution.

Department of Justice Canada
Help Desk and Support Services

Appendix C to Annex A
Service Domain: JUS Engineering Service

PROTECTED B

Version 2.0 - FINAL
August 15, 2016

Document Change Log

Version	Date	Authors(s)	Description of Change(s)
1.0	2014-06-30	Share Service Canada	Draft
1.1	2016-02-11	Truong-Vu Nguyen	- Cover page from SSC to Justice Canada - Replace 'SSC HDS Managed Service' by 'JUS HDS Services' (Department of Justice Help Desk and Support Services) - Replace 'SSC' by 'Justice Canada' - Replace 'HDS' by 'HDS'
2.0	2016-08-12	Vu Nguyen	Final version

Table of Contents

1 INTRODUCTION

(1) This section is provided for information only.

(2) The JUS Engineering Service established by the Contractor will be responsible for accepting and resolving Incidents and Service Requests assigned to them. In conjunction with the JUS Service Desk Service, the HDS On-Site Support Service and other Canada resolver groups, the JUS Engineering Service will act as the Level 3 Support group for Incidents requiring highly specialized technical skills and as such is expected to handle a small number of Incidents. The JUS Engineering Service will perform the duties of a Level 3 Support group for Operating System Images, software packages and the desktop management tools.

(3) The JUS Engineering Service objectives are:

a) to handle Incident Tickets that require advanced technical skills for software packages;

b) to handle Service Requests to prepare software packages;

c) to distribute software packages;

d) to keep operating system (OS) images and software packages up-to-date;

e) to patch devices;

f) to restore normal service operation as quickly as possible with minimum disruption to End Users, thus ensuring that the best achievable levels of service and availability are maintained;

g) to assist the Service Desk in managing information concerning Problems, and be responsible for problem trend analysis; and

h) to help identify and lower the overall cost of ownership for Information Technology (IT)Services as a whole.

(4) This annex describes the requirements for the JUS Engineering Service.

2 JUS ENGINEERING SERVICE

(1) The JUS Engineering Service is one of the HDS. When ordered by Canada, by issuing a Service Order, the JUS Engineering Service, as managed and implemented by the Contractor, must meet or exceed all of the requirements listed in this section of the Statement of Work (SOW), in the balance of the SOW and elsewhere in the Contract prior to acceptance by Canada and during the entire period specified in each Service Order.

(2) The Contractor must supply all hardware and software, except Government Furnished Equipment, for the JUS Engineering Service.

(3) The JUS Engineering Service infrastructure must be located at Canada Service Delivery Points.

(4) The Contractor must provide the JUS Engineering Service SCI:WES which allows Canada to obtain desktop engineering support services for its OS images and software packages.

2.1 Coverage Area and Standard Hours of Service

(1) The Contractor must provide the JUS Engineering Service in a Canada Service Delivery Point as agreed to between the Contractor and Canada.

(2) The Contractor must provide the JUS Engineering Service from 8:00 ET to 17:00 ET on FGWDs.

2.2 Personnel

(1) The Contractor must staff the JUS Engineering Service with personnel with the right skills, in the right quantity, at the right time and at the right place to meet the Service Level Targets.

2.2.1 Continuous Training

(1) The Contractor must provide at no additional cost to Canada all training the JUS Engineering Service personnel require to fulfil their duties with competence and effectiveness at all time during the Contract period.

2.3 Desktop Management Tool

(1) The JUS Engineering Service must use the mandatory GFE Microsoft System Centre Configuration Manager (version specified by Canada), as the desktop management tool.

(2) Canada will provide the security software required to secure the desktop management tool.

(3) Canada will provide server hosting up to the OS level in Canada data centres and the Contractor must install the desktop management tool on these servers.

(4) Canada will provide access to the management network from the servers so the Contractor can administer the desktop management tool.

(5) Canada will provide access to the desktop management tool from the Contractor SDP using Canada's secure remote access solution to allow the Contractor to remotely support End Users, to distribute software and to perform other required desktop administration actions.

(6) The JUS Engineering Service must implement any out-of-the-box capability of the desktop management tool as specified by Canada from time to time.

(7) The JUS Engineering Service must install and configure the desktop management tool to minimize the need to perform on-site work by implementing, at minimum, these capabilities:

a) remote administration of devices;

b) automatic distribution of OS Images;

c) automatic distribution of patches;

d) automatic distribution of upgrades;

e) automatic distribution of software;

f) self-service application store;

g) device and user policy management;

h) asset auto-discovery;

i) automatic collection of IT asset information on hardware and software licenses; and

j) automatic collection of software usage.

(8) The JUS Engineering Service must submit an implementation strategy for the desktop management tool before the end of the Operational Readiness Phase (see Annex A General SOW, Operational Readiness Phase subsection) for approval by Canada that includes:

a) a list of Canada key requirements;

b) a summary of key architecture driver requirements;

c) an assessment of the currently installed desktop management tool;

d) strategy to expedite the implementation;

e) an option analysis for the implementation approach choosing upgrading or re-installing;

f) a recommendation for the installation approach; and

g) an implementation plan for the recommended approach.

(9) The JUS Engineering Service must submit a design for the desktop management tool before the end of the Operational Readiness Phase (see Annex A General SOW, Operational Readiness Phase subsection) for approval by Canada.

(10) The design for desktop management tool must include:

a) an architecture and design of the various components with particular emphasis on the component interfaces;

b) design specifications for all system interfaces between the desktop management tool and other components; and

c) a deployment architecture that describes the allocation of logical service components to virtual and/or physical computing nodes and highlights the redundancy, scalability and security features of the architecture that support the achievement of all required service levels.

(11) The design for the desktop management tool must ensure that cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for the desktop management tool:

a) use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by Communications Security Establishment of Canada (CSEC), validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSA-11E (http://www.cse-cst.gc.ca/its-sti/publications/itsa-asti/itsa11e-eng.html) or in any subsequent version;

b) be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (http://www.cse-cst.gc.ca/its-sti/services/industry-prog-industrie/cmvp-pvmc-eng.html) to at least Federal Information Processing Standard (FIPS) 140-2 validation at Level 1; and

c) operate in FIPS Mode.

(12) The design for desktop management tool must conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg22-eng.pdf) and ITSG-38 (http://www.cse-cst.gc.ca/documents/publications/itsg-csti/itsg38-eng.pdf).

(13) The design for the desktop management tool must conform to security requirements, as specified by Canada, including but not limited to:

a) role based access control with least privilege;

b) separation of duties;

c) integrity control of Canada software;

d) prevent tampering with software images;

e) secured remote control sessions;

f) logging any action performed with the tool so it is fully auditable;

g) antivirus protection;
h) data loss prevention;
i) intrusion detection and prevention;
j) white listing of applications; and
k) persistent threat detection.

(14) The JUS Engineering Service must implement the desktop management tool in compliance with the approved implementation methodology and design when requested by Canada after the Transition-In (see Annex A General SOW, Transition-In subsection).

(15) The JUS Engineering Service must support and perform system management of the desktop management tool.

(16) The JUS Engineering Service must resolve Incidents for the desktop management tool.

3 DEVICE ENGINEERING SUPPORT

(1) The JUS Engineering Service must provide Level 3 Support for the OS images and software installation packages identified in the following table in Appendix C: Standard Hardware and Software List:

a) Table 3 – OS Image

b) Table 5 – SCCM Packages L3

(2) The scope of the JUS Engineering Service Level 3 Support the Contractor must provide is limited to OS Images and software installation packages distributed with the desktop management tool and to administrative functions that can be performed centrally with the desktop management tool.

(3) For clarity, the JUS Engineering Service must not provide Level 3 Support for the software products. The support is limited to the OS Images and the installation packages.

3.1 Service Remediation

(1) The JUS Engineering Service must work on Incidents assigned to them.

(2) The JUS Engineering Service must prioritize its efforts according to the priority of the Incident Ticket (see General SOW subsection Incident Management) where Incidents with the highest priority are resolved first.

(3) Upon receiving an Incident assigned by the JUS Service Desk Service or the Service Manager, the JUS Engineering Service must:

a) assign the Incident Ticket to a JUS Engineering Service representative;

b) confirm acceptance of the Incident Ticket to the JUS Service Desk Service;

c) contact the appropriate Contractor and/or other Canada representative(s) to confirm the assignment, if required;

d) use the desktop management tool to attempt to remotely resolve the Incident if necessary;

e) co-operatively work with Canada and any other third parties as requested by Canada to resolve Incidents as required;

f) involve other resolution groups as required;

g) report the resolution of the Incident to the appropriate Contractor and/or Canada representative(s);

h) conduct appropriate testing to ensure that the work was completed properly;

i) update the Incident Ticket promptly according to the Service Level Targets;

j) ensure that all applicable procedures, standards and quality controls have been adhered to; and

k) ensure that the Incident Ticket is properly “closed”.

3.2 Service Requests

(1) The JUS Engineering Service must accept and execute Service Requests assigned to it from the JUS Service Desk Service.

3.3 IT Service Management Activities

(1) The JUS Engineering Service must participate in Incident Management, Problem Management, Change Management, Release Management, Configuration Management, Asset Management and Software License Management when these processes as required.

3.3.1 Incident Management

(1) The JUS Engineering Service must perform Incident Management according to the HDS Managed Service Incident Management process (refer to General SOW, Incident Management

subsection).

3.3.2 Problem Management

(1) The JUS Engineering Service must participate in Problem Management in compliance with the Problem Management process (refer to General SOW, Problem Management subsection).

3.3.3 Change Management

(1) The JUS Engineering Service must participate in Change Management in compliance with the Change Management process (refer to General SOW, Change Management subsection).

3.3.4 Release Management

(1) The JUS Engineering Service must participate in Release Management in compliance with the Release Management process (refer to General SOW, Release Management subsection).

3.3.5 Configuration Management, Asset Management and Software License Management

(1) The JUS Engineering Service must ensure that updates for Asset Management, Software License Management and Configuration Management are made to the Configuration Management Database (CMDB) repository as a result of IT Service Management processes.

3.4 Engineering Support

(1) The JUS Engineering Service must provide engineering support for software installation packages and OS images managed by the desktop management tool.

(2) The JUS Engineering Service must escalate technology issues to the Service Manager for review by Canada.

(3) The JUS Engineering Service must adapt, tune, and improve the desktop management tool to ensure optimal performance.

(4) The JUS Engineering Service must assess capacity requirements for the HDS and provide recommendations for capacity changes.

(5) The JUS Engineering Service must evaluate Canada's technical, functional, and operational requirements to offer technology suggestions and solutions to technology issues.

3.5 Security and Configuration Policy Management

(1) The JUS Engineering Service must apply security and configuration policies on any given device as specified by Canada.

(2) The JUS Engineering Service must provide to Canada for approval a test plan to fully test the new or updated policy.

(3) The JUS Engineering Service must execute the test plan approved by Canada and provide Canada with the test results for approval.

(4) When the test results for the new or updated policy are approved by Canada, the JUS Engineering Service must:

a) store device policy as Configuration Items in the CMDB; and

b) invoke the Release Management Process to distribute the new or updated policy.

3.6 OS Image Management

(1) The goal of OS Image Management is to maintain the currency of both deployed and deployable images.

(2) The JUS Engineering Service OS Image Management must be initiated by a Change Request to integrate new or changed software components that are part of an OS image.

(3) The JUS Engineering Service must update the OS Image from updated software components from the Definitive Software Library.

(4) The JUS Engineering Service must group updated software components into a release as specified by Canada.

(5) The JUS Engineering Service must ensure the updated OS Image is still in compliance with Canada build books and Canada security configurations requirements as specified by Canada.

(6) The JUS Engineering Service must scan the updated OS Image with malware detection tools as specified by Canada.

(7) The JUS Engineering Service must provide to Canada for approval a verification test plan to test the updated OS Image.

(8) The JUS Engineering Service must execute the verification test plan approved by Canada and provide Canada with the test results for approval.

(9) When the test results for the updated OS Image are approved by Canada, the JUS Engineering Service must:

a) store updated OS Image as Configuration Items in the CMDB and in the Definitive Software Library; and

b) invoke the Release Management Process to make the updated OS Image available for distribution.

3.7 New OS Image Development

(1) The goal of OS Image Development is to develop new images to be available for deployment via Device Deployment or live updates.

(2) The JUS Engineering Service must create new OS Images as and when requested by Canada in a Service Request.

(3) The JUS Engineering Service must create new OS Images from software components in the Definitive Software Library.

(4) The JUS Engineering Service must configure the new OS Image in compliance with Canada build books and Canada security configuration requirements.

(5) The JUS Engineering Service must scan the new OS Image with malware detection tools as specified by Canada.

(6) The JUS Engineering Service must provide to Canada for approval a verification test plan to test the configuration of the new OS Image.

(7) The JUS Engineering Service must execute the test plan approved by Canada and provide Canada with the test results for approval.

(8) When the test results for the new OS Image are approved by Canada, the JUS Engineering Service must:

a) store new OS Image as Configuration Items in the CMDB and in the Definitive Software Library; and

b) invoke the Release Management Process to make the new OS Image available for automated distribution.

3.8 Component Integration

(1) The JUS Engineering Service Component Integration must be initiated by the Change Management process or a Service Request.

(2) The JUS Engineering Service must ensure:

a) the stability of the system with the introduction, modification, configuration, reinstallation and removal of new software components;

b) minimal impact to currently deployed software components by the introduction, update or removal of a software component;

c) that new software components function as designed within a managed configuration;

d) that the managed configuration is not impacted by the update or removal of a software component; and

e) that all deployed software components can be tracked and reported.

(3) The JUS Engineering Service must create a Software Package for the software component ensuring that:

a) installation, modification, reinstallation, removal and configuration routines for software components is as transparent and unobtrusive to End User as possible while providing the ability to monitor the status during their execution;

b) there is minimal impact to End User data and settings during the execution of the installation, modification, configuration, reinstallation and removal routines;

c) software components are self-configurable after installation routine;

d) conflict and dependency resolution is built-in to the installation, modification, reinstallation, configuration and removal routines;

e) every software component provide an installation, modification, configuration, removal and reinstallation routine;

f) installation, modification, reinstallation, removal and configuration routines minimize the required reboots with a goal of none;

g) installation, modification, reinstallation, removal and configuration routines do not require any End User input unless absolutely necessary;

h) installation of software component leaves source files on device for easy configuration, modification, reinstallation and removal; and

i) installation, modification, configuration, reinstallation and removal routines only execute on authorized devices (i.e. device policy).

(4) The JUS Engineering Service must scan software components with malware detection tools as specified by Canada.

(5) The JUS Engineering Service must document the software components to provide supporting organizations sufficient information to resolve incidents.

(6) The JUS Engineering Service must include in the software component repository all information pertaining to a software component, e.g. source files, documentation, routines, final package, signoffs, test plans, etc.

(7) The JUS Engineering Service must implement version control on all software components.

(8) The JUS Engineering Service must track package lifecycle (creation, publishing, production, retirement) including User Acceptance Testing signoff.

(9) The JUS Engineering Service must support an environment for application support and User Acceptance Testing of business applications.

(10) The JUS Engineering Service must provide to Canada for approval a test plan to verify the software component installation.

(11) The JUS Engineering Service must execute the test plan approved by Canada and provide Canada with the test results for approval.

(12) When the test results for the software component installation are approved by Canada, the JUS Engineering Service must:

a) store the software component as Configuration Items in the CMDB and in the Definitive Software Library; and

b) invoke Release Management Process to make the software component available for automated distribution.

3.9 Patch management

(1) The main goal of Patch Management is to protect devices from security vulnerabilities in the OS and software components deployed.

(2) The JUS Engineering Service must perform software updates, driver updates, firmware updates, and patch management for software components.

(3) The JUS Engineering Service must monitor software for patches, updates, hot fixes, firmware updates, or other updates that may require a software component to be updated and provide

Canada with a weekly update plan for approval by Canada.

(4) The JUS Engineering Service must perform Patch Management in compliance with the approved Configuration Management Plan (refer to General SOW, Configuration Management Plan subsection).

(5) The JUS Engineering Service must update software components impacted by patches (refer to Component Integration subsection).

4 SERVICE LEVEL TARGETS

(1) The JUS Engineering Service must have the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for the Standard Service Level Plan:

a) SLT-ES-MTTRTI-1 (Escalated Support - Maximum Time to Respond to Incident – Standard); and

b) SLT-ES-MTTRFI-1 (Escalated Support - Maximum Time to Restore from Incident – Standard).

(2) The JUS Engineering Service must have the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets) for the Premium Service Level Plan:

a) SLT-ES-MTTRTI-2 (Escalated Support - Maximum Time to Respond to Incident – Premium); and

b) SLT-ES-MTTRFI-2 (Escalated Support - Maximum Time to Restore from Incident – Premium).

(3) The JUS Engineering Service must have the following Service Level Targets (refer to Annex A: General SOW, subsection Service Level Targets):

a) SLT-ES-MTDCSU (Escalated Support – Maximum Time to Deploy Critical Security Update).

5 REPORTING

(1) The JUS Engineering Service must provide a monthly OS Image and Deployment report to Canada in tabular and graphical format that includes :

a) the number of OS Images created;

b) the number of OS Images updated;

c) the number of OS Images released in the month;

d) the number of successful OS Image deployments; and

e) the number of failed OS Image deployments.

(2) The JUS Engineering Service must provide a monthly Software Package and Deployment report to Canada in tabular and graphical format that includes :

a) the number of Software Packages created;

b) the number of Software Packages updated;

c) the number of Software Packages released in the month;

d) the number of successful Software Package deployments; and

e) the number of failed Software Package deployments.

(3) The JUS Engineering Service must provide a monthly Patches and Deployment report to Canada in tabular and graphical format that includes :

a) the number of Software Patches created;

b) the number of Software Patches released in the month;

c) the number of successful Software Patches deployments; and

d) the number of failed Software Patches deployments.

(4) The JUS Engineering Service must provide a monthly Policy Deployment report to Canada in tabular and graphical format that includes :

a) the number of policies created;

b) the number of policies applied;

c) the number of policy compliant devices; and

d) the number of non-compliant devices.

(5) The JUS Engineering Service must provide a monthly Policy Status report to Canada in tabular and format that includes :

a) A list of policies by device type.

Department of Justice Canada
Help Desk and Support Services

Appendix D to Annex A
Security Requirements

Table of Contents

The JUS HDS Services security requirements are listed in Table 1 - Security Requirements below. Each row of the table lists one or many Security Requirements that are of the same Type and that are assessed with the same Method of Assessment. The table contains the following columns:

Security Requirement

The Security Requirement column provides one or many security requirements identifier followed by a narrative description of the security requirements. The security requirement identifier (SEC ID) is the number in bold in the Security Requirement column that starts with “SR-“ followed by a sequence number and a colon.

Some security requirements are included in this Appendix by reference. The description of the security requirement is in the SOW rather than in this Appendix. For those security requirements, the narrative description refers to the SOW section where the description of the security requirement can be found. Consequently, the SOW contains a reference to the SEC ID that looks like this: ***<TRACEFROM>SEC ID</TRACEFROM>***. When this trace tag is found in the SOW, it means that the tagged clause represents the description of the security requirement. Only a small number of security requirements are described in the SOW to enhance its readability.

Type

The Type column indicates to the Contractor the type of the security requirement in the Security Requirement column. The types that will be utilized are:

a) **Basic**: The implementation of the security requirement(s) from the corresponding Security Requirement column must be included in the “Basic Per User Monthly Price” of pricing table 1-Service Desk Services in Annex B - Pricing and Financial Evaluation.
b) **Enhanced**: The implementation of the security requirement(s) from the corresponding Security Requirement column must be included in the “Premium for Enhanced Per User Monthly Price” of pricing table 1-Service Desk Services in Annex B - Pricing and Financial Evaluation.

Method of Assessment

The Method of Assessment column indicates to the Contractor how Canada will assess that the security requirement(s) in the Security Requirement column is (are) met. The assessment methods that will be utilized are:

a) **Examine:** A type of assessment method that is characterized by the process of checking, inspecting, reviewing, observing, studying, or analyzing one or more assessment objects to facilitate understanding, achieve clarification, or obtain evidence, the results of which are used to support the determination of security control effectiveness over time.

b) **Interview**: A type of assessment method that is characterized by the process of conducting discussions with individuals or groups within an organization to facilitate understanding, achieve clarification, or lead to the location of evidence, the results of which are used to support the determination of security control effectiveness over time.

c) **Test**: A type of assessment method that is characterized by the process of exercising one or more assessment objects under specified conditions to compare actual with expected behaviour, the results of which are used to support the determination of security control effectiveness over time.

Table 1 - Security Requirements

Security Requirement	Type	Method of Assessment
SR-1: The Contractor must develop, disseminate, review, and update annually, the access control policies and associated access control requirements for JUS HDS Services Infrastructure components.	**Basic**	**Examine:** Operational artefacts - Access control policy and procedures, supporting audit and compliance reports. **Interview:** Contractor personnel with access control responsibilities
SR-2: The Service Delivery Portal Identification and Authentication (I&A) Service must automatically provision Service Delivery Portal Accounts for End User Accounts and generic Accounts, as follows: a) assign a unique display name in accordance with the standard defined including the naming conventions, by applying configurable naming and conflict resolution rules; b) create an Service Delivery Portal Account with no privileges; c) assign a one-time temporary password to the Service Delivery Portal Accounts; d) assign Service Delivery Portal Account attributes and security access privileges as specified by Justice Canada; and e) return the assigned display name, Client unique key, Contractor unique key and one-time password to the Service Delivery Portal Account requester. **SR-3**: The Service Delivery Portal I&A Service must prevent the re-use of a Service Delivery Portal Account as specified by Justice Canada. **SR-4**: The Service Delivery Portal I&A Service must allow Service Delivery Portal Account suspension policies as specified by Justice Canada.	**Basic**	**Examine:** secure Software Development Life Cycle (SDLC) artefacts - JUS HDS Services access control policy; procedures addressing Account management; security plan; list of active system Accounts along with the name of the individual associated with each Account; list of guest, anonymous and temporary Accounts along with the name of the individual associated with each Account and the date the Account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled JUS HDS Services system Accounts along with the name of the individual associated with each Account; system-generated records with End User IDs and last login date; other relevant documents or records. **Interview:** Contractor personnel with Account management responsibilities.

Security Requirement	Type	Method of Assessment
SR-5: The Service Delivery Portal I&A Service must not allow access to a suspended Service Delivery Portal Account. **SR-6**: The Service Delivery Portal I&A Service must not allow direct access to the JUS HDS Services Infrastructure for any Service Delivery Portal Account, as specified by Justice Canada.		
SR-7: The Contractor must manage JUS HDS Services Infrastructure Operators Accounts by: a) identifying Account types (i.e., individual, group, system, Device, application, guest, anonymous, and temporary); b) establishing conditions for group membership; c) identifying authorized Operators of the JUS HDS Services Infrastructure and specifying access privileges; d) requiring appropriate approvals for requests to establish Accounts; e) selecting an identifier that uniquely identifies the Operator or Device; f) assigning the Operator identifier to the intended party or the Device identifier to the intended Device; g) establishing, activating, modifying, disabling, and removing Accounts; h) specifically authorizing and monitoring the use of guest,anonymous and temporary Accounts; i) notifying Account Administrator when temporary Accounts are no longer required and when JUS HDS Services Infrastructure Operators are terminated, transferred, or JUS HDS Services Infrastructure usage or need-to-know or need-to-share changes; j) preventing re-use of identifiers for at least one year; k) deactivating: i) temporary Accounts that are no longer required; ii) Accounts of terminated or transferred Operators; iii) Accounts after a number of day of inactivity as specified by Justice Canada, and iv) temporary and emergency Accounts over a given age; l) granting access to the JUS HDS Services Infrastructure based on:	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services access control policy; procedures addressing Account management; security plan; list of active system Accounts along with the name of the individual associated with each Account; list of guest, anonymous and temporary Accounts along with the name of the individual associated with each Account and the date the Account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled JUS HDS Services system Accounts along with the name of the individual associated with each Account; system-generated records with user IDs and last login date; other relevant documents or records. **Interview:** Contractor personnel with Account management responsibilities.

Security Requirement	Type	Method of Assessment
(i) a valid access authorization; (ii) intended system usage, and (iii) other attributes as required by the Contractor or Justice Canada; m) reviewing Accounts at least monthly; n) locking the Account after ten unsuccessful login attempts occurring within five minutes, and o) keeping the Account locked until manually unlocked by another Operator.		
SR-8: The JUS HDS Services must log the following events: a) Account creation; b) Account modifications; c) Account access; d) Account suspension; e) Account termination; f) Account deletion; and g) Account views of which the End User is not the primary owner.	**Basic**	**Examine:** Development/design artefacts – detailed design, configuration and build books; **Examine:** Operational artefacts - Account management procedures, audit and compliance reports; **Examine:** Security test and evaluation (ST&E) results
SR-9: The Contractor must define a working hours policy and monitor JUS HDS Services Infrastructure Operators Accounts utilization against that policy including: a) logging atypical usage of Operator Accounts; and b) alerting designated resources of atypical usage of Operator Accounts. The Contractor must provide the JUS HDS Services Infrastructure Operators Accounts atypical utilization log to Canada within 1 FGWD of a request by Justice Canada. The Contractor must ensure that JUS HDS Services Infrastructure Operators log out at the end of their working shift.	**Basic**	**Examine:** Operational Artefacts - Account management procedures, security reports, audit/compliance reports; **Examine:** Development/Installation Artefacts - Configuration/build books, Detailed Design; **Interview:** Contractor Operational Resources
SR-10: The JUS HDS Services Infrastructure must enforce access authorizations for Operators.	**Basic**	**Examine:** Development/Installation Artefacts - Configuration/build books; **Examine:** Operational Artefacts - Access control policy, access enforcement procedures,

Security Requirement	Type	Method of Assessment
SR-11: The Service Delivery Portal I&A Service must secure access as follows: a) secure access connection (e.g. TLS); b) minimize the requirement for additional Service Delivery Portal Account logins to the various services; c) request the JUS HDS Services unique user id and password for access; d) require an authentication using an X.509 credential, that has been issued by an Justice Canada approved certificate authority, for Service Delivery Portal Accounts that have been identified as requiring a stronger authentication for access, as specified by Justice Canada; and e) enforce a configurable idle session timeout period, as specified by Justice Canada.		audit/compliance reports, approved user privileges authorization records; **Test:** ST&E results confirming the implemented access control policy is being enforced.
SR-12: The JUS HDS Services must detect violations of data loss prevention policies and apply response actions, as specified by Justice Canada. **SR-13**: The service design for JUS HDS Services must conform to network security zoning in accordance with IT Security Guidance (ITSG) ITSG-22 (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg22-eng_0.pdf) and ITSG-38 (https://www.cse-cst.gc.ca/en/system/files/pdf_documents/itsg38-eng_0.pdf). **SR-14**: The JUS HDS Services must block all data flows, as specified by Justice Canada, in the event of failure of the content filtering function.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system identification and Authentication policy; password policy; procedures addressing password management; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records. **Test:** ST&E test results demonstrating automated mechanisms implementing password management functions.
SR-15: The Contractor must implement separation of duties for Operators, as necessary, to prevent malevolent activity without collusion according to the role-based access profile assigned to the Operator.	**Basic**	**Examine:** Development/Installation Artefacts - Design Documentation, configuration/build books; **Examine:** Operational Artefacts - Access control policy, access enforcement and separation of duties procedures, list of approved privileged commands and approved user privileges

Security Requirement	Type	Method of Assessment
		authorization; **Interview:** Contractor personnel with access enforcement responsibilities; **Test:** ST&E results related to separation of duties or dual authorization mechanisms.
SR-16: The Contractor must implement a least privileges policy for JUS HDS Services Infrastructure Operators as follows: a) the access control mechanisms must be configured to implement least privilege, allowing only authorized accesses for Operators (and processes acting on their behalf) that are necessary to accomplish assigned tasks; b) create non-privileged accounts to be used for non-operations tasks; c) restrict authorization to super user accounts (e.g., root) to designated Operators; d) restrict sharing of Operator Accounts; and e) must uniquely identify the human Operator who has performed each operation on the JUS HDS Services Infrastructure.	**Basic**	**Examine:** Development/Installation Artefacts - Design Documentation, configuration/build books; **Examine:** Operational Artefacts - Access control, least privileges and documented details of users & resources requiring enforcement of least privileges policies, access enforcement procedures; **Interview:** Contractor personnel with access enforcement responsibilities **Test:** ST&E result confirming the implementation and operation of least privileges policy.
SR-17: The JUS HDS Services must automatically lock an Account following a number of unsuccessful login attempts as specified by Justice Canada.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system access control policy; procedures addressing unsuccessful login attempts; security plan; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; other relevant documents or records. **Test:** ST&E test results demonstrating automated mechanisms implementing the access control policy for unsuccessful login attempts.

Security Requirement	Type	Method of Assessment
SR-18: The JUS HDS Services must display a logon banner approved by Canada on the login page of any web-based application for End Users. **SR-19**: The JUS HDS Services Infrastructure must include an access control mechanism that: a) prevents access to JUS HDS Services Infrastructure components or resources without identification, authentication, and authorization; b) displays a Justice Canada-approved logon warning banner that authorized Operators must acknowledge prior to being granted access to JUS HDS Services Infrastructure components; c) notifies the Operators, upon successful logon (access), of the date and time of the last logon (access), and d) uses a readily observable logout capability whenever authentication is used to gain access to JUS HDS Services Infrastructure components. **SR-20**: The JUS HDS Services Infrastructure access control mechanisms must include an Operator session lock mechanism that: a) prevents further access to JUS HDS Services Infrastructure components by automatically initiating an Operator session lock after a period of inactivity no longer than 60 minutes; b) prevents further access to JUS HDS Services Infrastructure components by initiating an Operator session lock when requested by the Operators; c) displays a screen saver that contains no meaningful information to completely replace what was previously displayed on the screen upon activation of an Operator session lock, and d) unlocks an Operator session after successful Authentication of the Operator.	**Basic**	**Examine:** Operational Artefacts - Access control policy; privacy and security policies; procedures addressing system use notification; documented approval of JUS HDS Services system use notification messages or banners; JUS HDS Services system notification messages; JUS HDS Services system configuration settings and associated documentation; information system audit records for user acceptance of notification message or banner; **Test:** ST&E results related to JUS HDS Services Infrastructure mechanisms implementing the access control policy for system use notification. **Examine:** Development/Installation Artefacts - Design Documentation; **Examine:** Operational Artefacts - Access control policy, configuration settings and procedures related to logon notification; audit results; **Test:** ST&E Artefacts covering the requirements related test results.
SR-21: Any use of Remote Management within the JUS HDS Services Infrastructure	**Basic**	**Examine:** secure SDLC artefacts – JUS HDS Services system access control policy;

Security Requirement	Type	Method of Assessment
must take place using a method approved by Canada that includes: a) Remote Management must be restricted to JUS HDS Services Infrastructure located within a Contractor Service Delivery Point using JUS HDS Services dedicated management consoles. b) Documenting allowed methods of Remote Management and establish usage restrictions and implementation guidance for each allowed remote management method; c) monitoring for unauthorized Remote Management; d) authorizing Remote Management prior to connection; e) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods; f) routing all Remote Management to JUS HDS Services Infrastructure components through a limited number of managed access control points; g) protecting information about Remote Management mechanisms from unauthorized use and disclosure; h) employing automated mechanisms to facilitate the monitoring and control of Remote Management methods.		procedures addressing remote access to the JUS HDS Services system; JUS HDS Services system configuration settings and associated documentation; information system audit records; other relevant documents or records; **Interview:** Contractor personnel with remote access authorization, monitoring, and control responsibilities, with responsibilities for monitoring remote connections to the information system. **Test:** ST&E test results that demonstrate remote access methods for the information system as per security requirements.
SR-22: The Contractor must not allow wireless access to the JUS HDS Services Infrastructure.	**Basic**	**Examine:** Development/Installation Artefacts - Design documentation, configuration settings; **Examine:** Operational Artefacts - Access control policy, procedures addressing wireless implementation disabling, audit reports of systems; **Test:** ST&E results demonstrating the disabling of all wireless capabilities with JUS HDS Services Infrastructure.
SR-23: The Contractor must: a) continuously monitor for wireless access points on the JUS HDS Services Infrastructure; b) immediately disable any wireless access point when one is discovered, and c) open an Incident Ticket for a Security Incident if a wireless access point is discovered.	**Basic**	**Examine:** Operational Artefacts - Access control policy, procedures addressing wireless implementation disabling, audit reports of systems; **Interview:** Contractor personnel responsible for monitoring wireless connections to JUS HDS Services Infrastructure;

Security Requirement	Type	Method of Assessment
		Test: ST&E results demonstrating the disabling of all wireless capabilities with JUS HDS Services Infrastructure.
SR-24: The Contractor must permanently disable all wireless networking functions internally embedded within JUS HDS Services Infrastructure.	**Basic**	**Examine:** Operational Artefacts - Access control policy, procedures addressing wireless implementation disabling, audit reports of systems; **Interview:** Contractor personnel responsible for monitoring wireless connections to JUS HDS Services Infrastructure; **Test:** ST&E results demonstrating the disabling of all wireless capabilities with JUS HDS Services Infrastructure.
SR-25: The Contractor must not allow Mobile Devices to access the JUS HDS Services Infrastructure. The Contractor must not allow the use of Mobile Broadband Modems on the JUS HDS Services Infrastructure. The Contractor must limit the use of Contractor-controlled portable storage media (e.g., thumb drive) as follows: a) restrict the use to authorized Operators only, and b) restrict the use to JUS HDS Services Infrastructure Components only. The Contractor must prohibit the use of VoIP technologies in the JUS HDS Services Infrastructure unless specifically authorized by Justice Canada.	**Basic**	**Examine:** Operational Artefacts - Access control policy, procedures addressing use of portable/mobile devices implementation disabling, audit reports of systems; **Examine:** Development/Installation Artefacts - Detailed Design documents; **Interview:** Contractor personnel responsible for monitoring mobile devices use within JUS HDS Services Infrastructure; **Test:** ST&E results demonstrating the disabling of access to all Mobile Devices with JUS HDS Services Infrastructure.
SR-26: The Contractor must obtain Justice Canada's approval for the use of third party	**Basic**	**Examine:** Operational Artefacts - Access control policy; procedures addressing the use of external information systems; external

Security Requirement	Type	Method of Assessment
(i.e., non-Contractor) information systems for the delivery of JUS HDS Services.		information systems terms and conditions; list of types of applications accessible from external information systems; maximum security categorization for information processed, stored, or transmitted on external information systems; information system configuration settings and associated documentation; **Interview:** Contractor personnel with responsibilities for defining terms and conditions for use of external information systems to access organizational systems.
SR-28: The Contractor must obtain Justice Canada's approval before making any JUS HDS Services content publicly available.	**Basic**	**Examine:** Operational Artefacts - Access control policy; procedures addressing the use of portable storage media; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system connection or processing agreements; account management documents.
SR-29: The Contractor must include in the operational security procedures how the security awareness and training requirements are addressed.	**Basic**	**Examine:** Operational Artefacts - Security awareness and training policy and procedures; other relevant documents or records; **Interview:** Contractor personnel with security awareness and training responsibilities.
SR-30: The Contractor must provide security awareness and training for JUS HDS Services Infrastructure Operators as follows: a) as part of initial training for new Operators; b) before authorizing access to the JUS HDS Services Infrastructure or performing assigned duties; and c) annually or when security impacting changes to the JUS HDS Services occur.	**Basic**	**Examine:** Operational Artefacts - Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of GC policies; security awareness training curriculum; security awareness training materials; training records; **Interview:** Contractor personnel comprising the JUS HDS Services system Administrator and

Security Requirement	Type	Method of Assessment
		Operator user community.
SR-31: The Contractor must monitor and document security awareness and training for JUS HDS Services Infrastructure Operators including: a) documenting who received what awareness and training course and when, and b) retaining records for the last 3 years.	**Basic**	**Examine:** Operational Artefacts - Security awareness and training policy; procedures addressing security awareness training implementation; appropriate codes of GC policies; security awareness training curriculum; security awareness training materials; training records; **Interview:** Contractor personnel comprising the JUS HDS Services system Administrator and Operator user community.
SR-32: The Contractor must include in the operational security procedures details of how the audit and accountability requirements specified in this SOW are addressed.	**Basic**	**Examine:** Development/Installation Artefacts - Design Documentation, configuration details; **Examine:** Operational Artefacts - Access control and remote access policy, procedures for remote access, audit reports of monitoring related to remote access; **Test:** ST&E test results related to remote access controls and monitoring.
SR-33: The JUS HDS Services must log and centrally manage the following events in accordance with the event logging requirements for Level 3 Assurance, as detailed in ITSG-31: a) successful Authentication; and b) unsuccessful Authentication.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable

Security Requirement	Type	Method of Assessment
		events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.
SR-34: The Contractor must review and update the list of auditable events for JUS HDS Services and the JUS HDS Services Infrastructure on an annual basis and provide the updated list to Justice Canada within five FGWDs of the review. The JUS HDS Services Infrastructure must perform audit logging for all JUS HDS Services Infrastructure components. The Contractor must log events as requested by Justice Canada. The JUS HDS Services Infrastructure must automatically generate real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise. **SR-35**: The Service Delivery Portal I&A Service must log the following transactions for Level 3 Assurance, as detailed in ITSG-31: a) password changes; b) credential registrations; c) password recovery; d) expired credentials. **SR-36**: The JUS HDS Services must log the following events: a) Account creation;	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events. **Examine:** secure SDLC artefacts - JUS HDS Services system audit and accountability policy; procedures addressing content of audit records; list of organization-defined auditable events; JUS HDS Services system audit records; JUS HDS Services system incident reports; other relevant documents or records.

Security Requirement	Type	Method of Assessment
b) Account modifications c) Account suspension; d) Account termination; e) Account deletion; and f) Account views of mailboxes of which the End User is not the primary owner.		**Test:** ST&E test results demonstrating automated mechanisms implementing JUS HDS Services system auditing of auditable events as per SR-35. **Examine:** secure SDLC artefacts - JUS HDS Services system procedures addressing account management; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; other relevant documents or records. **Test:** ST&E test results demonstrating automated mechanisms implementing account management functions.
SR-37: The JUS HDS Services must log the following information for all Administrator activities: a) Administrator identifier; b) date and time stamp of the activity; c) description of the activity performed; and d) data modified by the activity. **SR-38**: The JUS HDS Services audit records must include: a) what type of audit event occurred; b) when (date and time) the audit event occurred; c) where the audit event occurred; d) the audit source of the event; e) the outcome (success or failure) of the audit event, and f) the identity of any user/subject associated with the audit event.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of organization-defined auditable events.

Security Requirement	Type	Method of Assessment
SR-39: The Contractor must perform capacity management on the audit record storage by: a) allocating enough audit record storage capacity; b) configuring auditing to prevent storage capacity being exceeded; c) alerting the Operations Center when the allocated audit record storage volume reaches 75% of the audit record storage capacity; and d) overwriting the oldest audit records if storage reached maximum capacity.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing audit storage capacity; JUS HDS Services system audit records; **Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services-defined audit record storage capacity for JUS HDS Services system components that store audit records; list of JUS HDS Services-defined auditable events; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Test:** ST&E results related to audit record storage capacity and related configuration settings.
SR-40: The JUS HDS Services Infrastructure audit function must respond to auditing failures by: a) real-time alerting the Operations Center; and b) overwriting the oldest audit records if storage reached maximum capacity.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing response to audit processing failures; list of ESP/Justice Canada personnel to be notified in case of an audit processing failure; JUS HDS Services system audit records; **Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; **Test:** ST&E results covering the mechanisms implementing information system response to audit processing failures.
SR-41: The Contractor must perform capacity management on the audit record storage	**Basic**	**Examine:** secure SDLC artefacts -JUS HDS Services audit and accountability policy;

Security Requirement	Type	Method of Assessment
by: a) allocating enough audit record storage capacity; b) configuring auditing to prevent storage capacity being exceeded; and c) alerting the Operations Center when the allocated audit record storage volume reaches 75% of the audit record storage capacity.		procedures addressing audit storage capacity; JUS HDS Services system design documentation; JUS HDS Services-defined audit record storage capacity for JUS HDS Services system components that store audit records; list of JUS HDS Services-defined auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; other relevant documents or records. **Test:** ST&E test results demonstrating audit record storage capacity and related configuration settings.
SR-42: The Contractor must provide all evidence, in a COTS format specified by Justice Canada, associated to a Security Incident, within a time interval specified by Justice Canada that includes: a) results of historical logs and audit records research associated with one or many Clients based on criteria provided by Justice Canada; b) results of analysis of logs and audit records associated with one or many Clients based on criteria provided by Justice Canada; c) logs and audit records based on criteria provided by Justice Canada, and d) additional information or data as specified by Justice Canada. **SR-43**: The Contractor must implement an audit review process that includes: a) review and analysis of JUS HDS Services audit records annually and within 20 FGWDs of a request by Canada for indications of inappropriate or unusual activity; b) report findings of the audit review process to Canada within 10 FGWDs of completion of the audit, and c) adjust the level of audit review, analysis, and reporting when there is a change in risk or as requested by Justice Canada.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events. **Examine:** Operational Artefacts - Audit and

Security Requirement	Type	Method of Assessment
SR-44: The Contractor must: a) report any JUS HDS Services security issues to Justice Canada immediately upon learning of their existence; b) track identified security issues in the JUS HDS Services; and c) report progress to Justice Canada until each security issue is fixed or mitigated. **SR-45**: The Contractor must implement an audit and investigation process that: a) Allows only specific, pre-authorized representatives of Canada to request and receive discrete access and information associated with JUS HDS Services data (user data, event logs) for the purposes of conducting investigations; b) Is approved by Justice Canada. The Contractor must not disclose such access to End Users. The Contractor must report such access to Canada on a monthly basis by Client organization and by Contractor. **SR-46**: The Contractor must provide specified JUS HDS Services data requested by Justice Canada in a COTS file format and media specified by Justice Canada within 1 FGWD of a request by Justice Canada.		accountability policy; procedures addressing audit review, analysis, and reporting; reports of audit findings; records of actions taken in response to reviews and analyses of audit records, threat information documentation from law enforcement, intelligence community, or other sources; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; **Interview:** Contractor personnel with information system audit review, analysis, and reporting responsibilities; **Test:** ST&E test related to JUS HDS Services system audit review, analysis, and reporting capability. **Examine:** Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; **Interview:** Contractor personnel with risk assessment and vulnerability scanning responsibilities. **Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit

Security Requirement	Type	Method of Assessment
		records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.
SR-47: The Contractor must provide all evidence, in a COTS format specified by Justice Canada, associated to a Security Incident, within a time interval specified by Justice Canada that includes: a) results of historical logs and audit records research associated with one or many Clients based on criteria provided by Justice Canada; b) results of analysis and correlation of logs and audit records associated with one or many organizations based on criteria provided by Justice Canada; c) integrates with vulnerability scanning and network monitoring information for analysis, identification of unusual activity; d) logs and audit records based on criteria provided by Justice Canada, and e) additional information or data as specified by Justice Canada.	**Basic**	**Examine:** secure SDLC artefacts - operational policies and procedures detailing the security incident handling and management; JUS HDS Services system configuration settings documentation; **Test:** ST&E test results demonstrating the Security Incident information compliant with SR-47.
SR-48: The JUS HDS Services Infrastructure must allow audit and investigation activities such as: a) Provide Administrator access to any Service Delivery Portal Account that is undetectable to the Account owner; b) identify and process events of interest as defined by Justice Canada.	**Enhanced**	**Examine:** secure SDLC artefacts - Access control policy; procedures addressing JUS HDS Services information flow enforcement; procedures addressing source and destination domain identification and authentication, and information transfer error handling; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; other relevant documents or records;

Security Requirement	Type	Method of Assessment
		Test: ST&E test results that demonstrate the automated mechanisms implementing information flow enforcement policy.
SR-49: The JUS HDS Services Infrastructure must use internal system clocks that are synchronized with an authoritative time source, approved by Justice Canada, to generate time stamps for audit records.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing time stamp generation; JUS HDS Services system audit records; **Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; **Test:** ST&E test results associated with mechanisms implementing time stamp generation.
SR-50: The JUS HDS Services must: a) protect audit information from unauthorized access, modification, and deletion; b) use tamper resistant cryptographic mechanisms to protect the integrity of audit information, and c) backup audit records onto a different system or media than the system being audited on a schedule specified by Justice Canada.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures; information system design documentation; information system configuration settings and associated documentation, information system audit records; audit tools; other relevant documents or records. **Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation, system or media storing backups of JUS HDS Services system audit records; JUS HDS Services system audit records; JUS HDS Services system hardware settings.

Security Requirement	Type	Method of Assessment
		Interview: Contractor personnel with auditing and accountability responsibilities. **Test:** ST&E test results associated with JUS HDS Services mechanisms implementing audit information protection.
SR-51: The JUS HDS Services Infrastructure must capture events and audit logs to a centralized repository. The JUS HDS Services Infrastructure must perform automated real-time analysis and management of the centralized event audit and data logs to consolidate, protect, and retain logs and events, and to enable monitoring, analysis, and investigation of log events including at minimum: a) consolidating; b) correlating; c) aggregating; d) archiving; e) viewing; f) searching; g) filtering; h) sorting: i) exporting, and j) generating reports. The Contractor must provide view, search and reporting access to the JUS HDS Services Infrastructure auditing and logging central repository using the Service Delivery Portal, and under specific circumstances to be mutually agreed upon by Justice Canada and the Contractor.	**Basic**	**Examine:** Operational Artefacts - System and information integrity policy; procedures addressing JUS HDS Services system monitoring tools and techniques; JUS HDS Services system design documentation; JUS HDS Services system monitoring tools and techniques documentation; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system protocols documentation. **Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing protection of audit information; access control policy and procedures. **Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation, JUS HDS Services system audit records; audit tools. **Interview:** Contractor personnel with auditing and accountability responsibilities. **Test:** JUS HDS Services ST&E result supporting near real-time event analysis, mechanisms implementing audit information protection, mechanisms implementing non-repudiation capability, and media storage devices to hold audit records.

Security Requirement	Type	Method of Assessment
SR-52: From the date vulnerabilities are formally identified, the Contractor must, at a minimum: a) Mitigate all high-risk vulnerabilities within ten calendar days; and b) Mitigate all moderate risk vulnerabilities within 30 calendar days. Justice Canada and Contractor will mutually agree and determine the risk rating of vulnerabilities. **SR-53**: Please refer to SOW General, subsection Ongoing Security Assessment and Monitoring **SR-54**: Please refer to SOW General, subsection Ongoing Security Assessment and Monitoring	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system risk assessment policy; procedures addressing vulnerability scanning; risk assessment; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records. **Interview:** Contractor personnel with risk assessment and vulnerability scanning responsibilities. **Examine:** Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; **Interview:** Contractor personnel with risk assessment and vulnerability scanning responsibilities.
SR-56: Please refer to SOW General, subsection Ongoing Security Assessment and Monitoring	**Basic**	**Examine:** Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; **Interview:** Contractor personnel with risk assessment and vulnerability scanning responsibilities.
SR-57: The Contractor must include in the Operational Security Procedures, configuration management requirements specified in this SOW.	**Basic**	**Examine:** Development/Installation/Integration/Operational Artefacts - Configuration management policy and procedures; other relevant documents or

Security Requirement	Type	Method of Assessment
SR-58: Please refer to SOW General, subsection Change Management		records; **Interview:** Contractor personnel with configuration management and control responsibilities. **Examine:** secure SDLC phases - Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the JUS HDS Services system; JUS HDS Services system design documentation; JUS HDS Services system architecture and configuration documentation; other relevant documents or records; **Interview:** Contractor personnel with configuration change control responsibilities; **Test:** ST&E test result related to demonstrate mechanisms implementing baseline configuration maintenance.
SR-59: The Contractor must develop, document, and maintain under configuration control, a current baseline configuration of the JUS HDS Services Infrastructure Components	**Basic**	**Examine:** secure SDLC phases - Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the JUS HDS Services system; JUS HDS Services system design documentation; JUS HDS Services system architecture and configuration documentation; other relevant documents or records; **Interview:** Contractor personnel with configuration change control responsibilities; **Test:** ST&E test result related to demonstrate mechanisms implementing baseline configuration maintenance.

Security Requirement	Type	Method of Assessment
SR-61: Please refer to SOW General, subsection Configuration Management, Asset Management and Software License Management. **SR-63**: The Contractor must create an Emergency Change Request, within a time period specified by Justice Canada, for each mitigation measure requested by Justice Canada to contain a Security Incident. The Contractor must create an Emergency Change Request, based on severity as specified by Justice Canada, for each mitigation measure requested by Justice Canada to contain a Security Incident and must implement the Emergency Change Request in accordance with Justice Canada's priority level.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services configuration management policy; configuration management plan; procedures addressing JUS HDS Services system configuration change control; JUS HDS Services system architecture and configuration documentation; security plan; change control records; JUS HDS Services system audit records; other relevant documents or records. **Interview:** Contractor personnel with configuration change control responsibilities. **Examine:** secure SDLC phases - Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the JUS HDS Services system; JUS HDS Services system design documentation; JUS HDS Services system architecture and configuration documentation; other relevant documents or records; **Interview:** Contractor personnel with configuration change control responsibilities; **Test:** ST&E test result related to demonstrate mechanisms implementing baseline configuration maintenance. **Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident

Security Requirement	Type	Method of Assessment
		reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.
SR-64: Please refer to SOW General, subsection Release Management.	**Basic**	**Examine:** secure SDLC - Configuration management policy; configuration management plan; procedures addressing security impact analysis for changes to the JUS HDS Services system; security impact analysis documentation; JUS HDS Services system design documentation; JUS HDS Services system architecture and configuration documentation; change control records; JUS HDS Services system audit records; JUS HDS Services system test and operational environments; other relevant documents or records; **Interview:** Contractor personnel with responsibilities for determining security impacts prior to implementation of information system changes.
SR-65: The Contractor must assess the security impact of changes by: a) analyzing new software before installation in an operational environment, looking for security impacts due to flaws, weaknesses, incompatibility, or	**Basic**	**Examine:** secure SDLC phases - Configuration management policy; configuration management plan; procedures addressing the baseline configuration of the JUS HDS Services system; JUS HDS Services system design

Security Requirement	Type	Method of Assessment
intentional malice; b) informing Justice Canada of potential security impacts prior to change implementation, and c) checking the security functions, after changes are implemented, to verify that the functions are implemented correctly, operating as intended, and producing the desired outcome with regard to meeting the applicable security requirements. The Contractor must conduct audits of information system changes at least every 12 months and when indications so warrant determining whether unauthorized changes have occurred.		documentation; JUS HDS Services system architecture and configuration documentation; other relevant documents or records; **Interview:** Contractor personnel with configuration change control responsibilities.
SR-67: Please refer to SOW General, subsection Configuration Management, Asset Management and Software License Management.	**Enhanced**	**Examine:** secure SDLC - Configuration management policy; configuration management plan; procedures addressing least functionality in the JUS HDS Services system; security plan; JUS HDS Services system configuration settings and associated documentation; security configuration checklists; other relevant documents or records; **Interview:** Contractor personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the JUS HDS Services system; **Test:** ST&E test results associated with the demonstration of JUS HDS Services system disabling or restricting functions, ports, protocols, and services as well as mechanisms preventing software program execution on the JUS HDS Services system.
SR-69: The Contractor must employ an automated mechanisms to centrally manage, apply and verify configuration settings, and to respond to unauthorized configuration changes by creating a Security Incident.	**Enhanced**	**Examine:** secure SDLC - Configuration management policy; configuration management plan; procedures addressing least functionality in the JUS HDS Services system; security plan; JUS HDS Services system configuration settings and associated documentation; security

Security Requirement	Type	Method of Assessment
		configuration checklists; other relevant documents or records; **Interview:** Contractor personnel with responsibilities for identifying and eliminating unnecessary functions, ports, protocols, and services on the JUS HDS Services system; **Test:** ST&E test results associated with the demonstration of JUS HDS Services system disabling or restricting functions, ports, protocols, and services as well as mechanisms preventing software program execution on the JUS HDS Services system.
SR-70: The Contractor must open an Incident Ticket for a Security Incident when an unauthorized configuration change is detected.	**Basic**	**Examine:** secure SDLC - Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other relevant documents or records; **Interview:** Contractor personnel with information system installation and inventory responsibilities; **Test:** ST&E test results demonstrating the automated mechanisms implementing JUS HDS Services system component inventory management
SR-71: Please refer to SOW General, subsection Configuration Management, Asset Management and Software License Management.	**Basic**	**Examine:** secure SDLC - Configuration management policy; configuration management plan; procedures addressing information system component inventory; information system design documentation; information system inventory records; component installation records; other

Security Requirement	Type	Method of Assessment
		relevant documents or records; **Interview:** Contractor personnel with information system installation and inventory responsibilities; **Test:** ST&E test results demonstrating the automated mechanisms implementing JUS HDS Services system component inventory management
SR-72: The Contractor must employ mechanisms to maintain an up-to-date, complete, accurate and readily available inventory of JUS HDS Services Infrastructure components that: a) detect the addition of unauthorized components/devices into the JUS HDS Services Infrastructure, and b) create a Security Incident and disable network access by such components.	**Basic**	**Examine:** secure SDLC - Configuration management policy; configuration management plan; procedures addressing JUS HDS Services system component inventory; security plan; JUS HDS Services system design documentation; JUS HDS Services system inventory records; component installation records; change control records; other relevant documents or records; **Interview:** Contractor personnel with information system installation and inventory responsibilities; **Test:** ST&E test results that demonstrate the automated mechanisms for detecting unauthorized components/devices on the JUS HDS Services system as well as automated mechanisms implementing JUS HDS Services system component inventory management.
SR-73: Please refer to SOW General, subsection Configuration Management Plan.	**Basic**	**Examine:** secure SDLC artefacts - Access control policy; procedures addressing JUS HDS Services information flow enforcement; procedures addressing source and destination domain identification and authentication, and information transfer error handling; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and

Security Requirement	Type	Method of Assessment
		associated documentation; JUS HDS Services system audit records; other relevant documents or records; **Test:** ST&E test results that demonstrate the automated mechanisms implementing information flow enforcement policy.
SR-74: Please refer to SOW General, subsection Service Continuity Plan.	**Basic**	**Examine:** Contingency planning policy; procedures addressing contingency operations for the JUS HDS Services system; contingency plan; security plan; business impact assessment; other relevant documents or records; **Interview:** Contractor personnel with contingency planning and plan implementation responsibilities; Contractor personnel with incident handling responsibilities.
SR-75: The Contractor must provide under Operational Security Procedures, identification and authentication requirements specified in this SOW .	**Basic**	**Examine:** Development/Installation/Operational Artefacts - Identification and authentication policy and procedures; other relevant documents or records. **Interview:** Contractor personnel with identification and authentication responsibilities.
SR-76: The JUS HDS Services Infrastructure must uniquely identify and authenticate Operators (or processes acting on behalf of Operators). The Contractor must provide distinct JUS HDS Services Infrastructure Operator Accounts to each Operator.	**Basic**	**Examine:** Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing operator identification and authentication; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system accounts; other relevant documents or

Security Requirement	Type	Method of Assessment
SR-77: The Service Delivery Portal I&A Service must issue user id and password credentials for Service Delivery Portal Accounts that comply with the requirements for Level 2 Assurance as described in ITSG-31. **SR-78**: The Service Delivery Portal I&A Service must allow: a) challenge/response questions for password recovery; b) one-time temporary passwords for enrolment and password recovery; c) one-time temporary passwords that must be subject to a configurable validity period, as specified by Justice Canada; d) one-time temporary passwords that must be sufficiently random so as to not be predictable as approved by Justice Canada; e) automatic advanced notification of pending password expiry as specified by Justice Canada; and f) password recovery policies and processes.		records. **Test:** ST&E test results to demonstrate the automated mechanisms implementing identification and authentication capability for the JUS HDS Services system.
SR-79: The JUS HDS Services Infrastructure must enforce two-factor Authentication using hard crypto token for all Operator Accounts in compliance with CSEC ITSG-31.	**Basic**	**Examine:** Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing operator identification and authentication; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; list of privileged JUS HDS Services system accounts; other relevant documents or records. **Test:** ST&E test results to demonstrate automated mechanisms implementing identification and authentication capability for the information system.

Security Requirement	Type	Method of Assessment
SR-80: The JUS HDS Services Infrastructure must perform mutual Authentication of Portable Devices connected to the network and only accept authorized Portable Devices.	**Basic**	**Examine:** Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing user identification and authentication; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; list of non-privileged JUS HDS Services system accounts; other relevant documents or records. **Test:** ST&E test results to demonstrate automated mechanisms implementing identification and authentication capability for the JUS HDS Services system.
SR-82: The JUS HDS Services must log the following Operator Account events: a) account creation; b) account modifications c) account disabling d) account termination, and e) account deletion. The JUS HDS Services Infrastructure must record in the audit logs, at a minimum, and at all JUS HDS Services Infrastructure components where feasible.	**Basic**	**Examine:** secure SDLC artefacts -JUS HDS Services access control policy; procedures addressing account management; security plan; list of active system accounts along with the name of the individual associated with each account; list of guest, anonymous and temporary accounts along with the name of the individual associated with each account and the date the account expires; lists of recently transferred, separated, or terminated employees; list of recently disabled JUS HDS Services system accounts along with the name of the individual associated with each account; system-generated records with user IDs and last login date; other relevant documents or records. **Interview:** Contractor personnel with account management responsibilities. **Examine:** Development/Design Artefacts - Detail Level Design, Configuration/Build Books; **Examine:** Operational Artefacts - Account

Security Requirement	Type	Method of Assessment
		management procedures, audit/compliance reports; **Examine:** Security Test and Evaluation results
SR-83: The Contractor must manage user authenticators for Operators by: a) verifying, as part of the initial authenticator distribution, the identity of the individual receiving the authenticator; b) establishing initial authenticator content for authenticators defined by the Contractor; c) ensuring that authenticators have sufficient strength of mechanism for their intended use; d) establishing and implementing administrative procedures for initial authenticator distribution, lost, compromised or damaged authenticators, and revoking authenticators; e) changing default content of authenticators upon JUS HDS Services Infrastructure Component installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) changing or refreshing authenticators at a frequency not exceeding 180 calendar days; h) protecting authenticator content from unauthorized disclosure and modification, and i) requiring Operators to take specific measures to safeguard authenticators. **SR-84**: The Contractor must manage Device authenticators by: a) verifying, as part of the initial authenticator distribution, the identity of the Device receiving the authenticator; b) establishing initial authenticator content for authenticators defined by the Contractor; c) ensuring that authenticators have sufficient strength of mechanism for their intended use;	**Basic**	**Examine:** Development/Installation/Operational Artefacts - Identification and authentication policy; procedures addressing authenticator management; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; list of JUS HDS Services system accounts; other relevant documents or records. **Interview:** Contractor personnel with responsibilities for determining initial authenticator content. **Test:** ST&E test results to demonstrate automated mechanisms implementing authenticator management functions.

Security Requirement	Type	Method of Assessment
d) establishing and implementing administrative procedures for initial authenticator distribution, lost, compromised or damaged authenticators, and revoking authenticators; e) changing default content of authenticators upon JUS HDS Services Infrastructure component installation; f) establishing minimum and maximum lifetime restrictions and reuse conditions for authenticators; g) changing and refreshing authenticators at a frequency not exceeding 180 calendar days; h) protecting authenticator content from unauthorized disclosure and modification, and i) having Devices implement specific measures to safeguard authenticators. **SR-181**: The JUS HDS Services Infrastructure must, for password-based Authentication: a) enforce minimum password complexity of case sensitive, 15 characters, with at least one upper case, one lower case, one number, and one special character; b) encrypt passwords in storage and in transmission; c) enforce password maximum lifetime of 90 calendar days, and d) prohibit password reuse for 10 generations. **SR-182**: The Contractor must require that the registration process for Operators to receive identifiers and authenticators be carried out in person before a designated registration authority with authorization by a designated Contractor official (e.g., a supervisor). **SR-183**: The JUS HDS Services Infrastructure must not transmit clear text passwords over any network. **SR-184**:		

Security Requirement	Type	Method of Assessment
The Contractor must not allow unencrypted static authenticators to be embedded in JUS HDS Services Infrastructure applications or access scripts or stored on function keys. **SR-185**: The I&A Service for the JUS HDS Services system must enforce approved authorizations for logical access to the system in accordance with applicable Canada policy. **SR-186**: The I&A Service must not allow an Account to access HDS system if the Account is suspended.		
SR-85: The JUS HDS Services must obscure feedback of the Account Authentication data (e.g., masking password field) during the Authentication process.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system access and authentication control policy; procedures addressing obscure feedback of the Account Authentication data (e.g., masking password field) during the Authentication process; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; other relevant documents or records. **Test:** ST&E test results demonstrating automated mechanisms implementing the obscure feedback of the Account Authentication data (e.g., masking password field) during the Authentication process.
SR-86: The Contractor must establish a process for maintenance personnel authorization that includes:	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system maintenance policy; procedures addressing controlled maintenance for these JUS HDS Services system;

Security Requirement	Type	Method of Assessment
a) maintaining a current list of authorized maintenance organizations or personnel; b) ensuring that personnel performing maintenance on the HDS Service have required access authorizations, and c) having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.		maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records. **Interview:** Contractor personnel with JUS HDS Services system maintenance responsibilities.
SR-87: The Contractor'sOperational Security Procedures must include Incident response requirements specified in this SOW. **SR-88**: Please refer to SOW General, subsection Service Continuity Plan. Please refer to SOW General, subsection Implementation of Service Continuity Plan. **SR-90**: The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by Justice Canada, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by Justice Canada; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies Justice Canada of the degree of non-compliance. In addition to any sources of intelligence on cyber threats and Incidents sources that the Contractor monitors in its routine operations, the Contractor must monitor cyber threats and incidents publications, from sources identified by Canada (e.g. the Canadian Cyber Incident Response Centre (CCIRC)	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events. **Examine:** Operational Artefacts - Contingency planning policy; contingency plan; procedures addressing contingency plan testing and exercises; automated mechanisms supporting contingency plan testing and exercises; contingency plan testing and exercise documentation; other relevant documents or records;

Security Requirement	Type	Method of Assessment
(http://www.publicsafety.gc.ca). **SR-91**: The Contractor must automatically provide Security Incident ticket information by email to a pre-defined distribution list for each JUS HDS Services for Incidents where Justice Canada specifies: a) information from Incident Ticket; b) frequency of email updates; c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket). The Contractor must continue to automatically send email upon updates of Security Incidents until the Incident is closed or Justice Canada cancels the automatic update reporting for the Incident. The Incident Tickets for Security Incidents must include, the following additional information: a) type and description of the attack or event; b) whether attack or event appears to have been successful, and its impact; c) attack or event scope (to an organization or across many organizations); d) estimated number of systems affected by organization(s); e) list of systems affected by organization(s); f) apparent source or origin of the attack/Incident/event; g) date and time of the attack/Incident/event; h) estimated injury level and sector; i) estimated impact level; j) attack/Incident/event duration; k) actions taken; l) status of mitigations, and m) applicable logs or evidence data. The Contractor must implement mitigation measures (e.g., firewall blocks, customized Intrusion Detection Prevention signatures, removing malicious emails)		**Interview:** Contractor personnel with responsibilities for reviewing or responding to contingency plan tests and exercises, contingency planning, plan implementation, JUS HDS Services system recovery and reconstitution responsibilities, and testing responsibilities. **Examine:** Contingency planning policy; procedures addressing contingency operations for the JUS HDS Services system; contingency plan; security plan; business impact assessment; other relevant documents or records; **Interview:** Contractor personnel with contingency planning and plan implementation responsibilities; Contractor personnel with incident handling responsibilities.

Security Requirement	Type	Method of Assessment
to contain a Security Incident, protect against cyber threats or address vulnerabilities, when requested by Justice Canada authorized representatives, as specified by Justice Canada in accordance with Canada's priority level. The Contractor must provide a Security Incident post-mortem report to Justice Canada, within 72 hours of a request by Justice Canada, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with JUS HDS Services, and j) recommendations to improve JUS HDS Services. The JUS HDS Services Infrastructure must record in the audit logs, at a minimum, and at all JUS HDS Services Infrastructure Components where feasible The Contractor must monitor on a continuous basis events on the JUS HDS Services Infrastructure to: a) detect attacks, Incidents and abnormal events against the JUS HDS Services and the Infrastructure; b) identify unauthorized use and access of JUS HDS Services Data and JUS HDS Services Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the JUS HDS Services.		
SR-92: The Contractor must provide training for JUS HDS Services Infrastructure Operators in their security Incident response roles and responsibilities and	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system

Security Requirement	Type	Method of Assessment
provide annual refresher training.		configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.
SR-93: The Contractor must test the Incident response process for the JUS HDS Services at least annually using comprehensive test scripts to determine the Incident response effectiveness including: a) documenting the test results; b) reviewing the test results with Justice Canada, and c) implement corrective actions as required by Canada within a timeframe agreed to with Justice Canada. The Contractor must review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing and exercises.	**Enhanced**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.

Security Requirement	Type	Method of Assessment
SR-94: The Contractor must review lessons learned from ongoing Incident handling activities and implement resulting corrective measures to Incident response procedures, training, and testing/exercises. **SR-96**: The Contractor must physically separate information that identifies and details Security Incidents from all other types of Incidents. Any security related investigation information generated as a part of the ticket must be recorded in Justice Canada dedicated storage. **SR-97**: The Contractor must open an Incident Ticket within 5 minutes of notification for both Contractor-determined and Justice Canada-reported Incidents.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.
SR-98: The Incident Tickets for Security Incidents must include the following additional information: a) type and description of attack/event; b) whether attack appears to have been successful and impact; c) attack scope (to an organization and/or across many organizations); d) estimated number of systems affected by organization; e) list of systems affected by organization; f) apparent source/origin of attack/Incident/event; g) date/time of attack/Incident/event; h) estimated injury level /sector; i) estimated impact level; j) attack/Incident/event duration; k) actions taken; l) status of mitigations, and	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms

Security Requirement	Type	Method of Assessment
m) applicable logs or evidence data.		implementing information system auditing of JUS HDS Services-defined auditable events.
SR-99: The Contractor must report all suspected or actual privacy and security violations for JUS HDS Services as Security Incidents. The Contractor must provide a Security Incident post-mortem report to Justice Canada, within 72 hours of a request by Justice Canada, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with JUS HDS Services, and j) recommendations to improve JUS HDS Services. **SR-100**: The Contractor must report all suspected or actual privacy and security violations for JUS HDS Services as Security Incidents. **SR-101**: The Contractor must automatically provide Incident Ticket information by email to a pre-defined distribution list for each JUS HDS Services for Incidents where Justice Canada specifies: a) information from Incident Ticket; b) frequency of email updates;	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.

Security Requirement	Type	Method of Assessment
c) distribution lists, and d) criteria for selecting Incidents (severity, priority, content of Incident Ticket). The Contractor must provide all evidence, in a COTS format specified by Justice Canada, associated to a Security Incident, within a time interval specified by Justice Canada that includes: a) results of historical logs and audit records research associated with one or many Clients based on criteria provided by Justice Canada; b) results of analysis of logs and audit records associated with one or many organizations based on criteria provided by Justice Canada; c) logs and audit records based on criteria provided by Justice Canada, and d) additional information or data as specified by Justice Canada. **SR-102**: Please refer to SOW General, subsection Incident Management. **SR-103**: The Contractor must notify Justice Canada via phone and email (7 days x 24 hours x 365 days), based on priority as specified by Justice Canada, of any suspected or actual Security Incidents, including: a) denial of service attacks; b) malware; c) social engineering; d) unauthorized intrusion or access; e) information breach; and f) all other security breaches or cyber threats targeting Canada. **SR-104**: The Contractor must not withhold from Justice Canada any information or data in its possession that relates to JUS HDS Services or is associated with a Security Incident.		

Security Requirement	Type	Method of Assessment
SR-105: The Contractor must provide a Security Incident post-mortem report to Justice Canada, within 72 hours of a request by Justice Canada, that includes, but is not limited to: a) Security Incident number; b) Security Incident opened date; c) Security Incident closed date; d) description of Security Incident; e) scope of Security Incident; f) chain of events / timeline; g) actions taken by Contractor; h) lessons learned; i) limitations/issues with JUS HDS Services, and j) recommendations to improve JUS HDS Services.		
SR-106: The Contractor must provide the service of a Security Operations and Response Specialist who will be Justice Canada's point of contact for: a) Security Incidents; b) security issues; c) requests for information on security; d) coordination of security response, and e) security alerts. **SR-107**: The Security Operations and Response Specialist must have the following minimum qualifications: a) have relevant experience in security operations and response; b) have in-depth knowledge of the JUS HDS Services ; c) be capable of rapidly analyzing and assessing Incident data; d) be capable of providing a factual assessment of the situation; e) be fully trained on the JUS HDS Services security monitoring and reporting solution; f) be capable of rapidly responding to inquiries;	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.

Security Requirement	Type	Method of Assessment
g) be client oriented; h) be capable of working under high stress and pressure, and i) be bilingual. **SR-108**: The Contractor must have proper forensic procedures and safeguards in place that includes: a) the maintenance of a chain of custody for both the audit information, and b) the collection, retention, and presentation of evidence that demonstrate the integrity of the evidence.		
SR-109: The Contractor must develop an incident response plan that includes: a) how the Contractor plans to identify, report, and escalate Security Incidents; b) a roadmap for implementing the Security Incident response capability that includes preparation, detection, analysis, containment and recovery; c) a description of the structure and organization of the Security Incident response capability; d) a high-level approach for how the Security Incident response capability fits into the Contractor's overall organization; e) a definition of reportable Security Incidents; f) a definition of metrics for measuring the Security Incident response capability; and g) a definition of resources and management support needed to effectively maintain and mature the Security Incident response capability.	**Basic**	**Examine:** Operational Artefacts - Audit and accountability policy; procedures addressing auditable events; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; list of JUS HDS Services system auditable events; auditable events review and update records; JUS HDS Services system audit records; JUS HDS Services system incident reports; **Examine:** Development/Installation Artefacts - list of JUS HDS Services-defined auditable events; **Interview:** Contractor personnel with auditing and accountability responsibilities; **Test:** JUS HDS Services mechanisms implementing information system auditing of JUS HDS Services-defined auditable events.
SR-111: The Contractor must include in the Operational Security Procedures, maintenance requirements specified in this SOW.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system maintenance policy and procedures; other relevant documents or records. **Interview:** Contractor personnel with

Security Requirement	Type	Method of Assessment
		information system maintenance responsibilities.
SR-112: The Contractor must perform controlled maintenance by: a) scheduling, performing, documenting, and reviewing records of maintenance and repairs on JUS HDS Services Infrastructure Components in accordance with manufacturer or vendor specifications; b) controlling all maintenance activities, whether performed on site or remotely, and whether the equipment is serviced on site or removed to another location; c) requiring that a designated Contractor's official explicitly approve the removal of the JUS HDS Services Infrastructure Components from the Contractor data centre for off-site maintenance or repairs; d) sanitizing equipment to remove all data from associated media prior to removal from Contractor's facilities for off-site maintenance or repairs, and e) checking all potentially impacted security requirements to verify that the controls are still functioning properly following maintenance or repair actions.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system maintenance policy; procedures addressing controlled maintenance for the JUS HDS Services system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records. **Interview:** Contractor personnel with JUS HDS Services system maintenance responsibilities.
SR-113: Please refer to SOW General, subsection Change Management.	**Enhanced**	**Examine:** secure SDLC artefacts - JUS HDS Services system maintenance policy; procedures addressing controlled maintenance for the JUS HDS Services system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records. **Interview:** Contractor personnel with JUS HDS Services system maintenance responsibilities.
SR-114: The Contractor must approve, control, monitor and maintain, on an ongoing basis,	**Enhanced**	**Examine:** secure SDLC Artefacts - JUS HDS Services system maintenance policy; JUS HDS Services system maintenance tools and

Security Requirement	Type	Method of Assessment
the hardware and software used for maintaining the JUS HDS Services Infrastructure specifically for diagnostic and repair actions (e.g., a hardware or software tools that are introduced for the purpose of a particular maintenance activity).		associated documentation; procedures addressing JUS HDS Services system maintenance tools; maintenance records; other relevant documents or records. **Interview:** Contractor personnel with JUS HDS Services system maintenance responsibilities.
SR-115: The Contractor must check all media containing diagnostic and test programs for malicious code before the media are used on JUS HDS Services Infrastructure components. The Contractor must approve, control, monitor and maintain, on an ongoing basis, the hardware and software used for maintaining the JUS HDS Services Infrastructure specifically for diagnostic and repair actions (e.g., a hardware or software tools that are introduced for the purpose of a particular maintenance activity).	**Enhanced**	**Examine:** secure SDLC Artefacts - JUS HDS Services system maintenance policy; JUS HDS Services system maintenance tools and associated documentation; procedures addressing JUS HDS Services system maintenance tools; maintenance records; other relevant documents or records. **Interview:** Contractor personnel with JUS HDS Services system maintenance responsibilities.
SR-116: The Contractor must include in its Security Management Plan how it will install and use non-local maintenance and diagnostic connections. The JUS HDS Services must restrict Software Client access from network addresses specified by Justice Canada. The Contractor must authorize, monitor, and control maintenance and diagnostic activities on the JUS HDS Services Infrastructure by: a) allowing the use of maintenance and diagnostic tools approved by Justice Canada; b) employing strong identification and Authentication techniques in the establishment of maintenance and diagnostic sessions that are tightly bound to the End User and by separating the maintenance session from other network sessions with the JUS HDS Services Infrastructure by either: i) physically separated communications paths, or ii) logically separated communications paths using Communications Security Establishment Canada -approved cryptographic modules and algorithms (see subsection Encryption Standards); c) recording maintenance and diagnostic sessions, and d) having designated personnel review the records of the maintenance and	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system access management policies and procedures; design documentation; procedures for restricting Software Client access from network addresses ; **Test:** ST&E test results demonstrating compliance with SR requirements. **Examine:** secure SDLC artefacts - JUS HDS Services system maintenance policy; information system maintenance tools and associated documentation; procedures addressing JUS HDS Services system maintenance tools; JUS HDS Services system media containing maintenance programs (including diagnostic and test programs); maintenance records; equipment sanitization records; media sanitization records; exemptions for equipment removal; other relevant

Security Requirement	Type	Method of Assessment
diagnostic sessions. The Contractor must include in Security Management Plan how the Contractor will install and use non-local maintenance and diagnostic connections.		documents or records. **Interview:** Contractor personnel with JUS HDS Services system maintenance responsibilities. **Test:** ST&E test results demonstrating automated mechanisms supporting JUS HDS Services system maintenance activities.
SR-118: The Contractor must establish a process for maintenance personnel authorization that includes: a) maintaining a current list of authorized maintenance organizations or personnel; b) ensuring that personnel performing maintenance on the JUS HDS Services have required access authorizations, and c) having designated personnel with required access authorizations supervising the maintenance activities when maintenance personnel do not possess the required access authorizations.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system maintenance policy; procedures addressing controlled maintenance for the JUS HDS Services system; maintenance records; manufacturer/vendor maintenance specifications; equipment sanitization records; media sanitization records; other relevant documents or records. **Interview:** Contractor personnel with JUS HDS Services system maintenance responsibilities.
SR-119: The Contractor must include in Operational Security Procedures, media protection requirements specified in this SOW.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services media protection policy and procedures; other relevant documents or records. **Interview:** Contractor personnel with JUS HDS Services system media protection responsibilities.
SR-120: The Contractor must restrict access to IT media (digital and non-digital) containing JUS HDS Services Data to authorized Operators. **SR-121**: The Contractor must encrypt JUS HDS Services Data on Portable Digital Media in compliance with approved cryptographic standards (see subsection Encryption Standards).	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services media protection policy and procedures; other relevant documents or records. **Interview:** Contractor personnel with JUS HDS Services system media protection responsibilities.

Security Requirement	Type	Method of Assessment
SR-122: The Contractor must mark, in accordance with the provisions of the Contract, removable IT media containing Canada information indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system media protection policy; procedures addressing media labeling; physical and environmental protection policy and procedures; security plan; removable storage media and JUS HDS Services system output; other relevant documents or records]. **Interview:** Contractor personnel with JUS HDS Services system media protection and marking responsibilities.
SR-123: The Contractor must: a) physically control and securely store IT media containing JUS HDS Services Data in accordance with the RCMP G1-001, Security Equipment Guide; b) physically control and securely store IT media containing JUS HDS Services Data awaiting destruction (either on- or off-site) using Justice Canada approved equipment, techniques, and procedures.	**Enhanced**	**Examine:** secure SDLC artefacts - JUS HDS Services system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; JUS HDS Services system media; other relevant documents or records. **Interview:** Contractor personnel with information system media protection and storage responsibilities.
SR-124: The Contractor must: a) physically control and securely store IT media containing JUS HDS Services Data in accordance with the RCMP G1-001, Security Equipment Guide; b) physically control and securely store IT media containing JUS HDS Services Data awaiting destruction (either on- or off-site) using approved equipment, techniques, and procedures; c) protect and control IT media containing JUS HDS Services Data during transport outside of controlled areas in accordance with the TBS Operational Security Standard on Physical Security and the RCMP G1-009,	**Enhanced**	**Examine:** secure SDLC artefacts - JUS HDS Services system media protection policy; procedures addressing media storage; physical and environmental protection policy and procedures; access control policy and procedures; security plan; JUS HDS Services system media; other relevant documents or records. **Interview:** Contractor personnel with information system media protection and storage responsibilities.

Security Requirement	Type	Method of Assessment
Transport and Transmittal of Protected and Classified Information; d) maintain accountability for IT media containing JUS HDS Services Data during transport outside of controlled areas; and e) restrict and document the activities associated with transport of IT media containing JUS HDS Services Data to authorized personnel.		
SR-125: The Contractor must sanitize IT media containing JUS HDS Services Data, both digital and non-digital, prior to disposal, release out of the Provider's control, or release for reuse.	**Basic**	**Examine:** secure SDLC Artefacts - JUS HDS Services system media protection policy; procedures addressing media sanitization and disposal; media sanitization equipment test records; JUS HDS Services system audit records; other relevant documents or records. **Interview:** Contractor personnel with information system media sanitization responsibilities.
SR-126: The Contractor must hold or obtain from PWGSC CISD a Facility Security Clearance (FSC) with Document Safeguarding Capability, it applicable, for the HDS Service Facility at a level specified in the Security Requirements Checklist (SRCL). The Contractor must allow Canada to perform a site inspection within 3 FGWDs of a request by Justice Canada.	**Basic**	**Examine:** Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; JUS HDS Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. **Interview:** Contractor personnel with physical access control responsibilities. **Test:** Physical access control capability; physical access control devices.
SR-127: The Contractor must monitor physical access to the JUS HDS Services Facility by:	**Basic**	**Examine:** Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials;

Security Requirement	Type	Method of Assessment
a) monitoring in real-time physical intrusion alarms and surveillance equipment; b) recording all physical access events; c) reviewing physical access logs at least monthly; d) providing physical access logs on a monthly basis and as requested by Justice Canada; and e) create a Security Incident upon discovery of abnormal activity.		list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; JUS HDS Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. **Interview:** Contractor personnel with physical access control responsibilities. **Test:** Physical access control capability; physical access control devices.
SR-128: The Contractor must review visitor access records for the JUS HDS Services Facility at least every 90 calendar days.	**Basic**	**Examine:** Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; JUS HDS Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. **Interview:** Contractor personnel with physical access control responsibilities. **Test:** Physical access control capability; physical access control devices.
SR-129: The Contractor must implement protection devices to prevent the accidental activation of emergency power shutoff mechanisms of JUS HDS Services Infrastructure.	**Basic**	**Examine:** Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; JUS HDS Services system entry and exit points; storage locations for physical access devices;

Security Requirement	Type	Method of Assessment
		other relevant documents or records. **Interview:** Contractor personnel with physical access control responsibilities. **Test:** Physical access control capability; physical access control devices.
SR-130: The Contractor must authorize, monitor, and control all components entering and exiting the JUS HDS Services Facility and maintain records of those components and activities. Records must be made available monthly and as requested by Justice Canada.	**Basic**	**Examine:** Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; JUS HDS Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. **Interview:** Contractor personnel with physical access control responsibilities. **Test:** Physical access control capability; physical access control devices.
SR-131: The Contractor must implement management, operational, and technical security controls at any alternate work sites that achieve the same objectives as those implemented at the JUS HDS Services Facility. Any alternate work site must be approved by CISD.	**Enhanced**	**Examine:** Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; JUS HDS Services system entry and exit points; storage locations for physical access devices; other relevant documents or records. **Interview:** Contractor personnel with physical access control responsibilities. **Test:** Physical access control capability; physical access control devices.

Security Requirement	Type	Method of Assessment
SR-132: The Contractor must address within the Operational Security Procedures, personnel security requirements specified in this SOW.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system personnel security policy and procedures, other relevant documents or records. **Interview:** Contractor personnel with personnel security responsibilities.
SR-133: The Contractor must, upon termination of an individual's employment associated with JUS HDS Services: a) terminate physical access to JUS HDS Services Facilities for the individual; b) terminate JUS HDS Services Infrastructure access, including remote access, and c) retrieve all security-related property (e.g., employee identity card, physical authentication token).	**Basic**	**Examine:** Personnel security policy; procedures addressing personnel termination; records of personnel termination actions; list of information system accounts; other relevant documents or records. **Interview:** Contractor personnel with personnel security responsibilities.
SR-134: The Contractor must manage JUS HDS Services Infrastructure privileged Operators accounts as follows: a) create Operator Accounts in accordance with role-based access profiles that specify privileges; b) track and monitor Operator role assignments, and c) adjust role assignments as Operator role changes. **SR-135**: The Contractor must implement role-based physical access control to its JUS HDS Services Facility including: a) keeping an access list of personnel with authorized access to the JUS HDS Services Facility; b) issuing authorization credentials for access to the JUS HDS Services Facility; c) reviewing and approving the access list and authorization credentials at all times at least monthly, removing from the access list personnel no longer requiring access; d) authorizing physical access to the facilities, by access point, based on the	**Basic**	**Examine:** Operational Artefacts - Account management procedures, RACI for privileged account, audit/compliance reports; **Examine:** Development/Installation Artefacts - Configuration/build books, Detailed Level Design; **Interview:** Contractor Operational Resources with account management responsibilities. **Examine:** Physical and environmental protection policy; procedures addressing physical access authorizations; authorized personnel access list; authorization credentials; list of areas that are publicly accessible; procedures addressing physical access control; physical access control logs or records; JUS HDS Services system entry and exit points; storage locations for physical access devices;

Security Requirement	Type	Method of Assessment
role of the individual; e) adjust role assignment as Operator role changes to new role; f) implementing separation of duties where the authorization to access facilities is done by a different person than the authorization to access JUS HDS Services Infrastructure; g) allowing access to facilities to authorized personnel based on a need-to-know and need-to-access;, and h) keeping the management of the Contractor's physical access control authorizations to the JUS HDS Services Facility independent of the physical access control authorization to the JUS HDS Services Facility. i) If emergency access is required, contact the RCMP for advice.		other relevant documents or records. **Interview:** Contractor personnel with physical access control responsibilities. **Test:** Physical access control capability; physical access control devices.
SR-136: The Contractor must have access agreements to the JUS HDS Services Infrastructure or JUS HDS Services Data where: a) prior to being granted access to the JUS HDS Services Infrastructure or JUS HDS Services Data, Operators sign an access agreement that list the formal sanctions process for failing to comply with the terms and conditions of the access agreement, b) the Contractor reviews and updates access agreements to the JUS HDS Services Infrastructure or JUS HDS Services Data every two years, and c) the Contractor must provide training for JUS HDS Services Infrastructure Operators in their responsibilities to protect the privacy and confidentiality of the JUS HDS Services Data as per the terms and conditions of the JUS HDS Services Contract and in the sanctions for failure to comply. The Contractor must provide bi-annual refresher training to JUS HDS Services Infrastructure Operators.	**Basic**	**Examine:** Signed access agreement from Contractor training records for protection of privacy and confidentiality of JUS HDS Services data.
SR-138: Please refer to SOW General, subsection Ongoing Security Assessment and Monitoring.	**Basic**	**Examine:** Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; **Interview:** Contractor personnel with risk assessment and vulnerability scanning

Security Requirement	Type	Method of Assessment
		responsibilities.
SR-139: The Contractor must provide network access(es) to the JUS HDS Services Infrastructure to allow for Authenticated and unauthenticated scanning of network components and security appliances, using Justice Canada operated equipment, and Justice Canada specified tools.	**Enhanced**	**Examine:** Development/Installation Artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other relevant documents or records; **Interview:** Contractor personnel with risk assessment and vulnerability scanning responsibilities.
SR-140: Please refer to SOW General, subsection Ongoing Security Assessment and Monitoring.	**Enhanced**	**Examine:** secure SDLC artefacts - JUS HDS Services system risk assessment policy; procedures addressing vulnerability scanning; risk assessment; list of vulnerabilities scanned and JUS HDS Services system components checked; other relevant documents or records.
SR-141: The Contractor must include in the Operational Security Procedures, policy and procedures to facilitate the implementation and maintenance of the system and communications protection requirements specified in this Sow and in applicable GC standards specified in this SOW.	**Basic**	**Examine:** Development/Installation/Operational Artefacts - System and communications protection policy and procedures; other relevant documents or records **Interview:** Contractor personnel with system and communications protection responsibilities.
SR-142: The JUS HDS Services must include a Denial of Service capability that limits concurrent connections per hour as specified by Justice Canada.	**Enhanced**	**Examine:** secure SDLC artefacts -JUS HDS Services system policies and procedures addressing Denial of Service capability; design documentation; configuration settings; **Test:** ST&E test results demonstrating compliance to SR-142 requirements.

Security Requirement	Type	Method of Assessment
SR-143: The Contractor must monitor and analyze network traffic, in real time, to detect attacks and evidence of compromised JUS HDS Services Infrastructure components. The Contractor must detect attacks including but not limited to: a) Denial of Service; b) malware; c) social engineering; d) unauthorized intrusion or access; e) information breach; and f) any other security breaches or cyber threats targeting Canada. **SR-144**: The JUS HDS Services Infrastructure must monitor and control communications at the external boundary of the system and at key internal boundaries within the system in compliance with ITSG-22 and ITSG-38.	**Basic**	**Examine:** Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing security function isolation; list of security functions to be isolated from non-security functions; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Test:** ST&E test results demonstrating the separation of security functions from non-security functions within the JUS HDS Services system; Hardware separation mechanisms facilitating security function isolation; Isolation of security functions enforcing access and information flow control. **Examine:** Operational Artefacts - JUS HDS Services system and communications protection policy; procedures addressing boundary protection; communications and network traffic monitoring logs; other relevant documents or records; **Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; boundary protection hardware and software; JUS HDS Services system architecture and configuration documentation; JUS HDS Services system configuration settings and associated documentation; **Interview:** Contractor/Justice Canada personnel with boundary protection responsibilities; **Test:** ST&E test results associated with interfaces implementing JUS HDS Services

Security Requirement	Type	Method of Assessment
		traffic flow policy.
SR-145: The Contractor must actively manage all network connections to external services associated with the JUS HDS Services Infrastructure as follows: a) deny all network traffic by default; b) define allowable traffic for each network connection (i.e. deny all, permit by exception); c) terminate the network connection associated with a communications session at the end of the session or after a configurable number of minutes of inactivity specified by Justice Canada; d) document each exception to the traffic flow policy with a supporting need and duration of that need; e) review exceptions to the traffic flow policy at least annually; f) remove traffic flow policy exceptions that are no longer supported by an explicit business need; g) monitor traffic for unusual or unauthorized activities or conditions; and h) monitor traffic at selected interior points within the system (e.g., subnets, subsystems) to discover anomalies, as necessary.	**Basic**	**Examine:** Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing boundary protection; JUS HDS Services system design documentation; JUS HDS Services system hardware and software; JUS HDS Services system architecture; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system audit records; other relevant documents or records. **Test:** ST&E test results demonstrate mechanisms implementing managed interfaces within information system boundary protection devices.
SR-146: The Contractor must prevent Contractor-managed Devices (e.g.: notebook or other device used for administration) that are connected with the JUS HDS Services Infrastructure from communicating outside of that communications path (e.g. accessing the Internet via a separate connection available to the Device).	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services system and communications protection policy; procedures addressing boundary protection; JUS HDS Services system design documentation; hardware and software; architecture configuration settings and associated documentation; other relevant documents or records. **Test:** ST&E test results demonstrating automated mechanisms supporting non-remote connections with the JUS HDS Services system; Mechanisms implementing managed interfaces within JUS HDS Services system boundary protection devices.

Security Requirement	Type	Method of Assessment
SR-147: The JUS HDS Services Infrastructure must protect the integrity and confidentiality of JUS HDS Services Data during transmission and at rest using Communications Security Establishment Canada -approved cryptographic modules and algorithms (see subsection Encryption Standards). Unless otherwise protected by alternative physical measures approved by Justice Canada.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system and information integrity policy and procedures; other relevant documents or records; **Interview:** Contractor personnel with system and information integrity responsibilities.
SR-148: The Contractor must ensure that cryptographic solutions (e.g., VPN solutions, TLS, software modules, PKI, and authentication tokens where applicable) in use for JUS HDS Services: a) use cryptographic algorithms and cryptographic key sizes and crypto periods that have been approved by CSEC and validated by the Cryptographic Algorithm Validation Program (http://csrc.nist.gov/groups/STM/cavp/), and are specified in ITSA-11E (https://www.cse-cst.gc.ca/en/publication/itsa-11e) or in a subsequent version; b) be implemented in a Cryptographic Module, validated by the Cryptographic Module Validation Program (https://www.cse-cst.gc.ca/en/group-groupe/crypto-module-validation-program) to at least FIPS 140-2 validation at Level 1, and c) operate in FIPS Mode.	**Basic**	**Examine:** JUS HDS Services System and communications protection policy; procedures addressing use of cryptography; CMVP cryptography standards; JUS HDS Services system design documentation; system configuration settings and associated documentation; cryptographic module validation certificates; other relevant documents or records.
SR-149: The Contractor must only allow pre-approved mobile code in the JUS HDS Services Infrastructure thus denying any other mobile code from being downloaded and executed.	**Basic**	**Examine:** Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing mobile code; mobile code usage restrictions, mobile code implementation policy and procedures; list of acceptable mobile code and mobile code technologies; other relevant documents or records. **Interview:** Contractor personnel with mobile code authorization, monitoring, and control responsibilities. **Test:** ST&E test results to demonstrate mobile

Security Requirement	Type	Method of Assessment
		code authorization and monitoring capability for the organization.
SR-151: The JUS HDS Services Infrastructure component or components that collectively provide name and address resolution service for the JUS HDS Services must implement internal and external role separation.	**Enhanced**	**Examine:** Development/Installation/Operational Artefacts - System and communications protection policy; procedures addressing secure name/address resolution service (authoritative source); access control policy and procedures; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; assessment results from independent, testing organizations; other relevant documents or record. **Test:** ST&E test results that demonstrate automated mechanisms implementing child subspace security status indicators and chain of trust verification for resolution services; Automated mechanisms implementing data origin authentication and integrity verification for resolution services; automated mechanisms supporting name/address resolution service for fault tolerance and role separation.
SR-152: The JUS HDS Services Infrastructure must invalidate session identifiers upon Operator logout or other session termination. **SR-153**: The JUS HDS Services Infrastructure must use a readily observable logout capability whenever authentication is used to gain access to JUS HDS Services Infrastructure components. **SR-154**: The JUS HDS Services Infrastructure must: a) generate a unique session identifier for each session with randomness	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services System and communications protection policy; procedures addressing session authenticity; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records. **Test:** ST&E test results demonstrating automated mechanisms generating and monitoring unique session identifiers for JUS

Security Requirement	Type	Method of Assessment
using CSEC-approved cryptography (see subsection Cryptographic Standards); b) recognize only session identifiers that are generated by the JUS HDS Services Infrastructure; and c) invalidate session identifiers upon Operator logout or other session termination.		HDS Services.
SR-156: The Contractor must include under the Operational Security Procedures system and information integrity requirements specified in this SOW.	**Basic**	**Examine:** Development/Installation Artefacts - JUS HDS Services system and information integrity policy and procedures; other relevant documents or records; **Interview:** Contractor personnel with system and information integrity responsibilities.
SR-157: Please refer to SOW General, subsection Configuration Management Plan. **SR-158**: Please refer to SOW General, subsection Configuration Management Plan.	**Basic**	**Examine:** Development/Installation Artefacts - JUS HDS Services system and information integrity policy; procedures addressing flaw remediation; list of flaws and vulnerabilities potentially affecting the JUS HDS Services system; list of recent security flaw remediation actions performed on the JUS HDS Services system (e.g., list of installed patches, service packs, hot fixes, and other software updates to correct JUS HDS Services system flaws); test results from the installation of software to correct JUS HDS Services system flaws; other relevant documents or records; **Interview:** Contractor personnel with flaw remediation responsibilities. **Examine:** secure SDLC artefacts - Risk assessment policy; procedures addressing vulnerability scanning; risk assessment; security plan; vulnerability scanning results; patch and vulnerability management records; other

Security Requirement	Type	Method of Assessment
		relevant documents or records; **Examine:** Operational Artefacts - patch and vulnerability management records; list of vulnerabilities scanned; records of updates to vulnerabilities scanned; other relevant documents or records; **Interview:** Contractor personnel with risk assessment and vulnerability scanning responsibilities.
SR-159: The Contractor must implement a centrally-managed malware protection solution with the capability to detect and eradicate malicious code: a) at JUS HDS Services Infrastructure entry and exit points; b) at JUS HDS Services Infrastructure components; c) transported by electronic mail, electronic mail attachments, web accesses, removable media, or other common means; and d) inserted through the exploitation of JUS HDS Services Infrastructure vulnerabilities. **SR-160**: The Contractor must configure its malware protection solution to: a) automatically update malicious code protection mechanisms, including signature definitions; b) prevent non-privileged End Users from circumventing malicious code protection capabilities; c) perform periodic scans of the JUS HDS Services Infrastructure at least every 30 calendar days and real-time scans of files from external sources as the files are downloaded, opened, or executed; d) quarantine malicious code in response to malicious code detection; and e) log any malware detection events. **SR-161**: The Contractor must investigate false positive malware detections and assess the resulting impact on the availability of the JUS HDS Services.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services System and information integrity policy; procedures addressing malware protection; malware protection mechanisms; records of malware protection updates; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records. **Interview:** Contractor personnel with malware protection responsibilities. **Test:** ST&E test results demonstrating automated mechanisms implementing malware protection capability.

Security Requirement	Type	Method of Assessment
The JUS HDS Services must perform malware signature definitions updates within 6 hours of availability and as requested by Justice Canada. The Contractor must test the malware protection solution weekly by verifying that both detection capability and associated incident reporting function occur as required.		
SR-162: The Contractor must automatically monitor, on a continuous basis, events on the JUS HDS Services Infrastructure to: a) detect attacks, Incidents and abnormal events against the JUS HDS Services and the Infrastructure; b) identify unauthorized use and access of JUS HDS Services Data and JUS HDS Services Infrastructure components, and. c) respond, contain, and recover from threats and attacks against the JUS HDS Services. The Contractor must heighten the level of monitoring activity whenever there is an indication of increased risk to the JUS HDS Services either from the Contractor or from Canada based on law enforcement information, intelligence information, or other credible sources of information. **SR-163**: The JUS HDS Services Infrastructure must prevent non-privileged Operators from circumventing intrusion detection and prevention capabilities. **SR-164**: The JUS HDS Services Infrastructure security event and log management solution must: a) include centralized and time-synchronized logging of allowed and blocked JUS HDS Services activity with regular log analysis; b) keep 3 months of events and logs online; c) keep events and logs associated with a Security Incident for at least 2 years; d) store logs for at least 1 year; e) categorize events and logs based on Clients; and f) protect data and audit logs from unauthorized access, modification, and	**Basic**	**Examine:** Development/Installation Artefacts - information system design documentation; information system monitoring tools and techniques documentation; JUS HDS Services system configuration settings and associated documentation; JUS HDS Services system protocols documentation; **Examine:** Operational Artefacts- System and information integrity policy; procedures addressing JUS HDS Services system monitoring tools and techniques; other relevant documents or records]. **Interview:** Contractor personnel with JUS HDS Services system monitoring responsibilities. **Test:** ST&E test results demonstrating automated tools supporting near real-time event analysis.

Security Requirement	Type	Method of Assessment
deletion. **SR-165**: The Contractor must test intrusion monitoring tools at least annually by: a) Generating false attacks that mimic well known ones, in order to determine if the intrusion monitoring tools detect the attack and generate false positives; and b) Verifying that both detection of the test case and associated incident reporting occur, as required.		
SR-166: The JUS HDS Services Infrastructure must provide near real-time alerts (e.g. using correlation rules) following indications of compromise or potential compromise. **SR-167**: The Contractor must respond to security alerts, advisories, and directives from designated external organizations, approved by Justice Canada, on an ongoing basis including: a) constantly monitoring security alerts, advisories, and directives; b) generating internal security alerts, advisories, and directives as deemed necessary or as directed by Justice Canada; c) disseminating security alerts, advisories, and directives to Operators with security responsibilities, and d) implementing security directives in accordance with established time frames, or notifies Canada of the degree of non-compliance.	**Basic**	**Examine:** secure SDLC artefacts - JUS HDS Services System and information integrity policy; procedures addressing JUS HDS Services system monitoring tools and techniques; JUS HDS Services system monitoring tools and techniques documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records. **Test:** ST&E test results demonstrating JUS HDS Services system monitoring real-time alert capability as per SR requirements.
SR-168: The Contractor must implement a centrally managed integrity verification solution to detect unauthorized changes to Software and JUS HDS Services Infrastructure component configuration including: a) performing integrity scans at least every 30 calendar days, and b) automatically generating an Incident Ticket for a Security Incident upon discovering discrepancies during integrity verification.	**Enhanced**	**Examine:** Development/Installation Artefacts - System and information integrity policy; procedures addressing software and information integrity; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; integrity verification tools and applications documentation; other relevant documents or records]. **Examine:** Operational Artefacts - System and information integrity policy; procedures

Security Requirement	Type	Method of Assessment
		addressing software and information integrity; security plan; JUS HDS Services system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; JUS HDS Services system configuration settings and associated documentation; integrity verification tools and applications documentation; records of integrity scans; automated tools supporting alerts and notifications for integrity discrepancies; other relevant documents or records. **Test:** ST&E test results will verify and validate software integrity protection and verification capability.
SR-169: The Contractor must implement in End User interfaces: a) assisted data entry where input fields with pre-defined values are populated using lists, drop-down lists, checkboxes and radio buttons in plain language; b) assisted data entry where input fields with embedded meaning (i.e. multiple data elements concatenated within the same input field) are populated using a combination of lists, drop-down lists, checkboxes and radio buttons in plain language for predefined values and textboxes for user provided values; c) error verification where input fields are verified for format and validity, including cross-field validation, with detailed error messages in plain language that indicate to the user what is incorrect and what is the rule(s) that failed, and d) pre-defined fields (e.g. service, Service Delivery Point, work type, contact name, unit pricing, item number, quantities, etc.) approved by Justice Canada, with assisted data entry (where applicable) to minimize error entries.	**Basic**	**Examine:** Development/Installation Artefacts - documentation for automated tools and applications to verify validity of information; JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information validity; access control policy and procedures; separation of duties policy and procedures; other relevant documents or records. **Test:** ST&E test results provide JUS HDS Services system capability for checking validity of information inputs.
SR-170: The JUS HDS Services Infrastructure must log and report security-relevant error	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design

Security Requirement	Type	Method of Assessment
conditions, as specified by Justice Canada, and provide information necessary for corrective actions without revealing Protected B and potentially harmful information in error logs and administrative messages that could be exploited by adversaries.		documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system error handling capability.
SR-171: The Contractor handles and retains in accordance with applicable GC legislation and TBS policies, directives and standards, and operational requirements the following information: a) within the JUS HDS Services system; and b) output from the JUS HDS Services system.	**Basic**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.
SR-172: The Contractor must use stateful packet inspection firewalls for the zone interface points across JUS HDS Services Infrastructure.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.

Security Requirement	Type	Method of Assessment
SR-173: The Contractor must use physical firewalls for the zone interface points across JUS HDS Services Infrastructure.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.
SR-174: The Contractor must use physically and/or virtually partition the virtual devices within the zone interface points as applicable to the JUS HDS Services Infrastructure.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.
SR-175: The Contractor must only use physical dedicated firewall devices for the JUS HDS Services Infrastructure.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS

Security Requirement	Type	Method of Assessment
		Services system compliance with the SR.
SR-176: The Contractor must implement the JUS HDS Services Infrastructure so that the traffic related to the JUS HDS Services Infrastructure devices in the internetwork zone is always kept physically and/or virtually separate from the Contractor internal traffic.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.
SR-177: The Contractor must ensure that any virtual machines used within the JUS HDS Services Infrastructure must not use any machine to machine sharing mechanism (e.g. file sharing) which is implemented within the hypervisor.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.
SR-178: The Contractor must distribute the virtual machines within the JUS HDS Services physical resources in a manner such that the inferences regarding other virtual machines sharing the physical resource(s) are expected to be less than 25% accurate.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures

Security Requirement	Type	Method of Assessment
		addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.
SR-179: The Contractor must distribute the virtual machines within the JUS HDS Services using a pseudo random algorithm.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.
SR-180: The Contractor must ensure that all hypervisors managing the JUS HDS Services virtual machines are zoned as per ITSG-22 and ITSG 38 CSE guidance.	**Enhanced**	**Examine:** Development/Installation Artefacts - JUS HDS Services system design documentation; JUS HDS Services system configuration settings and associated documentation; other relevant documents or records **Examine:** Operational Artefacts - System and information integrity policy; procedures addressing information system error handling; **Test:** ST&E test result to demonstrate JUS HDS Services system compliance with the SR.

Department of Justice Canada
Help Desk and Support Services

Appendix E to Annex A
Definitions

Term	Definition
Abandoned Call	A telephone call that is connected to the Contractor's telephone system and the Calling Party terminates the call before a Service Desk Agent answers the call.
Acceptance Test Plan (ATP)	The document which describes the tests that the Contractor must perform on the Work before submitting it to Canada.
Account	The combination of Identity Profile, data attributes, credential bindings and authorizations.
Administrator	A User that is authorized to perform administrative operations for the JUS HDS Services.
Affiliate	For the purposes of this solicitation, an Affiliate will include any entity which does not operate at arm's length from the Respondent, including a parent or a branch, division or subsidiary of the Respondent.
Alternate Service Channel	All Service Channels to obtain support over and above Telephone and Web-Chat Support. This includes Voice-mail, Email and Service Delivery Portal Self Service.
Application Support	Support for a commercial software or custom developed application.
Asset Management	Discipline for tracking and managing the lifecycle of an asset including acquisition, installation, changes, and disposal. Assets can include Hardware or Software.
Asset Management Record	A collection of information for a specific Hardware or Software Asset. Information could include (but not limited to) Asset Tag, Description, Make, Model, Location and Assignee.
Authentication	Process to verify the digital identity of the sender of a network communication.
Authorized End User	An End User that has an Account on the Service Delivery Portal.
Bid	An offer to provide services and supply goods for the Contract Period as a result of this solicitation.
Bidder	A Respondent submitting a Bid.
Billing Detail File	File that contains Billing Records.
Billing Record	Record in a Billing Detail File that includes a single charge inclusive of all fees or discounts.

BlackBerry	A registered trademark of BlackBerry Corporation.
BlackBerry Device	Any Canada-owned Mobile Device from BlackBerry.
Building	Name of a building where a Service Delivery Point is located.
Calendar Month	From 00:00 the first day of the month to 24:59 the last day of the month
Canada Certificate Authority	Canada-owned Certificate Authorities.
Canada Data Centre LAN	LAN infrastructure located at Canada Service Delivery Points
Canada Directory	A Canada-owned directory system that is a repository for User identities information.
Canada File Service	A Canada-owned network service to allow End Users to store files on networked file servers.
Canada LAN	LAN infrastructure located at Canada Service Delivery Points
Canada Print Service	A Canada-owned network service to allow routing of print jobs to networked printers.
Canada Secure Perimeter	Canada-owned and managed IT infrastructure and services that mitigate security risks associated with connecting to GC Network (GCNet).
Catalogue	A collection of Services or Products available for ordering at a specified price.
Certificate	An public key certificate, in a format which is in accordance with ITU-T recommendation X.509 V3, as described in rfc5280(http://www.ietf.org/rfc/rfc5280.txt), which contains a public key of a subscriber, which can be an individual or a device, together with related information that is digitally signed with the private key of the Certification Authority that issued the Certificate.
Certificate Authority	An authoritative entity that issues Certificates.
Change Management	Standardized methods and procedures used for efficient and prompt handling of all changes to JUS HDS Services, in order to minimize the number and impact of any related Incidents upon a Service.
Change Request	Request to make a change to the hardware, software, applications and processes used by the Contractor to deliver the JUS HDS Services. A Change Request is also known as a Request for Change.
Change Ticket	The means to record a Change Request.

City	Name of a city where a Service Delivery Point is located.
Client	Canada, those government institutions for whom Canada's services are mandatory at any point during the Contract Period, and other organizations for whom Canada's services are optional at any point during the Contract Period and that choose to use those services from time to time.
Committed Delivery Date	Date proposed by the Contractor, and approved by Canada, to successfully complete a Service Order.
Component Integration	The practice of combining individually tested software components into a managed configuration such as an OS Image with common software products .
Configuration Management	Standardized methods and procedures for changes made to hardware and software components of JUS HDS Services.
Configuration Management Database (CMDB)	A repository that holds a collection of IT assets that are commonly referred to as Configuration Items (CIs), as well as descriptive relationships between such assets.
Contractor Secure Perimeter	Contractor owned and managed Information Technology (IT) infrastructure and services that mitigate security risks associated with connecting to the Government of Canada (GC) Network.
Coverage Period	Day and time to provide services. Coverage Period has the same meaning as principal period of maintenance.
Customer Satisfaction Measurement Survey	An instrument to collect service satisfaction rating from the End Users which is distributed according to pre-established rules via the Service Delivery Portal.
Data Centre	A facility used to house computer systems and associated components, such as telecommunications and storage systems.
Dedicated Contractor Data Centre LAN	LAN infrastructure located at Contractor Service Delivery Points and dedicated to the JUS HDS Services.
Definitive Software Library (DSL)	A secure location, consisting of physical media or a software repository located on a network file server, in which the definitive authorized versions of all software are listed, stored and protected and from which control and release is managed.
Degraded Performance	All of the functions of the impacted JUS HDS Services are operational. Performance is slower than normal but causes minimal or no disruption to service delivery.
Denial of Service	An attempt to make a machine or network resource unavailable to its intended users. Examples include: bandwidth attack, distributed denial of service, backscatter, consumption of system

	resource attack, communication obstruction, disruption of state information, disruption to routing/DNS information and web defacement.
Device	A physical object (e.g., a projector, whiteboard, computer/laptop, printer).
Device Deployment	The process of preparing a device with all the required software and configuration and installing it at the destination location.
Email Support	The ability for End Users to communicate with the HDS Service Desk Service via Email.
Emergency Change	A Change Request to operationally restore a Service where the failure or degradation of the Service severely impacts Service delivery or to correct a security Incident.
End User	A person that is authorized to use the JUS HDS Services.
End User Device	A desktop or laptop computer, a Smartphone or a Tablet.
Enhancement	Often referred to as an ”interim release”. An interim release version of the licensed software, which is often documented by adding a further decimal and digit to the version or release number (i.e., V.X.X.2 would be the next enhancement after V.X.X.1).
Feature Profile	Identifies the features (i.e., options) of a Service Catalogue Item (SCI) for a JUS HDS Services.
Federal Government Working Day (FGWD)	A calendar day, except for Saturday, Sunday and the following holidays: 1. New Year’s Day[1]; 2. Good Friday and Easter Monday; 3. Victoria Day; 4. Canada Day; 5. Labour Day; 6. Thanksgiving Day; 7. Thanksgiving Day; 8. Remembrance Day[1]; 9. Christmas Day[1]; and 10. Boxing Day[2]. [1]If this holiday occurs on a Saturday or Sunday, then the following

	Monday will be a holiday [2] If this holiday occurs on a Saturday, then the following Monday will be a holiday. If this holiday occurs on a Sunday or Monday, then the following Tuesday will be a holiday.
Firm Monthly Rate	Firm all-inclusive rate per month.
Firm Unit Hourly Rate	Firm all-inclusive unit rate per hour.
Firm Unit Monthly Rate	Firm all-inclusive unit rate per month.
Firm Unit Price	Firm all-inclusive unit price.
Floor	Floor at a civic address where a Service Delivery Point is located.
Frequently Asked Questions	A web site that provides answers to a list of typical questions that End Users might ask regarding the Workplace Technology Devices or the HDS Managed Service.
Full Outage	All functions of the impacted JUS HDS Services are unavailable.
GC Network (GCNet)	Wide Area Network (WAN) infrastructure that interconnects Canada Local Area Networks (LANs).
GEDS	The Government Electronic Directory Service.
Geographic Boundaries of Canada	Geographic Boundaries of Canada refers to all locations within Canada and locations in foreign jurisdictions, such as embassies or other Canadian government offices that are afforded consideration under diplomatic law permitting Canada to control its assets.
Go Live Date	The date that the Contractor must begin to deliver complete operational JUS HDS Services as per SOW requirements.
Government Furnished Equipment (GFE)	Equipment or software that is owned by Canada and provided to the Contractor.
Hardware	A physical device or component such as a desktop, laptop, printer or monitor.
HDS Data (Help Desk and Support Data)	All data associated with HDS Managed Service on any media. This could include troubleshooting scripts, Service Management information, and the Self-Help Knowledgebase.
HTTP Request	Any HTTP message sent or received over transport layer protocol. Includes both secure (i.e., https://) and non-secure (i.e., http://) requests. The calculation HTTP Request response time begins from the time the HTTP Request crosses the contractor's network demarcation point until a response leaves the Contractor's

	network demarcation point.
Identity Profile	A collection of data attributes associated with a User, Service or Resource.
Incident	Event which is not part of the standard operation of a Service and which causes, or may cause, an interruption to, or a reduction in, the quality of that Service.
Incident Management	Standardized methods and procedures to restore a service to normal operation as quickly as possible and to minimize the impact on business operations
Incident Number	Unique identifier for an Incident.
Incident Ticket	Information attributes captured for an Incident. Examples could include Incident Number, Description, Resolution and Severity.
Information Breach	The intentional or unintentional release of secure information to an untrusted environment.
Infrastructure	Set of hardware, software and networks required to support the JUS HDS Services.
Infrastructure Component	A specific instance of hardware, software or network required to support the JUS HDS Services.
Installation	The general installation services provided by the Contractor. The Installation services requirements are described in JUS HDS Services Annex A: SOW and elsewhere in the Contract.
Internet	Collection of interconnected networks and application servers that are publicly accessible worldwide and that are commonly referred to as the Internet.
iOS Mobile Device	A Mobile Device that implements the iOS operating system version 5 or higher.
Item Number or Item No.	Unique identifier for a Service or Product as described in JUS HDS Services Annex C Pricing.
Justice Canada (JUS)	The Department of Justice Canada
JUS HDS Services (Justice Canada Help Desk and Support Services)	A Service, owned and managed by the Contractor, which can be ordered by Canada.

JUS HDS Services Data	All JUS HDS Services System Data and JUS HDS Services Management Data on any media.
JUS HDS Services Facility	A Contractor Service Delivery Point where JUS HDS Services Infrastructure is located.
JUS HDS Services Infrastructure	All hardware and software at Contractor Service Delivery Points that processes and stores JUS HDS Services Data and that Operators use to operate, administer and manage JUS HDS Services.
Knowledge Repository	An online database that systematically captures, organizes, and categorizes knowledge-based information and allows End Users to search the repository with thanks advanced search capabilities.
Known Error	Identified root cause of a Problem
Level 1 Support	A first contact point for End Users that resolves relatively common Incidents with Hardware and Software
Level 2 Support	A more experienced and knowledgeable supporting group that typically resolve more complex Incidents for Hardware or Software that Level 1 Support could not resolve.
Level 3 Support	A highly experienced and knowledgeable supporting group that typically resolve very complex Incidents for a Hardware or Software that Level 2 Support could not resolve.
License Management	Discipline for tracking and managing the lifecycle of a software license, including acquisition, installation, changes, and removal.
Local Area Network (LAN)	Supplies networking capability to a group of computers in close proximity to each other.
Maintenance Plan	Plan defining requirements for maintenance of hardware or software.
Maintenance Service	Means the services provided by the Contractor to deliver the Maintenance Plan.
Malware	Short for malicious (or malevolent) software. Used or created by attackers to disrupt computer operation, gather sensitive information, or gain access to private computer systems. It can appear in the form of application source code, scripts, active content, and other software.
Management Service Plan	Plan that specifies the service management to be provided by the Contractor for a JUS HDS Services

Management Services	IT Service Management services that includes: incident management, problem management, change management and release management.
Maximum Service Outage Time	Maximum accumulated outage time attributable to one or more Incidents in a calendar month.
Maximum Time to Restore Service	Maximum time to restore a JUS HDS Services for an Incident.
Microsoft	Microsoft is a registered trademark of Microsoft Corporation.
Mobile Code	Software programs or parts of programs obtained from remote information systems, transmitted across a network, and executed on a local information system without explicit installation or execution by the recipient. Mobile code technologies include, for example, Java, JavaScript, ActiveX, Postscript, PDF, Shockwave movies, Flash animations, and VBScript.
Mobile Device	A tablet, cell phone or smart phone.
Mobile Network	Public network for mobile devices.
Multi-Functional Device Printer	A Device that prints digital content onto paper, faxes digital content over a telephone line, scan paper into digital content and email scanned digital content.
National Interest	Concerns the defence and maintenance of the social, political and economic stability of Canada.
Network Address Translation (NAT)	Process of modifying network address information in datagram (IP) packet headers while in transit across a traffic routing device for the purpose of remapping one IP address space into another.
New Release	Means a system release, a version release, and interim release of licensed software, regardless of whether the Contractor refers to it as a “new release”.
On-Site Support Service	A JUS HDS Services owned and managed by the Contractor and located at Canada locations (e.g. office building, conference centres, court of law), that can be ordered by Canada to provide support to End Users.
Operations Centre	Contractor location that includes infrastructure and resources required for the centralized management and operation of the JUS HDS Services.
Operator	A person, under the control of the Contractor, which administers JUS HDS Services infrastructure.
Operator Account	The combination of Identity Profile, data attributes, credential bindings and authorizations for an Operator for JUS HDS Services Infrastructure components.

Original Equipment Manufacturer (OEM)	The manufacturer of the hardware, as evidenced by the name appearing on the hardware and on all accompanying documentation.
OS Image	A replica of the content of the disk drive of a computer configured with an operating system and a set of software for the purpose of replicating the computer configuration on another computer without the need to go through a formal installation each component.
OS Image Development	The process of developing a new OS Image.
OS Image Management	The process of integrating and testing updated software components into an existing OS Image.
Partial Outage	One or more functions of the impacted JUS HDS Services are unavailable or performance is degraded to the level to cause considerable disruption to service delivery.
Personal Information	Please refer to the Privacy Act, R.S.C., 1985, c. P-21, Section 3. Definitions (http://laws-lois.justice.gc.ca/eng/acts/P-21/page-1.html#docCont). 1)
Platform	General purpose information systems components used to process and store electronic data, such as desktop computers, servers, network devices, and mobile devices. Platforms usually contain server hardware, storage hardware, utility hardware, software and operating systems.
Portable Device	A computer that is designed to be moved from one place to another and includes a display, a keyboard and a pointing device. The portable device (e.g., a laptop, a notebook, a netbook, an ultrabook, etc.) is essentially equivalent to a desktop computer in capability.
Portable Digital Media	A form of electronic removable media (i.e., a USB key, a USB hard drive, a memory stick, etc.) where data are stored in digital form, which can be easily transported from place to place.
Portal Administrator	Person who manages privileges and Accounts on the Service Delivery Portal.
Postal Code	Means the postal code associated with a civic address.
Premium Service Level Plan	A collection of Service Level Targets that together make up the Premium Service Level Plan for a specific End User.

Premium User	An End User of the GC that is assigned to the Premium Service Level Plan, as identified by Canada.
Price Summary	Summary of prices/rates for the components required to make up a complete Product.
Privacy Breach	Incident involving the unauthorized disclosure of personal information.
Problem	Unknown cause of one or more Incidents, often identified as a result of multiple similar Incidents.
Problem Management	Standardized methods and procedures to minimize the impact of Problems for JUS HDS Services.
Problem Ticket	Information attributes captured for a Problem. Examples could include Problem Number, Description, Resolution and Severity.
Product	A JUS HDS Services software application ordered and subsequently owned by Canada.
Prohibited Software	A Software not permitted to be located on an End User Computing Device.
Project Management Body of Knowledge (PMBOK Guide)	A book which presents a set of standard terminology and guidelines for project management published by the Project Management Institute (PMI).
Protected Information	Information is "protected" if its disclosure could harm interests other than the "national interest." There are three levels of protected information: Protected A (low-sensitive): Applies to information that, if compromised, could reasonably be expected to cause injury outside the National Interest, e.g., disclosure of exact salary figures. Protected B (particularly sensitive): applies to information that, if compromised, could reasonably be expected to cause serious injury outside the National Interest, e.g., loss of reputation or competitive advantage. Protected C (extremely sensitive): applies to the very limited amount of information that, if compromised, could reasonably be expected to cause extremely grave injury outside the National Interest, e.g., loss of life.
Public Key Infrastructure (PKI)	Infrastructure that binds the publically available encryption and signing keys with their registered users or devices by means of a certificate authority.
Public Service	Government agency at the federal, provincial/state and

	municipality level.
Regional On-Site Support Personnel	Canada personnel that provides on-site support to End Users located outside the National Capital Region.
Release Management	Standardized methods and procedures for the integration and flow of development, testing, and deployment of JUS HDS Services.
Release Record	Information attributes captured for a Release. Examples could include Release Identifier, Description, Planned Release Date and Actual Release Date.
Remote Access	Access to the JUS HDS Services Infrastructure through an external network (e.g., the Internet).
Remote Management	Administrative or maintenance activities conducted by an Operator over a network.
Request for Proposal (RFP)	A form of bid solicitation used for complex requirements, where the selection of a supplier cannot be made solely on the basis of the lowest price. An RFP is used to procure the most cost-effective solution based upon evaluation criteria identified in the RFP.
Resolvable Incident	An Incident that can be resolved using troubleshooting scripts or the desktop management tool (i.e. does not require physical access to the device).
Return Merchandise Authorization (RMA)	Numbered authorization provided by a seller or a manufacturer to permit Canada to return an item for refund or replacement.
Return-to-Depot Instructions	A set of instructions that detail the process by which Canada may return defective equipment to the Contractor's facilities.
Room	A static physical location.
Root Cause Analysis	A method of problem solving that focuses on identifying the root causes of Incidents and Problems from their symptoms.
Rush Service Plan	A Service Level Target with maximum request per month for emergency situation to make up the Rush Service Level Plan for a specific End User.
SDPID	Alpha-numeric location identifier of the Service Delivery Point.
SDPName	Name of the Service Delivery Point.
Secure Perimeter	Logical and physical boundary around network accessible

	resources and information, which is controlled and protected against unauthorized access from outside of the boundary.
Security Assessment	The on-going process of evaluating the performance of IT security controls throughout the lifecycle of information systems to establish the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the departmental business needs for security. Security assessment supports authorization by providing the grounds for confidence in information system security.
Security Authorization	The on-going process of obtaining and maintaining official management decision by a senior organizational official to authorize operation of an information system and to explicitly accept the risk of relying on the information system to support a set of business activities based on the implementation of an agreed-upon set of security controls, and the results of continuous security assessment.
Security Incident	An unauthorized behaviour (against the security policy of the IT system) regarding the operation and administration of the IT system that has the potential to compromise the IT systems confidentiality, integrity, or availability.
Security Information and Event Management (SIEM)	A technology that provides real-time analysis (collection, aggregation, correlation) of security alerts generated by infrastructure components and applications.
Security Posture	A characteristic of an information system that represents the ability of implemented security controls to satisfy the business needs for security and counter a selected threat environment. Note: 1) A security posture that satisfies the business needs for security and counters a selected threat environment is deemed adequate. The security posture may vary over time, as threats and business needs for security evolve, and vulnerabilities are discovered. To maintain an adequate security posture requires the review and update of implemented security controls to adapt to changes. 2) The security posture of an information system is assessed using the same methodology as security risks assessment, and is thus a closely related concept. The adequacy of a security posture implies that the residual risks are low.
Security Requirements Checklist (SRCL)	Personnel and facility clearance requirements.

Self Service	A Service Channel for an End User to use the Service Delivery Portal to perform transactions (such as create an Incident Ticket) or get information (such as reference the Knowledgebase).
Service	A JUS HDS Services provided by the Contractor to Canada that is owned and managed by the Contractor.
Service Access Point	A logical reference label for a Service.
Service Catalogue Item (SCI)	A Service or Product that can be ordered from the pricing catalogue.
Service Channel	A mechanism for an End User to obtain support. Service Channels include Telephone Support, Self Service Support, Voice-Mail Support, Email Support and Web-Chat Support.
Service Credit	A fee that the Contractor must pay Canada upon failure to deliver on a Service Level Target for a given time frame.
Service Credit Period	The period of time from which a Service Credit is calculated and applied.
Service Delivery Interval (SDI)	The maximum amount of time for the Contractor to complete the Work described in a Service Order.
Service Delivery Point	Physical location in a building where a Service or Product is implemented.
Service Delivery Portal	Means the service portal, provided and managed by the Contractor after Operational Readiness. The requirements for the Service Delivery Portal are described in JUS HDS Services Annex A: SOW General subsection Service Delivery Portal and elsewhere in the Contract.
Service Delivery Portal Account	The combination of Identity Profile, data attributes, credential bindings and authorizations for a User, Administrator, Service or Resource defined by an Administrator in the Service Delivery Portal.
Service Desk	Refer to the section as described in JUS HDS Services SOW General subsection Service Desk.
Service Domain	Logical grouping of Services and Products that share a business or technical affinity such as type of Service and/or Product, trust relationship, technical authority, etc.
Service Level Plan	A collection of Service Level Targets that together make up the Plan that can be assigned to an End User population.
Service Level Target (SLT)	Value that is used to assess the performance, availability or quality of Service, Product or system as described in JUS HDS Services Annex A: SOW General subsection Service Level

	Targets.
Service Management Plan	Plan that specifies the service management to be provided by the Contractor for a JUS HDS Services.
Service Order	The request from Canada for a Service or Product that can be ordered from the pricing catalogue.
Service Order Period	Means the period between the date that the Service Order is transmitted to the Contractor and the end date specified in the Service Order.
Service Order Response	Number of Federal Government Working Days from the date of issuance of the Service Order to the Contractor until acceptance of the Work by Canada.
Service Platform	Hardware and/or software that is required for a JUS HDS Services Product to operate.
Service Project	Means the service project resulting from the Contracting Authority issuing a Service Order - Service Project. The requirements are described in the article titled Process for Issuing a Service Order sub-article Conducting The Work Ordered Under A Service Order - Service Project and elsewhere in the Contract.
Service Project Plan	Means the service project plan prepared by the Contractor for each Service Project. The requirements are described in the article titled Process for Issuing a Service Order sub-article Conducting The Work Ordered Under A Service Order - Service Project and elsewhere in the Contract.
Service Releases	Means a release of the Software which is designed to operate on designated combinations of computer hardware and operating systems. A new Service Release typically will be indicated by the addition of one (1) to the first digit of the release number i.e., v.2.X.X would be the next Service Release after v.1.X.X).
Service Request	Request from Canada for the Contractor to perform a service such as install software, or move a desktop.
Service Request Number	Unique Identifier for a Service Request.
Social Engineering	The manipulation of people into performing actions or divulging confidential information. Examples include phishing, whaling, and clone fishing.
Software	An application used by an End User. Software is typically installed on Hardware.
Software Client	Any GC-owned or managed user agent or application that connects to the JUS HDS Services.

Software License Record	A collection of information attributes for tracking a software license. Examples of information tracked could include an Identifier, Title of the License, Publisher, Version and Maintenance Expiry Date.
Software Package	A program or a set of programs that performs the installation of a Software on a target operating system.
Software Patches	An engineering fix to a problem that may be incorporated into a New Release to update licensed software in order to improve or correct errors or defects in the program code.
Software Publisher	The owner of the copyright in any software included in the bid, who has the right to license (and authorize others to license/sub-license) its software products.
Standard	Means the standard applicable to a JUS HDS Services Managed Service or Product. The Standard requirements are described in JUS HDS Services Annex A: SOW General, subsection Standards, and elsewhere in the Contract.
Standard Hardware and Software	The list of Canada approved hardware and software platforms, as presented in Appendix D - Standard Hardware and Software that must be supported by the Contractor.
Standard User	An End User of the GC that is assigned to the Standard Service Level Plan, as identified by Canada.
Statement of Work (SOW)	The Statement of Work (SOW) is a narrative description of the work required and stipulates the deliverables or services required to fulfill the contract. It defines the task to be accomplished or services to be delivered in clear, concise and meaningful terms.
Stop Clock	Time period that starts from the time one of the following event occurs and ends and when the event is resolved: 1. the affected application or device is not available to the Contractor when the Contractor arrives at the Service Delivery Point ready to resolve an Incident; 2. the Contractor encounters a health or safety related issue at the Service Delivery Point that prevents resolving an incident; 3. the Contractor is prevented from resolving an Incident as a result of a malfunction of an application or device for which the Contractor is not responsible; and 4. the Contractor is prevented from resolving an Incident as a result of delays caused by Canada.

System	A generic term used to mean network and other devices, operating systems, computing platforms, virtualization software and applications or any combination thereof. Its use is context specific.
Telephone Support	The ability for End Users to communicate with the HDS Service Desk Service by telephone.
Threat and Risk Assessment (TRA)	Structured process designed to identify risks and provide recommendations for risk mitigation through analysis of system / service critical assets, potential threat events / scenarios, and inherent vulnerabilities.
Threat Vector	A path or a tool that a hacker uses to gain access to a computer or network server in order to deliver a malicious outcome.
Total Response and Resolution Time	Time period that starts from the time an Incident Ticket is assigned to the Contractor, including the time the Contractor uses to travel to the affected Service Delivery Point, excluding the Stop Clock time, and ends when the malfunctioning application or device has been repaired and is turned over to the End User for regular use at full functionality.
Unauthorized Access	When an entity gains unauthorized access to a system in order to commit another crime such as destroying information contained in that system. Examples include: infiltration, compromise, hacking, privilege escalation and unauthorized access/privilege.
Upgrades	Means an update to the Licensed Software to add, extend, enhance and/or improve the existing features, functionality and/or performance of the program code, which is documented by a version or build number change to the right of the first decimal (i.e., Product X Version 1.0 changes to Product X Version 1.1 or Product X Version 1.0.0 changes to Product X Version 1.0.1), regardless of whether the Contractor refers to it as a “minor upgrade” or “major upgrade”.
User Agent	Software that is acting on behalf of a User.
User Service Domain (USD)	Service Domain containing one or more user based Products and/or Services
Virtual Assistant	A virtual chat capability within the SDP tools that gives the End Users the ability to ask questions without the assistance of an Service Desk agent by searching answers from the Knowledge Repository

Voice-mail Support	The ability for End Users to communicate with the HDS Service Desk Service via Voice-mail.
Web Browser Client	A mobile or desktop web browser that connects to the JUS HDS Services using HTTP/HTTPS.
Web-Chat	A Service Channel for an End User to get support by on-line chatting with the HDS Service Desk Service.
Windows Mobile Device	A Mobile Device that implements the Windows operating system version 8 or higher.
Work Completion Notice	Means the Contractor's certification that the Work has been inspected and tested in accordance with the Acceptance Test Plan (ATP).

Department of Justice Canada
Help Desk and Support Services

Appendix F to Annex A
Standard Hardware and Software

This appendix contains the following information:

Table 1 - Software List L1	Presents the detailed list of Software currently in use at Justice Canada that must be supported by the JUS HDS Services.
Table 2 - Hardware List	Presents the detailed list of Hardware currently in use at Justice Canada that must be supported by the JUS HDS Services.
Table 3 - OS Image	Presents the current OS Images at Justice Canada that must be supported by the JUS HDS Services
Table 4 - Software List L2	Presents the list of Software currently in use at Justice Canada that must be supported by the JUS On-Site Support Service
Table 5 - SCCM Packages L3	Presents the list of SCCM Software Packages currently in use at Justice Canada that must be supported by the JUS HDS Services

Table 1 - Software List L1

Software Product	Install Type	Supported Version	Language	Scope
7-ZIP	Client	9.20 and higher	EN	NCR
ABBYY FineReader Professional Edition	Client	9.0	EN	NCR
Aboriginal Litigation Management Portal	None (Web)		EN	NCR
Aboriginal Research Network	None (Web)		EN	National
Access Pay			EN	Regional - ARO
AccessPro by Privasoft (see ATIPFlow and ATIPImage)	Client		EN	National
Accommodation and Car Rental Directory			EN	
Admin Law Digest			EN	National
Adobe Acrobat Professional X	Client	10	EN	National
Adobe Acrobat Reader	Client	8.1.5	EN and FR	National
Adobe Acrobat Reader X	Client	10.1.13	EN	National
Adobe Acrobat Writer	Client	All versions	EN	National
Adobe Creative Suite	Client	All versions	EN	National
Adobe Digital Editions	Client		EN	NCR
Adobe Flash Professional CS6	Client	CS6	EN	NCR
Adobe FlashPlayer (formerly Macromedia Flash)	Client	All versions	EN	National
Adobe Photoshop	Client		EN	National
Amax		3.1	EN	
AMX	Client		EN	NCR
Antidote HD - FR	Client		FR	National
Antidote 8 (Druide)	Client		FR	National
AnzioWin (Library group)	Client	12.6	EN	National
ArcGis	Client	10.0	EN	NCR
Archibus		17.0	EN	NCR
ArcMap	Client		EN	Regional - BCRO
ArcSoft Photosuite	Client		EN	Regional - ARO
ArcView	Client	9.3	EN	National
ARO Phone Directory	None (Web)		EN	Regional - ARO
ATIP Log			EN	Regional - ORO
ATIPFlow - being replaced by Privasoft AccessPro	Client	7.0	EN	NCR
ATIPImage - EN - being replaced by Privasoft AccessPro	Client	1.6	EN	NCR
Atlantic Regional Office Intranet	None (Web)		EN	Regional - ARO
Autocad	Client		EN	National
AVS Media Player	Client		EN	Regional - ARO
Bamboo Fun Pen & Touch Software by Wacom	Client		EN	NCR
BassetPro	Both		EN	NCR
BB USB Drivers	Client	4.7	EN	National
BCRO Phone List			EN	Regional - BCRO
Beyond 20/20	Client		EN	NCR
Biblionet PC Setup Procedures (includes Marc Notepad, BookWhere, Handheld Pen Scanners, SnagIT, OPAC Kiosk and AnzioWin Terminal - Innopac)	Client		EN	NCR
BlackBerry Web Components	Client		EN	National
Boardroom Booking			EN	Regional - ARO
Book Collector			EN	NCR
BrainBuilder	Client		EN	NCR
Business Objects XI (Crystal Reports)	Client	XI	EN	National
Camtasia	Client	Studio 7 and 8	EN	NCR
Canada Lands Overlay	Client		EN and FR	National
Canadian Registry of Divorce Proceedings			EN	National
CardFile	Client		EN	
Casebook Scan Share Desktop Shortcut			EN	National
Casemap		5.0	EN	NCR and Region - ARO
Caseview			EN	National
ccmMercury			EN	National
ccmMercury 4.01 Patch 5		4.01 patch 5	EN	National
CD Burner Software	Client	All versions	EN	National
Check and Get	Client		EN	NCR
Citrix XenApp Web ICA Client	Both	11	EN	National
ClearQuest		All versions	EN	NCR

Table 1 - Software List L1

Software Product	Install Type	Supported Version	Language	Scope
Code Criminel Annoté		All	FR	National
Codian Video Decoder	Client	All versions	EN	NCR
Cognos PowerPlay	Client		EN	NCR
Commissionaires Enterprise Management System	Client	All	EN	NCR
COMMport	Client	All versions	EN	National
CommVault	Server		EN	National
Compensation Web Access	Server		EN and FR	National
Computrace	Client		EN	Regional - BCRO
Consolidated Statutes and Regulations of Canada	Client		EN	National
Copernic Agent Basic	Client		EN	NCR
Corel Draw	Client	13.0	EN	National
Corel WordPerfect for Windows	Client	All versions except 5.1, 6 and 6.1	EN	National
Corel WordPerfect Office X5	Client	X5	EN	National
Corporate Antivirus	Both		EN	National
Corporate Email System	Both		EN	National
Correspondence Tracking			EN	Regional - ARO
Cost Recovery System			EN	Regional - BCRO
CPC View ax (download when installing Régistre Foncier du Québec - http://www.registrefoncier.gouv.qc.ca/sirf/)	Client	All versions	FR	National
Crime/Knowledge Base	Server		EN	National
Criminal Pleading and Practice in Canada	Client		EN	National
CryptoCard Token Software	Both		EN	National
Crystal Reports	Client		EN	National
Dashboard	Client		EN	Regional - ARO
Dashboard (ARO Software)	None (Web)		EN	Regional - BCRO
Dashboard (ticket and inventory tracking)	None (Web)		EN	Regional - PRO
Database - Bibliothèque-Library			EN	Regional - QRO
DBText			EN	Regional - ARO
DBText/Genie			EN	Regional - BCRO
Deliveries Log	Server		EN	Regional - BCRO
Delrina Form Flow Version (Required for Eforms to run)	Client	1.0	EN	National
Description Plus (also known as UCS)	Client		EN	National
Dial-Up Connectivity (AT&T) / Connexion par accès commuté (AT&T)	Client		EN	National
DocMapper	Client	5.2	EN	National
Document Scrubber	Client		EN	Regional - BCRO
Dot Net	Client	2.0	EN	National
Dragon Naturally Speaking (Dragon Dictate)	Client	All versions	EN	National
DreamWeaver MX	Client	All versions	EN	National
Drug Treatment Court Information System (DTCIS)			EN	NCR
Dymo LabelWriter Printer	Client	8.3	EN	National
eCarswell CiteLink Canada - EN	Client	1.0	EN	National
eCopy	Client		EN	NCR
eFormXpress	Both	3.0	EN	National
EICON Aviva	None (Web)	n/a	EN	National
Electronic Document Management System	Both		EN	National
Electronic Exit Report			EN	Regional - QRO
Electronic Register for Visitor Management			EN	Regional - QRO
Enfish	Client		EN	National
Enterprise Connect (open text)	Client	N/A	EN	National
Entrust Entelligence Security Provider 9.1 - PLEASE NOTE THAT USERS WHO HAVE SSM CANNOT BE UPGRADED AND MUST KEEP VERSION 7 OF ENTRUST	Client	9.1	EN	National
Epic (now called Arbortext Editor)	Client		EN	National
ePO Client Upgrade	Both	4.0	EN	NCR
ePO Fix	Both		EN	National
Ergonomics Application			EN	Local

Table 1 - Software List L1

Software Product	Install Type	Supported Version	Language	Scope
eTravel (Web-based)	None (Web)		EN	Local
Eureka Intranet Site	Client		EN	NCR
Evidence Reviewer by March Networks	Client	5.4 and 5.5	EN	National
Evidence Tracking			EN	Regional - BCRO
Expertise of Staff			EN	Regional - ORO
Expertise Search			EN	Regional - BCRO
Extranet	Client		EN	National
Extranet Forums	Client		EN	National
Extranet Surveys	Client		EN	National
Family Orders and Agreements Enforcement Assistance			EN	NCR
FCYInfo and FCYCOM			EN	NCR
FedEx Ship Manager Software	Client	2509	EN	NCR
File Association Fix	Client		EN	National
Filemaker Pro	Client	8.0	EN	National
Financial Signing Authority			EN	National
Financial Situation Report (FSR Desktop Shortcut)			EN	National
Fines and Recoveries (FRIC)			EN	Regional - QRO
Fireworks MX	Client	2004	EN	National
Folio Views (Required for Consolidated Statutes to work)	Client	4.7	EN	National
Folio-based Reference tools (Ewashcuk, Nova Scotia)			EN	Regional - ARO
FPS National Intranet Web Site	None (Web)		EN	National
FTI Ringtail IEM			EN	Regional - ARO
FTR Player and FTR Gold Player Plus	Client		EN	National
Garnishment, Attachment and Pension Diversion Action			EN	National
GC Secure Remote Access	Client		EN and FR	National
Generic Log			EN	Regional - BCRO
Génie automatisé et stratégique - Amélioration de la recherche en			FR	National
Google Earth	Client		EN and FR	National
Grants and Contributions Information Management System		8.0	EN	National
Groove 2007 - OAS	Client	2007	EN	NCR
HardCopy	Client		EN	NCR
HotDocs	Client		EN	NCR
HP Precision Scan	Client	5.0	EN	National
HR Charter	Client	9.5	EN	National
HR Exit Report			EN	Regional - PRO
HR Exit Survey / Sondage sur le départ des employés menés par			EN	National
Human Resources Management Systems (also known as MyLeave	Server		EN	National
Hummingbird DM	Both		EN	National
HW/SW Inventory			EN	Regional - ORO
iCal Web Calendars			EN	Regional - PRO
iCase	Both	1.3.1	EN	National
iCase Button	Client	1.4	EN	National
iCase Desktop Shortcut	Client		EN	National
iCase Email Add-in	Client		EN	National
iCase Timekeeping Video	None		EN	National
iCase Timekeeping Video for Montreal Users in Ottawa	None		EN	National
IDEA	Client		EN	NCR
Individual Learning Plan	Server	All versions	EN	National
Informatic Reformater		9.0	EN	Regional - ARO
InMagic CS/TextWorks			EN	Regional - BCRO
INNOPAC			EN	NCR
Inspections Application			EN	Regional - ARO
Integrated Finance and Materiel System IFMS SAPGUI 7.28 - EN		7.28	EN	National
Intellitrack			EN	Regional - ORO
Interest Calculator - Pre and Post Judgement			EN	Regional - BCRO
Internet DOJ			EN	National
Intranet (JUSnet) Search	None (Web)		EN	National
Intranet (JUSnet) Web 500	None (Web)		EN	National
Intranet (JUSnet) Web News Management	None (Web)		EN	National
Intranet (JUSnet) Web Stats	None (Web)		EN	National

Table 1 - Software List L1

Software Product	Install Type	Supported Version	Language	Scope
Intranet 404 Error	None (Web)		EN	National
Intranet Calendar			EN	National
Intranet Content Management			EN	National
Intranet DOJ	None (Web)		EN	National
Intranet Forms			EN	National
Intranet Forums			EN	National
Intranet HRDC Web Site			EN	National
Intranet Permissions Management			EN	National
Intranet Pro Active Disclosures			EN	National
Intranet Publications Management			EN	National
Intranet SetLang			EN	National
Intranet Site List			EN	National
Intranet SOQ			EN	National
Intranet Surveys			EN	National
IP Printer Web Page			EN	Regional - BCRO
iRIMS 9.1 for RDIMS (including bar codes) (Web-based Recorded Information Management System)	Client	9.1	EN	National
ISYS			EN	Regional - BCRO
iTunes	Client	10.5	EN	National
Java Runtime Environment - EN	Client	6.0.200.2	EN	National
JAWS for Windows	Client	All versions	EN	NCR
JMP (made by SAS)		All versions	EN	National
JUST			EN	NCR
Justice Electronic Forms	None (Web)		EN	
JusticeClass			EN	Regional - BCRO
Kentika	Both	All versions	EN	National
Keyview for Lotus	Client		EN	National
Le Grand Robert	Client		FR	National
Le Petit Robert	Client		FR	National
Legal Opinions and Precedents Online Retrieval System			EN	National
Legal Reference			EN	National
Legislation Information Management System			EN	National
LIMS Consolidation			EN	National
LIMS Drafting			EN	National
LIMS Printing			EN	National
LIMS Publishing			EN	National
Liste téléphonique			FR	Regional - QRO
Litigation - Blood			EN	Regional - QRO
Litigation - Breast Implant			EN	Regional - QRO
Litigation - Commandite			EN	Regional - QRO
Litigation - Opinion-Révocation			EN	Regional - QRO
Litige - Biere			FR	Regional - QRO
Macromedia FlashPlayer / disable autoupdates EN/FR	Client	10	EN and FR	National
Mail Log and BF System			EN	NCR
MailFrontier Anti-Fraud Component	Server		EN	
Management Commentary			EN	Regional - BCRO
McAfee Desktop Firewall	Client		EN	National
McAfee Host Intrusion Prevention System (HIPS)	Both		EN	National
McAfee RegFix	Client	8.0	EN	National
Microsoft Access 2007	Client	2007	EN	National
Microsoft Bitlocker			EN	National
Microsoft Exchange	Server	2007	EN	National
Microsoft FrontPage 2002	Client	2002	EN	National
Microsoft FrontPage 2003	Client	2003	EN	National
Microsoft IIS	Server	4.5, 5	EN	National
Microsoft InfoPath	Client	2007	EN	National
Microsoft Internet Explorer	Client	8.0	EN	National
Microsoft Live Meeting	Both	2007	EN	National
Microsoft Lync	Both	2013	EN	National
Microsoft Office Professional Plus 2013 MUI	Client	2013	EN and FR	National
Microsoft Project 2010 Professional - EN / FR	Client	2010	EN and FR	National
Microsoft Project 2013 Professional - EN / FR	Client	2013	EN and FR	National
Microsoft Sharepoint Designer 2010	Client	2010	EN	National

Table 1 - Software List L1

Software Product	Install Type	Supported Version	Language	Scope
Microsoft Silverlight	Client	4.0.51204.0	EN	National
Microsoft Visio 2010	Client	2010	EN	
Microsoft Visio 2013	Client	2013	EN	
Microsoft Visual Basic	Client	All versions	EN	National
Microsoft Visual Studio	Client	All versions	EN	NCR
Microsoft Windows	Client	WIN 7 / WIN 8	EN and FR	National
Microsoft Windows Media Player	Client	All versions	EN	National
Microsoft Windows Millenium ILS	Client	2009B 1.3	EN	NCR
Mindjet MindManager Pro	Client	6.0	EN	NCR
Minutes Meeting Edition Wizard			EN	Regional - QRO
Mozilla Firefox	Client	3.0	EN	National
MSDN Library for Visual Studio 2005	Client		EN	National
Nakisa OrgManagement Series	Client	2007 R6	EN	National
Neevia Document Converter Pro			EN	Regional - ARO
Nero CD and DVD Burning Software	Client	7.0	EN	National
Netscape	Client	All versions	EN	National
New Staff Notification			EN	Regional - BCRO
NewsDesk (NewsClippings) / InfoMédia			EN and FR	National
Non-Biz			EN	Regional - ORO
Office Automation Suite			EN	National
Official Languages Information System (OLIS) / Système d'information sur les langues officielles (SILO). This product is also known as SLE (Second Language Evaluation).		All versions	EN	National
Olympus Dictation Software	Client		EN	National
Olympus DSS Player Pro	Client	All versions	EN	National
Omniform (Nuance)	Client	4 and 5	EN	National
Omnipage Pro	Client		EN	National
Online Inventory Learning Materials	None (Web)		EN	Regional - PRO
Online Pay (also known as Eicon Aviva)			EN	National
Online Training System			EN	Regional - BCRO
Orchestra			EN	NCR
Ordering			EN	Regional - BCRO
OrgPlus	Client		EN	National
ORO Phone Book			EN	Regional - ORO
Outil de gestion des initiatives nationales			FR	Regional - QRO
Outlook Holiday Patch	Client		EN	National
Pay and Benefits Calculator			EN	Regional - ARO
PC Inventory and Application Deployment			EN	NCR
PDF Creator	Client	0.9.3	EN	National
PeopleSoft Enterprise (may also be called MyLeave or HRMS)		8 SP 1	EN	National
Perseus Survey Solutions - EN	Client	7.0	EN	National
PESDM FoxPro Database (Position Exclusion System			EN	NCR
Photorooter			EN	Regional - ORO
PKI Certificate	Client		EN	National
Post MDT Apps			EN	National
PRO Phone Directory			EN	Regional - PRO
ProCite	Client		EN	NCR
Project Control System (PCS) / Système de contrôle des projets			EN	National
PRONet Regional Intranet	None (Web)		EN	Regional - PRO
Public DOJ Internet 404 Error	None		EN	National
Public DOJ Internet Content Management	None (Web)		EN	National
Public DOJ Internet Forms	None (Web)		EN	National
Public DOJ Internet Forums	None (Web)		EN	National
Public DOJ Internet Keep in Touch	None (Web)		EN	National
Public DOJ Internet NewsRoom	None (Web)		EN	National
Public DOJ Internet ProActive Disc Web	None (Web)		EN	National

Table 1 - Software List L1

Software Product	Install Type	Supported Version	Language	Scope
Public DOJ Internet Publishing Management	None (Web)		EN	National
Public DOJ Internet Research and Stats	None (Web)		EN	National
Public DOJ Internet SetLang	None (Web)		EN	National
Public DOJ Internet Surveys	None (Web)		EN	National
Public DOJ Internet Verity Search	None (Web)		EN	National
Public DOJ Internet Victims of Crimes	None (Web)		EN	National
Public DOJ Internet Web Stats	None (Web)		EN	National
Pure Edge Viewer		6.5	EN	Regional - ARO
Q&A (Questions and Answers)			EN	National
QRO Business Planning			EN and FR	Regional - QRO
QRONET/Intranet Web Site and Tools	None (Web)		EN and FR	Regional - QRO
Qualisult (NO NEED TO LOG A CASE)			EN	National
QuickLaw and Quickfind - EN		Web	EN	National
QuickLaw and Quickfind - FR		Web	FR	National
QuickLaw Invoicing			EN	Regional - BCRO
Quicktax	Client	All versions	EN	National
Quicktime	Client		EN	National
Quickview Plus - EN	Client	8.0 and now 12.0	EN	National
QWS3270 Plus Jolly Giant Software - ENG	Client	4.4	EN	
RDIMS - Patch 1 (TO1)			EN	Regional - ORO
RDIMS Cache Patch			EN	National
RDIMS_01E (TO1)			EN	Regional - ORO
RealPlayer	Client	15.0.1.13	EN	National
Recorded Information Management System		All	EN	National
Records, Document and Information Management System		All	EN	National
Reda/Electronic Register Appeal File			EN	Regional - QRO
Reference Materials Library			EN	National
Registre Foncier du Québec en ligne				National
Report Web			EN	Regional - BCRO
RE-TOS Calculation System - EN		4.0.1	EN	National
Revue de presse / Newspaper cutting			EN and FR	Regional - QRO
RIMS 9.1 (DSN and Bar Code 99 and Shortcut)			EN	National
Ringtail Image Viewer	Client	3.100	EN	National
Ringtail Litigation Support Software			EN	National
Rogers Sierra Aircard USB-308 for Rogers	Client		EN	National
Roxio CD and DVD Burning Software	Client	All versions	EN	National
RSS Feed	Client		EN	National
Salary Forecasting Tool			EN	National
Salary Management System - EN / FR replaced by Salary			EN	National
Sales Tax Generator			EN	Regional - ARO
Sanyo Digital Voice Recorder	Client	All versions	EN	National
SAP GUI 7.10 Icon (only)		7.28	EN	National
SAP R/3		R/3 4.7	EN	National
SAS JMP		All versions	EN	National
Scanner Software		All versions	EN	National
SCCM 2007 Console		2007	EN	National
Search Engine Builder	Client		EN	National
Second Language Evaluation - same as Official Languages		All versions	EN	National
Secure Docs		4.9 r1	EN	National
Secure Remote Access (JUSaccess)	Client		EN	National
Secure System Model (SSM)			EN	National
Self-Assessment Checklist on the Implementation of the United Nation Convention Against Corruption			EN	NCR
Sentencing Decisions			EN	Regional - PRO
Sesame		2.2	EN	NCR
SmartDraw			EN	Regional - PRO
SnagIt	Client	All versions	EN	National
Snapshot-Boomerang Wizard			EN	Regional - BCRO

Table 1 - Software List L1

Software Product	Install Type	Supported Version	Language	Scope
Sony® Player Plug-in for Windows Media® Player Update (dvf	Client		EN	National
SPAM	Client		EN	National
Speech Exec Dictate from Phillips	Client	7.0	EN	NCR
SPSS (PASW)		All versions	EN	National
SQL Server		All versions	EN	National
SQL Server Client Utilities		7.0	EN	National
Staff Entry Exit Form			EN	Regional - ARO
Starship (Gov)		6.5.0	EN	National
Start Stop Universal Transcription System		All versions	EN	National
Stata		11	EN	NCR
Summation			EN	National
Supertext			EN	
Switch Plus Audio Converter Software		All versions	EN	National
Systems Management Server			EN	National
Tan Generator			EN	Regional - ARO
Tax Litigation Services			EN	National
Tax Pro			EN	National
Techshare			EN and FR	National
Termicom dBase			EN	National
Termium Plus			EN and FR	National
TextAloud		All versions	EN	National
TextAloud	Client	Any version	EN	NCR
TimeKeeper			EN	Regional - BCRO
TimeKeeping System (TKS) - Administrator Module			EN	National
TimeMap		4.0	EN	National
Train_Net			EN	National
Travel Expert System (Discontinued)		2.0	EN	
TreeAge			EN	Regional - BCRO
TrialMax		6.1	EN	National
Tunnel Guard or SmartCard (part of System Secure Model - SSM)			EN	National
Unsolicited Resumés			EN	Regional - ORO
USMT 4.0 Backup		4.0	EN	National
Virusscan 8.5 - SP7	Client	8.5	EN	NCR
Virusscan 8.5 - SP8 (only)	Client	8.5	EN	NCR
Virusscan 8.7i	Client	8.7i	EN	NCR
Visio Studio Tools for Office 2005	Client	2005.0	EN	NCR
VLC Media Player	Client	2.0.0	EN	National
WebEvent	Client		EN	Regional - ORO
Webex Player - EN	Client	All versions	EN	National
Whitesmoke Writer for Business			EN	National
Windows 7	Client		EN	National
Windows 8	Client		EN	National
Winnebago Serials Manager			EN	Regional - PRO
Winnebago Spectrum			EN	Regional - PRO
WipeDrive	Client		EN	NCR
Wireless	Client		EN	National
WORDQ	Client	2.0 and 3.0	EN	NCR
WorkDynamic		All versions	EN	National
Workflow File Management System			EN	NCR
WorkFlows Client for Unicorn			EN	Regional - PRO
WS_FTP (Ipswitch)	Client	All Versions (including the PRO version)	EN	National
Zoomtext Magnifier/Reader and Zoomtext Keyboard, CCTV	Client	All versions	EN	National

Table 2 - Hardware List

PRODUCT	SUPPORTED MODELS	INSTALLED BY	SUPPORTED BY	EFFECTIVE DATE	RETIREMENT DATE	WARRANTY	ADDITIONAL INFO
DESKTOPS							
Ciara	Q87M-XA	Contractor	Contractor	Jan/2014	Jan/2018	4 years	i5-4570
Northern Micro	P8Q77-IN SFF	Contractor	Contractor	Mar/2013	Mar/2017	4 years	
Hewlett-Packard	6005 Pro SFF	Contractor	Contractor	Mar/2012	Mar/2016	4 years	
LAPTOPS							
Toshiba	Portege R930	Contractor	Contractor	Mar/2014	Mar/2018	4 years	i5-3320M, 320 GB hard drive, 4GB RAM, DVD-RW
Toshiba	Portege R930	Contractor	Contractor	Mar/2013	Mar/2017	4 years	i5-3320M, 320 GB hard drive, 4GB RAM, DVD-RW
Toshiba	Tecra R850	Contractor	Contractor	Aug/2011	Aug/2015	4 years	i3-2310M, 320 GB hard drive, 4GB RAM, DVD-RW
Toshiba	Portégé R830 (tablet)	TSD	TSD	Aug/2011	Aug/2015	4 years	i3-2310M, 250 GB hard drive, 4GB RAM, DVD-RW
TABLETS							
Microsoft	Surface Pro	CSS	CSS	Pilot Project	Pilot Project	1 year	
Samsung	ATIV XE500T1C	CSS	CSS	Pilot Project	Pilot Project	1 year	
Dell	Latitude 10	CSS	CSS	Pilot Project	Pilot Project	1 year	
HP	elitePad 900	CSS	CSS	Pilot Project	Pilot Project	1 year	
PDA							
Blackberry	Z10	Contractor	Contractor			1 year	The Blackberry is the Department of Justice standard PDA.
Blackberry	Z30	Contractor	Contractor			1 year	The Blackberry is the Department of Justice standard PDA.
Blackberry	Q10	Contractor	Contractor			1 year	The Blackberry is the Department of Justice standard PDA.
Blackberry	Classic	Contractor	Contractor			1 year	The Blackberry is the Department of Justice standard PDA.
PRINTERS							
Network Multi-Function Printers							
Kyocera	Kyocera TASKalfa 4505ci KX	Contractor	Contractor				
Kyocera	Kyocera TASKalfa 4500i KX	Contractor	Contractor				
Xerox	Xerox Workcenter 7665	Contractor	Contractor	Aug/2010	Aug/2015	1 year on-site	Prior to purchasing network multi-function printers, users must contact the Help Centre.
Konica/Minolta	Konica/Minolta Bizhub C452	Contractor	Contractor	Nov/2010	Nov/2015	1 year on-site	Prior to purchasing network multi-function printers, users must contact the Help Centre.
Canon	Canon Image Runner C5045	Contractor	Contractor	Nov/2010	Nov/2015	1 year on-site	Prior to purchasing network multi-function printers, users must contact the Help Centre.
HP	HP LaserJet 4730	Contractor	Contractor	Jan/2011	Jan/2016	1 year on-site	Prior to purchasing network multi-function printers, users must contact the Help Centre.
HP	HP Laserjet 5035	Contractor	Contractor			1 year on-site	Prior to purchasing network multi-function printers, users must contact the Help Centre.
HP	HP Laserjet 4345	Contractor	Contractor			1 year on-site	Prior to purchasing network multi-function printers, users must contact the Help Centre.
HP	HP Laserjet 3035	Contractor	Contractor			1 year on-site	Prior to purchasing network multi-function printers, users must contact the Help Centre.
Network Colour Printers							
Lexmark	Lexmark c736dn	Contractor	Contractor	Aug/2010	Aug/2015	1 year on-site	
Network Printers							
Local printers							
Label printers							
Seiko	Seiko Smart Label 100	Contractor	Contractor				
Seiko	Seiko Smart Label 120	Contractor	Contractor				
Seiko	Seiko Smart Label 200	Contractor	Contractor				
Seiko	Seiko Smart Label 220	Contractor	Contractor				
Seiko	Seiko Smart Label 240	Contractor	Contractor				
Seiko	Seiko Smart Label 410	Contractor	Contractor				
Seiko	Seiko Smart Label 420	Contractor	Contractor				
Seiko	Seiko Smart Label 430	Contractor	Contractor				
Seiko	Seiko Smart Label 440	Contractor	Contractor				
Seiko	Seiko Smart Label 450	Contractor	Contractor				
Avery	Avery Personal Label 9100	Contractor	Contractor				
Brother	Brother PT-1950 (P-Touch)	Contractor	Contractor				
Brother	Brother PT-1960 (P-Touch)	Contractor	Contractor				
Brother	Brother PT-2100 (P-Touch)	Contractor	Contractor				
Brother	Brother PT-2500 (P-Touch)	Contractor	Contractor				
DYMO	DYMO LabelWriter 310	Contractor	Contractor				
DYMO	DYMO LabelWriter 320	Contractor	Contractor				
DYMO	DYMO LabelWriter 330	Contractor	Contractor				
DYMO	DYMO LabelWriter 400 Turbo	Contractor	Contractor				
DYMO	DYMO LabelWriter Duo	Contractor	Contractor				
DYMO	DYMO LabelWriter Twin Turbo	Contractor	Contractor				
MONITORS							
BenQ	BenQ BL2400	Contractor	Contractor	Mar/2013	Mar/2019	3 years	24" LED
Philips	Philips 225B2CB	Contractor	Contractor	Oct/2010	Oct/2016	3 years	22" LCD

Table 2 - Hardware List

PRODUCT	SUPPORTED MODELS	INSTALLED BY	SUPPORTED BY	EFFECTIVE DATE	RETIREMENT DATE	WARRANTY	ADDITIONAL INFO
LG	LG Flatron W2242PM	Contractor	Contractor			3 years	22" LCD
Samsung	Samsung 2243WM	Contractor	Contractor	Jul/2009	Jul/2015	3 years	22" LCD
PERIPHERALS							
Secure USB drives	Stealth MXP	Contractor	SRA			1 year	"ClipDrive" Bio only.
	Imation F100, 150					1 year	
	MXP Bio clips					1 year	
Scanner	Fujitsu 6130	Contractor	Contractor	Dec/2010	Dec/2015	1 year	recommended scanner for medium-volume scanning
	Fujitsu 6140	Contractor	Contractor	Dec/2010	Dec/2015	1 year	recommended scanner for high-volume scanning
	Fujitsu 6230	Contractor	Contractor	Dec/2010	Dec/2015	1 year	recommended scanner for medium-volume scanning
	Fujitsu 6240	Contractor	Contractor	Dec/2010	Dec/2015	1 year	recommended scanner for high-volume scanning
	HP 9250c Digital Senter	Contractor	Contractor			1 year	recommended scanner for medium-volume scanning
	HP Scanjet 8420	Contractor	Contractor			1 year	recommended scanner for medium-volume scanning
	HP Scanjet 8350	Contractor	Contractor			1 year	recommended scanner for medium-volume scanning
	Canon DR-9080c	Contractor	Contractor			1 year	recommended scanner for high-volume scanning
	Canon DR-7580	Contractor	Contractor			1 year	recommended scanner for high-volume scanning
Bar code scanner	Unitech MS100-4G	Contractor	Contractor				Model determined based on client requirements
	PSC Quickscan 6500	Contractor	Contractor				
DVD drive	All	Contractor	Contractor				Included with desktops
DVD-RW drive	All	Contractor	Contractor				Model determined based on client requirements
CD-RW drive	All	Contractor	Contractor				Model determined based on client requirements
External hard drive	All	Contractor	Contractor				Model determined based on client requirements
Video Card (Dual Monitor)	All	Contractor	Contractor				Model determined based on client requirements
TV tuner card	Hauppauge WinTV – HVR-1600	Contractor	Contractor				
Linksys router 4 port (wired)	BEFSR41	SRA	SRA				
Wireless routers	WRT54G	SRA	SRA				
Air Cards	Rogers 308USB, Rogers MF668USB, Rogers 330U, Bell U679, Bell U330, Telus 306USB, Telus 598USB.	OSS	OSS				
Digital Voice Recorder	Olympus	Contractor	Contractor	Dec/2009			Model determined based on client requirements - Minister's Office and SAT-6 Aboriginal Law Directorate - BRQ use Olympus Digital Voice Recorder
Webcam	Logitech	DESKTOP	DESKTOP	Jan/2011			Logitech 2.0/3.7 and Logitech C-310 (Procedures)

Number of OS Images to Support:

One (1) Windows 7 Enterprise 32-bit with French and English language pack
One (1) Windows 7 Enterprise 64-bit with French and English language pack
Contains:

- Microsoft Internet Explorer 11
- .NET framework 3.5 SP1 (included with Windows 7)
- Adobe Reader X
- Adobe Flash 21
- Silverlight 5.1x
- Java runtime environment 7 update 67
- Microsoft Office 2013 32-bit
- Windows Media Player 12 (comes with Windows 7)
- VLC 2.x
- PDF Creator 1.6x
- McAfee Agent 4.6.x
- McAfee VirusScan 8.8
- McAfee HIPS 7.0.0.1021
- SecureDoc 4.6
- Citrix Receiver 4.3
- Entrust ESP 9.2 for Windows

One (1) Windows 8 Enterprise (Tablets) 32-bit with French and English language pack
Contains:

- Microsoft Internet Explorer 11
- .NET framework 3.5 SP1 (NOT included with Windows 8 but installed as it is required for eBinder app)
- Adobe Reader X
- Adobe Flash 11 (included with IE 10)
- Silverlight 5.1x
- Microsoft Office 2013 32-bit
- Java runtime environment 7 update 67
- Windows Media Player 12 (comes with Windows 8)
- VLC 2.x
- McAfee Agent 4.6.x
- McAfee VirusScan 8.8
- McAfee HIPS 7.0.0.1021
- Citrix Receiver 4.3
- Entrust ESP 9.2 for Windows

One (1) Windows 8.1 Enterprise (Tablets) 64-bit with French and English language pack
Contains:

- Microsoft Internet Explorer 11
- .NET framework 3.5 SP1 (NOT included with Windows 8 but installed as it is required for eBinder app)
- Adobe Reader X
- Adobe Flash 11 (included with IE 11)
- Silverlight 5.1x (included with Windows 8.1)
- Java runtime environment 7 update 67
- Microsoft Office 2013 32-bit
- Windows Media Player 12 (comes with Windows 8.1)
- VLC 2.x
- McAfee Agent 4.6.x
- McAfee VirusScan 8.8
- McAfee HIPS 7.0.0.1021
- Citrix Receiver 4.3
- Entrust ESP 9.2 for Windows

Table 4 - Software List L2

Software Product	Install Type	Supported Version	Language
Adobe Acrobat Professional X	Client	10	EN
Adobe Acrobat Reader	Client	8.1.5	EN and FR
Adobe Acrobat Reader X	Client	10.1.2	EN
Adobe Acrobat Writer	Client	All versions	EN
Adobe Creative Suite	Client	All versions	EN
Adobe FlashPlayer (formerly Macromedia Flash)	Client	All versions	EN
Adobe Photoshop	Client		EN
Antidote HD - FR	Client		FR
Antidote RX (Druide) - FR	Client		FR
AnzioWin (Library group)	Client	12.6	EN
ATIPFlow - being replaced by Privasoft AccessPro	Client	7.0	EN
ATIPImage - EN - being replaced by Privasoft AccessPro	Client	1.6	EN
BB USB Drivers	Client	4.7	EN
Beyond 20/20	Client		EN
Biblionet PC Setup Procedures (includes Marc Notepad, BookWhere, Handheld Pen Scanners, SnagIT, OPAC Kiosk and AnzioWin Terminal - Innopac)	Client		EN
Casemap		5.0	EN
CD Burner Software	Client	All versions	EN
Citrix XenApp Web ICA Client	Both	11	EN
Code Criminel Annoté		All	FR
Cognos PowerPlay	Client		EN
Corel Draw	Client	13.0	EN
Corel WordPerfect for Windows	Client	All versions except 5.1, 6 and 6.1	EN
Corel WordPerfect Office X5	Client	X5	EN
CPC View ax (download when installing Régistre Foncier du Québec - http://www.registrefoncier.gouv.qc.ca/sirf/)	Client	All versions	FR
Description Plus (also known as UCS)	Client		EN
Dial-Up Connectivity (AT&T) / Connexion par accès commuté (AT&T)	Client		EN
DocMapper	Client	5.2	EN
Dot Net	Client	2.0	EN
Dragon Naturally Speaking (Dragon Dictate)	Client	All versions	EN
DreamWeaver MX	Client	All versions	EN
Drug Treatment Court Information System (DTCIS)			EN
Dymo LabelWriter Printer	Client	8.3	EN
eCarswell CiteLink Canada - EN	Client	1.0	EN
eCopy	Client		EN
Entrust Entelligence Security Provider 9.1 - PLEASE NOTE THAT USERS WHO HAVE SSM CANNOT BE UPGRADED AND MUST KEEP VERSION 7 OF ENTRUST	Client	9.1	EN
Eureka Intranet Site	Client		EN
File Association Fix	Client		EN
Filemaker Pro	Client	8.0	EN
Financial Signing Authority			EN
Financial Situation Report (FSR Desktop Shortcut)			EN
Fireworks MX	Client	2004	EN
Folio Views (Required for Consolidated Statutes to work)	Client	4.7	EN
FTR Player and FTR Gold Player Plus	Client		EN
GC Secure Remote Access	Client		EN and FR
HardCopy	Client		EN
HP Precision Scan	Client	5.0	EN
iCase Button	Client	1.4	EN
iCase Desktop Shortcut	Client		EN
iCase Email Add-in	Client		EN
iCase Timekeeping Video	None (Web)		EN
iCase Timekeeping Video for Montreal Users in Ottawa	None (Web)		EN
INNOPAC			EN
iRIMS 9.1 for RDIMS (including bar codes) (Web-based Recorded Information Management System)	Client	9.1	EN
Java Runtime Environment - EN	Client	6.0.200.2	EN
JAWS for Windows	Client	All versions	EN
JMP (made by SAS)		All versions	EN
Keyview for Lotus	Client		EN
Le Petit Robert	Client		FR

Table 4 - Software List L2

Software Product	Install Type	Supported Version	Language
Legal Reference			EN
Macromedia FlashPlayer / disable autoupdates EN/FR	Client	10	EN and FR
McAfee RegFix	Client	8.0	EN
Microsoft Access 2003	Client	2003	EN
Microsoft Access 2007	Client	2007	EN
Microsoft Bitlocker			EN
Microsoft Exchange	Server	2007	EN
Microsoft FrontPage 2002	Client	2002	EN
Microsoft FrontPage 2003	Client	2003	EN
Microsoft IIS	Server	4.5, 5	EN
Microsoft InfoPath	Client	2007	EN
Microsoft Live Meeting	Both	2007	EN
Microsoft Office 2007 Redaction Tool (Add-On)	Client	2007	EN
Microsoft Office 2007 Viewer - Compatibility Pack	Client	2007	EN
Microsoft Office 2007 Viewer - Compatibility Pack - Uninstall Old Versions	Client	2007	EN
Microsoft Office 2007 w/RDIMS	Client	2007	EN
Microsoft Office Live Meeting	Both	2007	EN
Microsoft Office Professional 2003 Pro Plus SP3 MUI	Client	2003	EN and FR
Microsoft Office Professional 2007 Pro MUI	Client	2007	EN and FR
Microsoft Outlook 2007 FR - Second Page Printing	Client	2007	EN
Microsoft Outlook Web Access	None (Web)	2003	EN
Microsoft Project 2003	Client	2003	EN
Microsoft Project 2007 Professional - EN / FR	Client	2007	EN and FR
Microsoft Project 2007 Standard - EN / FR	Client	2007	EN and FR
Microsoft Project 2007 Standard Uninstalll	Client	2007	EN and FR
Microsoft Publisher 2003	Client	2003-2007	EN
Microsoft Sharepoint Designer 2007 - no longer require to pay for licence but FP 2002 must be installed as it is the standard	Client	2007	EN
Microsoft Silverlight	Client	4.0.51204.0	EN
Microsoft Visio 2003 PRO	Client	2003	EN
Microsoft Visio 2007 PRO	Client	2007	EN
Microsoft Visio 2007 Viewer	Client	2007	EN
Microsoft Visual Basic	Client	All versions	EN
Microsoft Windows	Client	2002 (XP)	EN and FR
Microsoft Windows Media Player	Client	All versions	EN
Mozilla Firefox	Client	3.0	EN
Nero CD and DVD Burning Software	Client	7.0	EN
Netscape	Client	All versions	EN
Office Automation Suite			EN
Official Languages Information System (OLIS) / Système d'information sur les langues officielles (SILO). This product is also known as SLE (Second Language Evaluation).		All versions	EN
Olympus Dictation Software	Client		EN
Olympus DSS Player Pro	Client	All versions	EN
Omnipage Pro	Client		EN
Online Pay (also known as Eicon Aviva)			EN
OrgPlus	Client		EN
Outlook Holiday Patch	Client		EN
PDF Creator	Client	0.9.3	EN
Post MDT Apps			EN
ProCite	Client		EN
QuickLaw and Quickfind - EN		Web	EN
QuickLaw and Quickfind - FR		Web	FR
Quicktime	Client		EN
Quickview Plus - EN	Client	8.0 and now 12.0	EN
RDIMS Cache Patch			EN
RealPlayer	Client	15.0.1.13	EN
Reference Materials Library			EN
RE-TOS Calculation System - EN		4.0.1	EN
RIMS 9.1 (DSN and Bar Code 99 and Shortcut)			EN
Rogers Sierra Aircard USB-308 for Rogers	Client		EN
Roxio CD and DVD Burning Software	Client	All versions	EN

Table 4 - Software List L2

Software Product	Install Type	Supported Version	Language
Sanyo Digital Voice Recorder	Client	All versions	EN
SAP GUI 7.10 Icon (only)		7.28	EN
SAP R/3		R/3 4.7	EN
SAS JMP		All versions	EN
Scanner Software		All versions	EN
Second Language Evaluation - same as Official Languages Information System (OLIS)		All versions	EN
Secure Docs		4.9 r1	EN
Secure Remote Access (JUSaccess)	Client		EN
SnagIt	Client	All versions	EN
Sony® Player Plug-in for Windows Media® Player Update (dvf files)	Client		EN
SPSS (PASW)		All versions	EN
Start Stop Universal Transcription System		All versions	EN
Termium Plus			EN and FR
TimeMap		4.0	EN
Virusscan 8.5 - SP7	Client	8.5	EN
Virusscan 8.5 - SP8 (only)	Client	8.5	EN
Virusscan 8.7i	Client	8.7i	EN
Visio Studio Tools for Office 2005	Client	2005.0	EN
VLC Media Player	Client	1.2	EN
Whitesmoke Writer for Business			EN

Table 5 - SCCM Packages L3

SCCM Software Packages	Install Type	Supported Version	Language
Adobe Acrobat Professional X	Client	10	EN
Adobe Acrobat Reader	Client	8.1.5	EN and FR
Adobe Acrobat Reader X	Client	10.1.2	EN
Corel WordPerfect Office X5	Client	X5	EN
DocMapper	Client	5.2	EN
Dot Net	Client	2.0	EN
Dymo LabelWriter Printer	Client	8.3	EN
eCarswell CiteLink Canada - EN	Client	1.0	EN
Entrust Entelligence Security Provider 9.1 - PLEASE NOTE THAT USERS WHO HAVE SSM CANNOT BE UPGRADED AND MUST KEEP VERSION 7 OF ENTRUST	Client	9.1	EN
Epic (now called Arbortext Editor)	Client		EN
File Association Fix	Client		EN
iCase Button	Client	1.4	EN
iCase Desktop Shortcut	Client		EN
Integrated Finance and Materiel System IFMS SAPGUI 7.28 - EN		7.28	EN
iRIMS 9.1 for RDIMS (including bar codes) (Web-based Recorded Information Management System)	Client	9.1	EN
Java Runtime Environment - EN	Client	6.0.200.2	EN
Macromedia FlashPlayer / disable autoupdates EN/FR	Client	10	EN and FR
Microsoft Access 2003	Client	2003	EN
Microsoft Access 2007	Client	2007	EN
Microsoft FrontPage 2003	Client	2003	EN
Microsoft InfoPath	Client	2007	EN
Microsoft Internet Explorer	Client	8.0	EN
Microsoft Lync	Both	2010	EN
Microsoft Office Professional 2013 Pro Plus MUI	Client	2007	EN and FR
Microsoft OneNote 2007	Client	2007	EN
Microsoft Outlook 2007 FR - Second Page Printing	Client	2007	EN
Microsoft Project 2003	Client	2003	EN
Microsoft Project 2007 Standard - EN / FR	Client	2007	EN and FR
Microsoft Sharepoint Designer 2007 - no longer require to pay for licence but FP 2002 must be installed as it is the standard	Client	2007	EN
Microsoft Visio 2007 PRO	Client	2007	EN
Microsoft Visio 2007 Viewer	Client	2007	EN
Microsoft Windows Millenium ILS	Client	2009B 1.3	EN
Mozilla Firefox	Client	3.0	EN
PDF Creator	Client	0.9.3	EN
Post MDT Apps			EN
QWS3270 Plus Jolly Giant Software - ENG	Client	4.4	EN
RDIMS - Patch 1 (TO1)			EN
RDIMS Cache Patch			EN
RDIMS_01E (TO1)			EN
Recorded Information Management System		All	EN
Records, Document and Information Management System		All	EN
RIMS 9.1 (DSN and Bar Code 99 and Shortcut)			EN
Ringtail Image Viewer	Client	3.100	EN
Ringtail Litigation Support Software			EN
Rogers Sierra Aircard USB-308 for Rogers	Client		EN
SAP R/3		R/3 4.7	EN
SCCM 2007 Console		2007	EN
Sesame		2.2	EN
Sony® Player Plug-in for Windows Media® Player Update (dvf files)	Client		EN
USMT 2.6 Backup		2.6	EN
VLC Media Player	Client	1.2	EN

TASK AUTHORIZATION FORM
FORMULAIRE D'AUTORISATION DE TÂCHES

PART 1 (completed by the Technical/Project Authority) / PARTIE 1 (complété par le Responsable technique / Chargé du projet)

A. General Information / Informations générales

Contract Number / Numéro du contrat :

Contractor Name / Nom du Contracteur :

Task Authorization (TA) No. / Nº de l'autorisation de tâches (AT) :	Commitment No. / Nº de l'engagement :	Financial Coding / Code financier :	Date of Issuance / Date d'émission :	Response required by / Réponse requise par :

B. For Amendments Only / Aux fins de modification seulement

Amendment No. / Nº de la modification :

Reason for the Amendment / Raison pour la modification :

C. TA Requirements / Exigences relatives à l'AT

Required Resource(s) / Ressource(s) requise(s)

Category / Catégorie	Level / Niveau	Estimated Level of Effort (days) / Niveau d'effort estimatif (jours)	Linguistic Profile / Profile linguistique	Required Level(s) of Security / Niveau(x) de sécurité requis

Statement of Work (tasks, deliverables, reports, etc.) / Énoncé des travaux (tâches, livrables, rapports, etc.)

Period of Services / Période de service:

Initial Start Date / Date de début initiale :

Initial End Date / Date de fin initiale :

Extented End Date (See Reason for the Amendment) / Date de fin prolongée (voir Raison pour la modification) :

☐ Option To Extend Initial End Date / Option pour prolonger la date de fin initiale

Travel Requirement(s) / Exigence(s) de voyage :

Work Location(s) / Lieu(x) de travail :

PART 2 (completed by the Contractor and/or the Technical/Project Authority) / PARTIE 2 (complété par le Contracteur et/ou le Responsable technique / Chargé du projet)

A. Contractor Resource(s) / Ressource(s) du Contracteur

Note: once approved, only the following resources may provide services under this TA. / Nota : une fois approuvée, seules les ressources suivantes peuvent fournir des services sous la présente AT.

TASK AUTHORIZATION FORM
FORMULAIRE D'AUTORISATION DE TÂCHES

Name / Nom	Category / Catégorie	Level / Niveau	Linguistic Profile / Profile linguistique	Level of Security / Niveau de sécurité	PWGSC Security File No. / Nº du dossier de sécurité TPSGC	
						+ -

B. Estimated Cost / Coût estimatif

Category / Catégorie	Level / Niveau	Per Diem Rate / Taux journalier	Estimated Level of Effort (days) / Niveau d'effort estimatif (jours)	Total Cost / Coût estimatif	
					+ -
			Estimated Cost / Coût estimatif		
			Total Estimated Travel and Living Cost / Estimé des frais de déplacement et de subsistance	$0.00	
			Total Estimated Cost / Coût total estimatif	$0.00	

PART 3 - TA APPROVAL BY CANADA / PARTIE 3 - APPROBATION DE L'AT PAR LE CANADA

By signing this TA, the authorized client authority and/or the PWGSC Contracting Authority certify(ies) that the content of this TA is in accordance with the conditions of the Contract.

The client's authorization limit is $300,000.00 . When the value of a TA and its amendments (excluding GST/HST) is in excess of this limit, the TA must be signed by the authorized client and forwarded to the PWGSC Contracting Authority for authorization.

Name of Authorized Client / Nom du client autorisé

Date

Signature

En apposant sa signature sur l'AT, le client autorisé et/ou l'autorité contractante de TPSGC atteste(nt) que le contenu de cette AT est conforme aux conditions du contrat.

La limite d'autorisation du client est $300,000.00 . Lorsque la valeur de l'AT et ses modifications (excluant la TPS/TVH) dépasse cette limite, l'AT doit être signée par le client autorisé et transmise à l'autorité contractante de TPSGC pour autorisation.

Name of Contracting Authority / Nom de l'autorité contractante

Date

Signature

PART 4 - CONTRACTOR SIGNATURE / PARTIE 4 - SIGNATURE DU CONTRACTEUR

Name and Title of individual authorized to sign on behalf of the Contractor / Nom et titre de la personne autorisée à signer au nom de l'entrepreneur

Signature

Date

ATTACHMENT 1
CURRENT STATE INFORMATION

Safe Harbour Statement

The information contained in this document has been captured at various points from 2013 to 2016. It has been provided to help Bidders understand the current IT environment and related volumetrics for Justice Canada. Please note that this information is subject to change prior to contract award. This information cannot be interpreted as a contractual commitment.

Tab 1. Existing Service Levels includes the current service levels targets and calculation of service levels.
Tab 2. Office Locations presents the current Justice Canada locations across Canada.
Tab 3. Workstations by City summarizes the laptop and desktop distribution by major cities.
Tab 4. Workstations by Location summarize the laptop and desktop distribution by location.
Tab 5. Printer Assets summarizes the distribution of network printers of Justice Canada.
Tab 6. SSC Infrastructure provides background information on the SCCM Infrastructure.
Tab 7. Call Volume by Service presents call volumes by type of service for Justice Canada.
Tab 8. Call Volume by Interval presents call volume by hour for Justice Canada.
Tab 9. Calls by Source presents call volume by service channel source.
Tab 10. Calls by Product presents call volumes by type of product the call is about.
Tab 11. Incidents by Region presents incident counts by regions and service level.
Tab 12. Incidents by Product presents incident counts by type of product the call is about.
Tab 13. Incidents by Type presents incident counts by type of incident.
Tab 14. Break&Fix Metrics presents the statistics for Break/Fix related incidents.
Tab 15. Incident & Service Request presents incidents and service request volume metrics by region.
Tab 16. Service Request by Type presents services request counts by type of service performed.
Tab 17. Security Operations presents detections of undesirable software.
Tab 18. Encryption statistics to perform full disk encryption

Measurable Event	Service Level Requirement	Calculation
Service Desk – Telephone initial response time	Telephone calls are answered on or before the third ring, 95% of the time.	Call answer times must meet this maximum no less than 95% of the time. Otherwise, financial credits become available to the Department.
Service Desk – E-mail or web form incident report response time	Incidents reported via e-mail or web form are responded to within 30 minutes, 95% of the time.	Service response time must meet this maximum no less than 95% of the time. Otherwise, financial credits become available to the Department.
Service Desk – Telephone caller wait time	A Service Desk agent receives the call and speaks to the telephone caller within a maximum of 2 minutes, 95% of the time.	Call waiting times must meet this maximum no less than 95% of the time. Otherwise, financial credits become available to the Department.
Service Desk – Incident resolution percentage at First Point of Contact	85% of incidents reported to the Service Desk that are resolvable are resolved by the Service Desk agent, without escalation to another resolution group.	A minimum of 85% of resolvable incidents reported to the Service Desk must be resolved without escalation. Otherwise, financial credits become available to the Department.
Service Desk – Incident resolution time at First Point of Contact	The Service Desk agent resolves the incident or escalates to another resolution group within a maximum of 15 minutes, 95% of the time.	Initial incident resolution times must meet this maximum no less than 95% of the time. Otherwise, financial credits become available to the Department.
Onsite Services – Incident response time	An Onsite Services Representative visits the user and/or equipment involved and begin efforts to resolve the incident within a maximum of: Mission Critical Servers: 30 minutes Non-Mission Critical Servers: 4 hours Workstations / Printers: 4 hours from the time the Onsite Representative is assigned the	Incident response times must meet these maximums no less than 95% of the time. Otherwise, financial credits become available to the Department.
Onsite Services – Incident resolution time	75% of incidents are resolved the same business day, 95% of the time.	A minimum of 75% of incidents assigned to the Onsite Services team must be resolved the same business day. Otherwise, Justice Canada and the Contractor will have to discuss changes necessary to consistently achieve this service level.
Onsite Services – Correctly loading CD image, when required	Image loaded correctly 100% of the time	Incident reports and random testing to confirm service has been delivered as required.
Onsite Services – Complete installations (IMACRR – Installations)	Single workstation– max 2 hours Single notebook – max 2 hours Single Server – max 4 hours	Installation times must conform to these maximums.

Measurable Event	Service Level Requirement	Calculation
Onsite Services – Testing installations	Installation is tested to ensure all equipment functions correctly 100% of the time	Incident reports and random testing to confirm service has been delivered as required.
Onsite Services – Reporting on installations	The installation report is filed correctly 100% of the time	All reports checked at monthly SLR review meetings.
Hardware Break/Fix – Incident response time	A Hardware Technician visits the user and/or equipment involved and begins efforts to resolve the incident within a maximum of 4 hours from the time the Hardware Technician is assigned the incident, 95% of the time.	Incident response times must meet these maximums no less than 95% of the time. Otherwise, financial credits become available to the Department.
Hardware Break/Fix – Incident resolution time	All incidents are resolved within a maximum of 1 business day from the time the Hardware Technician is assigned the incident, 95% of the time.	Initial incident resolution times must meet these maximums no less than 95% of the time. Otherwise, financial credits become available to the Department.
Systems & LAN Mgt – Server Break / Fix Incident response time	A System & LAN Management Resource visits the user and/or equipment involved and begin efforts to resolve the incident within a maximum of: Mission Critical Servers: 30 minutes Non-Mission Critical Servers: 4 hours from the time the System & LAN Management Resource is assigned the incident, 95% of the time.	Initial incident response times must meet these maximums no less than 95% of the time. Otherwise, financial credits become available to the Department.
Systems & LAN Mgt – Server Break / Fix Incident resolution time	All incidents are resolved within a maximum of: Mission Critical Servers: 4 hours Non-Mission Critical Servers : 1 business day from the time the System & LAN Management Resource is assigned the incident, 95% of the time.	Initial incident resolution times must meet these maximums no less than 95% of the time. Otherwise, financial credits become available to the Department.
Systems & LAN Mgt – Backups completed correctly	Daily, Weekly, and Monthly backup operations are completed correctly 100% of the time.	Incident reports checked, backup reports checked at monthly SLR review meetings, random testing to confirm backups have been completed as required.
Systems & LAN Mgt – Backup media (tapes) handled and stored per approved procedures	Backup media (tapes) are handled and stored as per approved procedures 100% of the time.	Incident reports and random testing to confirm media has been handled and stored as per approved procedures.
Systems & LAN Mgt – Restore operations completed correctly	Restore operations are completed correctly 100% of the time.	Incident reports and random testing to confirm restores have been completed as required.
Systems & LAN Mgt – Restore operations completed on time	Restore operations are completed within one business day from when the request is received 95% of the time.	Incident reports and random testing to confirm restores have been completed as required.

Measurable Event	Service Level Requirement	Calculation
Systems & LAN Mgt – Data retention policies observed	Data retention policies are observed and adhered to 100% of the time.	Incident reports and random checking to confirm data retention policies are being observed and adhered to as required.
Systems & LAN Mgt – Documentation concerning major system and network events completed as required	Documentation concerning major system and network events are completed correctly 100% of the time.	Reports checked at monthly SLR review meetings, random checking, and annual audit.
Systems & LAN Mgt – Security policies and procedures adhered to	Security policies and procedures are observed and adhered to 100% of the time.	Incident reports and random checking to confirm security policies and procedures are being observed and adhered to as required.
Systems & LAN Mgt – Server system operations procedures adhered to	Server system operations procedures are observed and adhered to 100% of the time.	Incident reports and random checking to confirm server system operations procedures are being observed and adhered to as required.
Systems & LAN Mgt – Responding to Alarms	Alarms generated by server systems are responded to within a maximum of 15 minutes, 100% of the time.	Periodic and random checking of system logs to confirm server system alarms are being responded to as required.
Overall Services – Reports are accurate	Reports are accurate 100% of the time.	Reports checked at monthly SLR review meetings and random checking.
Overall Services – Reports delivered on time.	Reports are delivered on time 100% of the time.	Reports checked at monthly SLR review meetings.
Overall Services – Preventative Maintenance completed as required	All preventative maintenance tasks are comple ted as required 100% of the time.	Incident reports and random testing to confirm preventative maintenance tasks have been completed as required.
Overall Services – Disk erasure completed correctly	Whenever requested, disk erasures are completed correctly 100% of the time.	Incident reports and random testing to confirm disk erasures have been completed as required.
Overall Services – Security policies and procedures adhered to	Security policies and procedures are observed and adhered to 100% of the time.	Incident reports and random checking to confirm security policies and procedures are being observed and adhered to as required.
Overall Services – Invoicing accurate	Invoices are correct 100% of the time.	Invoices checked at monthly SLR review meetings and random checking.
Overall Services – Customer Satisfaction – Annual Survey	Customer satisfaction surveys demonstrate that 90% of Justice Canada users are very satisfied or satisfied	Annual survey checked.

Region	Province/Territories	Location	Building/Address
Prairie	Alberta	Calgary	Calgary - Barclay - 606-4th Street Southwest
Prairie	Alberta	Calgary	Calgary - Bantrel - 700 6th Avenue Southwest
Prairie	Ontario	Ottawa	Iqaluit - 933 Mivvik - 2nd Floor
Prairie	Alberta	Edmonton	Calgary - Bantrel - 700 6th Avenue Southwest
Prairie	Alberta	Edmonton	Calgary - Barclay - 606-4th Street Southwest
Prairie	Alberta	Edmonton	Edmonton - EPCOR
Prairie	Alberta	Edmonton	NRC - Wireless LAN
Atlantic	Nova Scotia	Halifax	ARO - Duke Tower
Atlantic	Nova Scotia	Halifax	ARO - Moncton
Atlantic	Nova Scotia	Halifax	ARO - St. Johns
Atlantic	Nova Scotia	Halifax	NRC - Wireless LAN
Northern Regions	Nunavut	Iqaluit	Iqaluit - 933 Mivvik - 2nd Floor
Northern Regions	Nunavut	Iqaluit	Iqaluit - 933 Mivvik - 3rd Floor
Quebec	Quebec	Montreal	NRC - Wireless LAN
Quebec	Quebec	Montreal	QRO - Complexe Guy Favreau
Ontario	Ontario	Ottawa	Iqaluit - 933 Mivvik - 3rd Floor
Ontario	Ontario	Ottawa	NCR - 160 Elgin
Ontario	Ontario	Ottawa	NCR - 180 Elgin
Ontario	Ontario	Ottawa	NCR - 222 Queen Street
Ontario	Ontario	Ottawa	NCR - 301 Elgin Street
Ontario	Ontario	Ottawa	NCR - 473 Albert - Trebla
Ontario	Ontario	Ottawa	NCR - 50 O'Connor Street
Ontario	Ontario	Ottawa	NCR - 99 Bank Street
Ontario	Ontario	Ottawa	NCR - BOC
Ontario	Ontario	Ottawa	NCR - Constitution Sq.
Ontario	Ontario	Ottawa	NCR - EMB
Ontario	Ontario	Ottawa	NCR - Jean Edmonds
Ontario	Ontario	Ottawa	NCR - SAT
Ontario	Ontario	Ottawa	NCR - Trebla
Ontario	Ontario	Ottawa	NCR - URB
Ontario	Ontario	Ottawa	NRC - Wireless LAN
Ontario	Ontario	Ottawa	Vancouver - 840 Howe St
Ontario	Ontario	Ottawa	Yellowknife - Joe Tobie Bldg
Prairie	Saskatchewan	Saskatoon	NRC - Wireless LAN
Prairie	Saskatchewan	Saskatoon	Saskatoon - 22nd Street East
Prairie	Saskatchewan	Saskatoon	Saskatoon - Princeton Tower - 2nd Avenue South
Ontario	Ontario	Toronto	NRC - Wireless LAN
Ontario	Ontario	Toronto	ORO - 130 King Street
Ontario	Ontario	Toronto	ORO - Brampton
Ontario	Ontario	Toronto	ORO - Exchange Tower 130 King Street
Ontario	Ontario	Toronto	ORO - Kitchener
Ontario	Ontario	Toronto	ORO - London

Region	Province/Territories	Location	Building/Address
Ontario	Ontario	Toronto	ORO - New Market
Ontario	Ontario	Toronto	ORO - Queen Street
Ontario	Ontario	Toronto	ORO - Watline Road
BC	British Columbia	Vancouver	NCR - URB
BC	British Columbia	Vancouver	NRC - Wireless LAN
BC	British Columbia	Vancouver	Vancouver - 211 Columbia Street
BC	British Columbia	Vancouver	Vancouver - 222 Main St
BC	British Columbia	Vancouver	Vancouver - 666 Burrard
BC	British Columbia	Vancouver	Vancouver - 800 Burrard
BC	British Columbia	Vancouver	Vancouver - 840 Howe St
BC	British Columbia	Vancouver	Vancouver - 900 Howe St
Northern Regions	Yukon	Whitehorse	Whitehorse
Northern Regions	Yukon	Whitehorse	Whitehorse - Elijah Smith Building - 300 Main Street
Prairie	Manitoba	Winnipeg	Edmonton - EPCOR
Prairie	Manitoba	Winnipeg	NRC - Wireless LAN
Prairie	Manitoba	Winnipeg	Winnipeg - Centennial House
Prairie	Manitoba	Winnipeg	Winnipeg - Donald Street
Northern Regions	The Northwest Territories / les Territoires du Nord-Ouest	Yellowknife	NRC - Wireless LAN
Northern Regions	The Northwest Territories / les Territoires du Nord-Ouest	Yellowknife	Yellowknife - Joe Tobie Bldg
Northern Regions	The Northwest Territories / les Territoires du Nord-Ouest	Yellowknife	Yellowknife - Nova Plaza - 52nd Street

3. Workstations by City

Cities/Villes	Desktop		Laptop		Totals		All Combined	
Ottawa	387	9%	963	21%	**1350**	30%	**1818**	40%
Toronto*	159	4%	406	9%	**565**	13%	**742**	16%
Vancouver	129	3%	306	7%	**435**	10%	**562**	12%
Montreal	110	2%	245	5%	**355**	8%	**417**	9%
Edmonton	84	2%	161	4%	**245**	5%	**318**	7%
Winnipeg	34	1%	74	2%	**107**	2%	**147**	3%
Moncton	4	0%	4	0%	**8**	0%	**16**	0%
St. John's	5	0%	5	0%	**10**	0%	**20**	0%
Halifax	36	1%	63	1%	**99**	2%	**136**	3%
Saskatoon	35	1%	68	2%	**103**	2%	**134**	3%
Yellowknife	14	0%	35	1%	**48**	1%	**76**	2%
Calgary	17	0%	27	1%	**44**	1%	**59**	1%
Whitehorse	8	0%	20	0%	**28**	1%	**43**	1%
Iqaluit	3	0%	8	0%	**12**	0%	**21**	0%
Totals/Totaux:	**1025**	23%	**2385**	53%	**3409**	76%	**4509**	100%

4. Workstations by Location

	Count of Desktop / Laptop
Calgary	60
Desktop	60
Calgary - Bantrel - 700 6th Avenue Southwest	40
Calgary - Barclay - 606-4th Street Southwest	20
Edmonton	449
Desktop	301
Edmonton - EPCOR	301
Notebook	148
Calgary - Bantrel - 700 6th Avenue Southwest	19
Calgary - Barclay - 606-4th Street Southwest	11
Edmonton - EPCOR	99
NRC - Wireless LAN	19
Halifax	**199**
Desktop	**143**
ARO - Duke Tower	126
ARO - Moncton	8
ARO - St. Johns	9
Notebook	**56**
ARO - Duke Tower	50
ARO - St. Johns	1
NRC - Wireless LAN	5
Iqaluit	**15**
Desktop	**13**
Iqaluit - 933 Mivvik - 2nd Floor	10
Iqaluit - 933 Mivvik - 3rd Floor	3
Notebook	**2**
Iqaluit - 933 Mivvik - 2nd Floor	1
Iqaluit - 933 Mivvik - 3rd Floor	1
Montreal	**499**
Desktop	**445**
QRO - Complexe Guy Favreau	445
Notebook	**54**
NRC - Wireless LAN	5
QRO - Complexe Guy Favreau	49
Ottawa	**2586**
Desktop	**1868**
Iqaluit - 933 Mivvik - 2nd Floor	15
Iqaluit - 933 Mivvik - 3rd Floor	6
NCR - 160 Elgin	178
NCR - 180 Elgin	18
NCR - 222 Queen Street	2
NCR - 301 Elgin Street	68
NCR - 473 Albert - Trebla	38
NCR - 50 O'Connor Street	37
NCR - 99 Bank Street	66
NCR - BOC	6
NCR - Constitution Sq.	134
NCR - EMB	371
NCR - Jean Edmonds	23
NCR - SAT	718
NCR - URB	188
Notebook	**718**
Iqaluit - 933 Mivvik - 2nd Floor	7
NCR - 160 Elgin	34
NCR - 180 Elgin	2
NCR - 222 Queen Street	13
NCR - 301 Elgin Street	8
NCR - 473 Albert - Trebla	7
NCR - 50 O'Connor Street	45
NCR - 99 Bank Street	47
NCR - BOC	8
NCR - Constitution Sq.	36
NCR - EMB	128
NCR - Jean Edmonds	8
NCR - SAT	137

4. Workstations by Location

	Count of Desktop / Laptop
NCR - Trebla	1
NCR - URB	21
NRC - Wireless LAN	215
Yellowknife - Joe Tobie Bldg	1
Saskatoon	**177**
Desktop	**143**
Saskatoon - 22nd Street East	143
Notebook	**34**
NRC - Wireless LAN	3
Saskatoon - 22nd Street East	22
Saskatoon - Princeton Tower - 2nd Avenue South	9
Toronto	**816**
Desktop	**716**
ORO - 130 King Street	530
ORO - Brampton	21
ORO - Exchange Tower 130 King Street	118
ORO - Kitchener	6
ORO - London	8
ORO - New Market	2
ORO - Queen Street	20
ORO - Watline Road	11
Notebook	**100**
NRC - Wireless LAN	4
ORO - 130 King Street	55
ORO - Brampton	6
ORO - Exchange Tower 130 King Street	23
ORO - Kitchener	2
ORO - London	2
ORO - New Market	1
ORO - Queen Street	3
ORO - Watline Road	4
Vancouver	**621**
Desktop	**540**
Vancouver - 211 Columbia Street	18
Vancouver - 222 Main St	16
Vancouver - 666 Burrard	62
Vancouver - 800 Burrard	16
Vancouver - 840 Howe St	398
Vancouver - 900 Howe St	30
Notebook	**81**
NCR - URB	1
NRC - Wireless LAN	7
Vancouver - 211 Columbia Street	1
Vancouver - 666 Burrard	15
Vancouver - 800 Burrard	2
Vancouver - 840 Howe St	55
Whitehorse	**54**
Desktop	**50**
Whitehorse	11
Whitehorse - Elijah Smith Building - 300 Main Street	39
Notebook	**4**
Whitehorse	2
Whitehorse - Elijah Smith Building - 300 Main Street	2
Winnipeg	**169**
Desktop	**137**
Winnipeg - Centennial House	94
Winnipeg - Donald Street	43
Notebook	**32**
Edmonton - EPCOR	1
NRC - Wireless LAN	2
Winnipeg - Centennial House	19
Winnipeg - Donald Street	10
Yellowknife	**88**
Desktop	**83**
Yellowknife - Joe Tobie Bldg	83
Notebook	**5**
NRC - Wireless LAN	1

4. Workstations by Location

	Count of Desktop / Laptop
Yellowknife - Joe Tobie Bldg	2
Yellowknife - Nova Plaza - 52nd Street	2
Grand Total	**5733**

Region/région	Network Printers
NCR/Région de la capitale nationale	391
Calgary	20
Edmonton	136
Halifax	28
Iqaluit	8
Montreal	272
Saskatoon	41
Toronto	110
Vancouver	111
Whitehorse	12
Winnipeg	37
Yellowknife	9
Total Network Printers/ total des imprimantes réseau	**1175**

Printer Type	Count	Ratio	Total
Network Printers	391	1 to 1	391
Desktop Printers	256	1 to 5	51
Label Printers	989	1 to 7.5	132
Classified	44	1 to 1	44

Note that all of the Kyocera are new MFD printers (2 years old max).

Location	Printer Make/Model	Quantity
222 Queen	Kyocera TASKalfa 4550ci KX	1
301 Elgin - 205A	Lexmark T644	1
301 Elgin - 215	HP LJ5550	1
	HP M5035 MFP	1
301 Elgin - 307	Lexmark T644	1
301 Elgin - 339	HP M5035 MFP	1
301 Elgin - 350	HP LaserJet 5550	1
50 O'Connor	Canon iR-ADV 6075	1
	Lexmark T654	1
50 O'Connor	Canon iR-ADV 6075	1
50 O'Connor - 518	Kyocera TASKalfa 4500i KX	1
50 O'Connor - 521	Kyocera TASKalfa 4550ci KX	1
50 O'Connor - 537	Kyocera TASKalfa 4500i KX	1
50 O'Connor - 544A	Kyocera TASKalfa 4500i KX	1
50 O'Connor - 547	Kyocera TASKalfa 4500i KX	1
50 O'Connor - 565	Kyocera TASKalfa 4500i KX	1
50 O'Connor - 572B	Kyocera TASKalfa 4500i KX	1
50 O'Connor - 573	Canon iR-ADV 6065	1
	Canon iR-ADV 6075	2
50 O'Connor - 585	Kyocera TASKalfa 4500i KX	2
50 O'Connor - 605	Kyocera TASKalfa 4550ci KX	1
50 O'Connor - 607	Kyocera TASKalfa 4550ci KX	1
50 O'Connor - 615	Kyocera TASKalfa 4500i KX	1
50 O'Connor - 621	Kyocera TASKalfa 4550ci KX	1
50 O'Connor - 628	HP Colour LaserJet CM4540 MFP	1
50 O'Connor - 632	HP Colour LaserJet CM4540	1
99 Bank	Kyocera TASKalfa 4500i KX	1
99 Bank - 1003	Kyocera TASKalfa 4500i KX	1
99 Bank - 1006F	Kyocera TASKalfa 4550ci KX	1
99 Bank - 1014	Kyocera TASKalfa 4550ci KX	1
99 Bank - 1112	Kyocera TASKalfa 4500i KX	1
99 Bank - 1125B	Kyocera TASKalfa 4500i KX	1
99 Bank - 1145B	Kyocera TASKalfa 4550ci KX	1
99 Bank - 1145E	HP LaserJet 4250	1
99 Bank - 1145H	Kyocera TASKalfa 4500i KX	1
99 Bank - 1170	Kyocera TASKalfa 4550ci KX	1
99 Bank - 1177I	Kyocera TASKalfa 4500i KX	1
99 Bank - 1195C	Kyocera TASKalfa 4550ci KX	1
BAR 718	HP Colour LaserJet 5550	1
CSC 1402	HP LaserJet 4250	1
CSC 1413	Konica Minolta bizhub C452	1
CSC 1429	Kyocera TASKalfa 4500i KX	1
CSC 1442	Konica Minolta bizhub C452	1
CSC 1456	Kyocera TASKalfa 4550ci KX	1
CSC 1472	Kyocera TASKalfa 4550ci KX	1
CSC 1480	Xerox WorkCentre 7665	1
CSC 334	Kyocera TASKalfa 4550ci KX	1
CSC 355	Kyocera TASKalfa 4500i KX	1
CSC 361	Kyocera TASKalfa 4550ci KX	1
CSC 399	HP LaserJet M5035 MFP Series	1
	Lexmark C782	1
CSC 800-09	Kyocera TASKalfa 4550ci KX	1
CSC 800-3	Canon iR-ADV C5045	1
CSC 9??	HP LaserJet 4250	1
CSC 910	Lexmark T644	1
CSC 919	Kyocera TASKalfa 4550ci KX	1
CSC 933	Kyocera TASKalfa 4500i KX	1
CSC 947	Canon iR5050	1
CSC 949	Lexmark T654	1
CSC 954	Kyocera TASKalfa 4550ci KX	1
CSC 967	Kyocera TASKalfa 4500i KX	1
CSC 981	HP LaserJet M5035 MFP	1
CSC 986	Konica Minolta bizhub 501	1
EMB 1005	HP LaserJet 4250	1

EMB 1009	Samsung ML-4550	1
EMB 1022	Kyocera TASKalfa 4550ci KX	1
EMB 1040	Samsung ML-4550	1
EMB 1070	Konica Minolta bizhub C452	1
EMB 1089	Samsung ML-4550	1
EMB 1092	Kyocera TASKalfa 4500i KX	1
EMB 1113	Kyocera TASKalfa 4550ci KX	1
EMB 1211	Kyocera TASKalfa 4500i KX	1
EMB 1243	Kyocera TASKalfa 4550ci KX	1
EMB 1277	Kyocera TASKalfa 4500i KX	1
EMB 1291	Lexmark T644	1
EMB 1309	Kyocera TASKalfa 4500i KX	1
	Kyocera TASKalfa 4550ci KX	1
EMB 1376	Kyocera TASKalfa 4550ci KX	1
EMB 1387	HP Colour LaserJet CP4525	1
EMB 2016	Kyocera TASKalfa 4500i KX	1
EMB 2049	Kyocera TASKalfa 4550ci KX	1
EMB 2072	Kyocera TASKalfa 4500i KX	1
EMB 2103	Kyocera TASKalfa 4550ci KX	1
EMB 2135	Ricoh Aficio MP 8001	1
EMB 2143	HP LaserJet M5035 MFP	1
EMB 2167	HP LaserJet 4050	1
EMB 2178	Kyocera TASKalfa 4500i KX	1
EMB 3015	Lexmark T654	1
EMB 3021	Kyocera TASKalfa 4550ci KX	1
EMB 3055	Kyocera TASKalfa 4500i KX	1
EMB 3060	Kyocera TASKalfa 4550ci KX	1
EMB 3101	Xerox WorkCentre 7665	1
EMB 3123	Lexmark T644	1
EMB 3143	Kyocera TASKalfa 4500i KX	1
EMB 3179	Kyocera TASKalfa 4550ci KX	1
EMB 3198	Kyocera TASKalfa 4500i KX	1
EMB 3258	Kyocera TASKalfa 4500i KX	1
EMB 3283	Kyocera TASKalfa 4550ci KX	1
EMB 3306	Kyocera TASKalfa 4500i KX	1
EMB 3331	Kyocera TASKalfa 4550ci KX	1
EMB 4014 MO	Lexmark T654	1
EMB 4032 MO	Lexmark T654	1
EMB 4036	Canon iR3245	1
EMB 4040 MO	HP Colour LaserJet 4600	1
EMB 4046 MO	HP LaserJet 4250	1
EMB 4053 MO	HP Colour LaserJet 4700	1
EMB 4056	Kyocera TASKalfa 4500i KX	1
EMB 4061 MO	HP LaserJet 4250	1
EMB 4080	Konica Minolta bizhub C452	1
EMB 4093	Kyocera TASKalfa 4500i KX	1
EMB 4117	HP LaserJet 4250	1
EMB 4143	Kyocera TASKalfa 4550ci KX	1
EMB 4165	Kyocera FS-3540MFP	1
EMB 4177	Kyocera TASKalfa 4550ci KX	1
EMB 4200	Kyocera TASKalfa 4550ci KX	1
EMB 4222	Canon IR 5065	1
EMB 4248	Kyocera TASKalfa 4550ci KX	1
EMB 4282 MO	HP LaserJet 4250	1
EMB 4291	Kyocera TASKalfa 4550ci KX	1
EMB 4329	HP LaserJet 4250	1
EMB 4330	Kyocera TASKalfa 4500i KX	1
EMB 4343A	Lexmark T644	1
EMB 4347	Lexmark T644	1
EMB 4371	HP LaserJet 4250	1
EMB 5017	Kyocera TASKalfa 4500i KX	1
EMB 5055	Kyocera TASKalfa 4500i KX	1
EMB 5078	Kyocera TASKalfa 4500i KX	1
EMB 5107	Kyocera TASKalfa 4500i KX	1
EMB 5135 Printer on Left	Xerox WorkCentre 7556	1
EMB 5135 Printer on Right	Xerox WorkCentre 7556	1
EMB 5163	Lexmark T644	1
EMB 5171	HP Colour LaserJet 4650	1

EMB 5181	Kyocera TASKalfa 4500i KX	1
EMB 5200	Kyocera TASKalfa 4550ci KX	1
EMB 5220	Kyocera TASKalfa 4550ci KX	1
EMB 5258	Kyocera TASKalfa 4550ci KX	1
EMB 5263	Samsung ML-4550	1
EMB 5283	Kyocera TASKalfa 4550ci KX	1
EMB 5307	Kyocera TASKalfa 4500i KX	1
EMB 5363 Printer on Left	Xerox WorkCentre 7556	1
EMB 5363 Printer on Right	Xerox WorkCentre 7556	1
EMB 6	HP Colour LaserJet 4700	1
EMB 6044	Kyocera TASKalfa 4500i KX	1
EMB 6088	Kyocera TASKalfa 4550ci KX	1
EMB 6135	Xerox WorkCentre 7556	1
EMB 6159	Xerox WorkCentre 7556	1
EMB 6194	Kyocera TASKalfa 4550ci KX	1
EMB 6250	Kyocera TASKalfa 4500i KX	1
EMB 6283	Kyocera TASKalfa 4550ci KX	1
EMB 6314	Kyocera TASKalfa 4500i KX	1
EMB 6335	Kyocera TASKalfa 4500i KX	1
EMB 6355	Xerox WorkCenter 7556	1
EMB 6355 Left Device	Xerox WorkCentre 7556	1
EMB 6363	Samsung ML-4550	1
EMB A	HP Colour LaserJet 4650	1
EMB A 062	HP Colour LaserJet 4700	1
EMB A 070	Kyocera TASKalfa 4550ci KX	1
EMB A 194	Lexmark T644	1
EMB A 216	Canon IR 6075	1
EMB A 224	Kyocera TASKalfa 4500i KX	1
EMB A 345	HP LaserJet 4250	1
EMB A 358	Kyocera TASKalfa 4550ci KX	1
EMB AA 125	Lexmark T644	1
EMB AA 2055	Samsung ML-4550	1
EMB AA 230	HP LaserJet M5035 MFP	1
EMB AA 238	Samsung ML-4550	1
EMB AA 528	Lexmark T644	1
EMB AA 564	HP Colour LaserJet 4700	1
EMB Library	Canon iR-ADV C5045	1
JE 1584	HP LaserJet 4250	1
JE C1556	Kyocera TASKalfa 4500i KX	1
JE C1571	Kyocera TASKalfa 4550ci KX	1
JE D1579	HP LaserJet 4250	1
Place Bell - 1204	HP 4700DN	1
	Lexmark T654DN	1
Place Bell - 1205C	HP 4250DN	1
	Lexmark T644	1
Place Bell - 12103	HP DesignJet T1100ps	1
Place Bell - 1215D	HP Laserjet 5550dn	1
Place Bell - 1217B	HP 4250dtn	1
	HP 5550DN	1
Place Bell - 1226D	Lexmark T644	1
Place Bell - 1227D	Lexmark C782	1
Place Bell - 1230G	HP 4200dtn	1
	Lexmark C748	1
Place Bell - 1244B	HP CP5525	1
	T654dn	1
Place Bell - 1264D	Lexmark C736dn	1
	Lexmark MS810dtn	2
Place Bell - 1266G	HP 4250	1
	HP 4700	1
Place Bell - 1273D	HP 4250dtn	1
Place Bell - 1277B	HP 4250dtn	1
	Lexmark T644	1
Place Bell - 1286G	HP 5550DN	1
	HP M5035 MFP	1
Place Bell - 1402D	Lexmark C748de	1
	Lexmark T654DN	1
Place Bell - 1418E	Lexmark E460dn	1
Place Bell - 1432F	Samsung ML-4551ND	1

Place Bell - 1456E	HP 8150dn	1
	Lexmark C736dn	1
Place Bell - 1462C	Lexmark T644	1
Place Bell - 1475D	HP 4200dtn	1
Place Bell - 1487E	Lexmark MS811dn	1
Place Bell - 1496F	Lexmark X748	1
Queen 1137	HP LaserJet 4250	1
Queen 1139	HP Colour LaserJet CM4540 MFP	1
SAT 10001	Kyocera TASKalfa 4550ci KX	1
SAT 10005	Kyocera TASKalfa 4500i KX	1
SAT 10007	HP LaserJet 4250	1
SAT 10045	Konica Minolta bizhub C452	1
SAT 10051	HP LaserJet M5035 MFP PCL 6	1
SAT 10052	Kyocera TASKalfa 4550ci KX	1
SAT 10066	Kyocera TASKalfa 4500i KX	1
SAT 10071	Canon iR5050	1
SAT 11007	Kyocera TASKalfa 4550ci KX	1
SAT 11008	Kyocera TASKalfa 4500i KX	1
SAT 11042	Kyocera FS-3540MFP	1
SAT 11050	Kyocera TASKalfa 4500i	1
SAT 11090	Kyocera TASKalfa 4500i KX	1
SAT 12002	HP DesignJet 500PS	1
SAT 12005	Kyocera TASKalfa 4500i KX	1
SAT 12026	HP LaserJet 4250	1
SAT 12036	HP LaserJet 4250	1
SAT 12037	Kyocera TASKalfa 4550ci KX	1
SAT 2???	Xerox WorkCentre 7665	1
SAT 2002	HP Colour LaserJet 4700	1
SAT 2015	KONICA MINOLTA C652	1
SAT 2049A	Kyocera TASKalfa 4500i KX	1
SAT 2106	HP DesignJet 800PS	1
	Xerox Workcenter 7665	1
SAT 2121A	Kyocera TASKalfa 4550ci KX	1
SAT 3002	HP LaserJet M5035 MFP PCL 6	1
SAT 3005	HP LaserJet 4250	1
SAT 3034	Kyocera TASKalfa 4550ci KX	1
SAT 3084	Kyocera TASKalfa 4500i KX	1
SAT 3089	HP LaserJet 4250	1
SAT 3131	Kyocera TASKalfa 4500i KX	1
SAT 3147	Kyocera TASKalfa 4500i KX	1
SAT 3159	KONICA MINOLTA 501	1
	Konica Minolta bizhub C452	1
	Kyocera TASKalfa 4500i KX	1
SAT 4011	HP LaserJet 4250	1
	Lexmark T644	1
SAT 4014	Kyocera TASKalfa 4550ci KX	1
SAT 4064	Lexmark T644	1
SAT 4066	Kyocera TASKalfa 4500i KX	1
SAT 4085	Lexmark Universal XL	1
SAT 4135	Kyocera TASKalfa 4550ci KX	1
SAT 4163	HP LaserJet M5035 MFP	1
	Kyocera TASKalfa 4500i KX	1
SAT 5007	Kyocera TASKalfa 4550ci KX	1
SAT 5009	Canon iR-ADV C5045	1
SAT 5016	Kyocera TASKalfa 4500i KX	1
SAT 5031	Lexmark T654	1
SAT 5032	Samsung ML-4551 ND	1
SAT 5033	Lexmark T644	1
SAT 5060	Kyocera TASKalfa 4550ci KX	1
SAT 5102	Samsung ML-4550	1
SAT 5105	HP LaserJet 4700	1
SAT 5108	HP Colour LaserJet 4650	1
	HP LaserJet 4100	1
SAT 5112	HP LaserJet 4250	1
SAT 5114	HP Laser Jet 4250	1
SAT 5203	HP Colour LaserJet CM4540 MFP	1
SAT 5209	Lexmark T644	1
SAT 6003	HP Colour LaserJet CM4540 MFP	1

SAT 6007	Kyocera TASKalfa 4500i KX	1
SAT 6019	Kyocera TASKalfa 4500i KX	1
SAT 6033	Kyocera TASKalfa 4500i KX	1
SAT 6042	HP Colour LaserJet CM4540 MFP	1
SAT 6047	HP LaserJet 4250	1
SAT 6056	Kyocera TASKalfa 4500i KX	1
SAT 6058	Kyocera TASKalfa 4500i KX	1
SAT 6076	Xerox WorkCentre 7665	2
SAT 7007	Kyocera TASKalfa 4500i KX	1
SAT 7036	Kyocera TASKalfa 4500i KX	1
SAT 7047	HP LaserJet 4250	1
SAT 7069	Kyocera TASKalfa 4550ci KX	1
SAT 7097	Kyocera TASKalfa 4500i KX	1
SAT 7104	Kyocera TASKalfa 4550ci KX	1
SAT 8002	Kyocera TASKalfa 4550ci KX	1
SAT 8006	HP LaserJet 4250	1
SAT 8020	HP LaserJet 9050	1
SAT 8044	Kyocera TASKalfa 4500i KX	1
SAT 8049	Kyocera TASKalfa 4500i KX	1
SAT 8050	Kyocera TASKalfa 4500i KX	1
SAT 8060	Kyocera TASKalfa 4550ci KX	1
SAT 8073	Kyocera TASKalfa 4550ci KX	1
SAT 8121	Kyocera TASKalfa 4550ci KX	1
SAT 8175	HP LaserJet M5035 MFP	1
SAT 8183	Lexmark T644	1
SAT 9006	Kyocera TASKalfa 4500i KX	1
SAT 9019	Kyocera TASKalfa 4550ci KX	1
SAT 9027	Xerox WorkCentre 7428	1
SAT 9036	Kyocera TASKalfa 4550ci KX	1
SAT 9038	HP Colour LaserJet 4700	1
SAT 9041	HP LaserJet 4250	1
SAT 9047	Xerox WorkCentre 7556	1
SAT 9049	Kyocera TASKalfa 4550ci KX	1
SAT 9069	Kyocera TASKalfa 4550ci KX	1
SAT B149	HP LaserJet M5035 MFP	1
SAT B153	HP LaserJet M2727	1
TREBLA 3-25	Kyocera TASKalfa 4500i KX	1
TREBLA 3-29	Kyocera TASKalfa 4550ci KX	1
TREBLA 3-58	Konica Minolta bizhub C452	1
TREBLA 3-72	Kyocera TASKalfa 4500i KX	1
TREBLA 3rd floor - Copy room	HP LaserJet M5035 MFP	1
	Kyocera TASKalfa 4500i KX	1
URB 239	HP LaserJet 4100	1
URB 207	HP LaserJet 5Si	1
URB 208	Ricoh Aficio MP 3351	1
URB 210	Lexmark T654	1
URB 228	HP LaserJet 4100	1
URB 236 (Training Room)	Samsung ML-4550	1
URB 308	Kyocera TASKalfa 4500i KX	1
URB 327	Lexmark T644	1
URB 327B	Kyocera TASKalfa 4500i KX	1
URB 329	HP DesignJet 500	1
URB 333	Kyocera TASKalfa 4550ci KX	1
URB 356	HP Colour LaserJet 4650	1
	Kyocera TASKalfa 4550ci KX	1
URB 408	Kyocera TASKalfa 4550ci KX	1
URB 414	Kyocera TASKalfa 4500i KX	1
URB 436	Canon iR-ADV 8095	1
URB 445	HP LaserJet M5035 MFP	1
URB 455	Kyocera TASKalfa 4550ci KX	1
URB 5	HP LaserJet 4250	1
URB 510	Kyocera TASKalfa 4550ci KX	1
URB 521	HP LaserJet M5035 MFP	1
	Konica Minolta bizhub C452	1
URB 538	Kyocera TASKalfa 4550ci KX	1
URB 545	Kyocera TASKalfa 4550ci KX	1
URB 548	HP LaserJet 4250	1
URB 549	Lexmark T644	1

URB 614	Kyocera TASKalfa 4550ci KX	1
URB 621	Konica Minolta bizhub C452	1
URB 629	Kyocera TASKalfa 4550ci KX	1
URB 635	HP LaserJet 4250	1
URB 637	HP LaserJet 4250	1
URB 648	Kyocera TASKalfa 4550ci KX	1
URB 713B	HP LaserJet M5035 MFP	1
URB 719	Xerox WorkCentre 7775	1
URB 734	HP LaserJet M5035 MFP	1
URB 753	Lexmark X658de	1
Grand Total		350

SCCM 2012 infrastructure
- Parent Site (national)
- 13 regional distribution points
- SCCM is leveraged for desktop software distribution, automated desktop operating system deployment, desktop software update deployment, desktop hardware/software inventorying.

Call Volume by Service for DOJ

Start Date: **2013-08-01**
End Date: **2013-10-15**

Summary at Application Level

Summary	Calls Offered	Calls Abandoned	Calls Handled	Calls Disconnected	Calls Routed
	4984	47	4937	0	22
		0.94%	99.06%		

Hnd Thres 94.5% / 120 s	<= 0 s	<= 15 s	<= 20 s	<= 30 s	<= 36 s	<= 45 s	<= 50 s	<= 60 s	<= 80 s	<= 90 s	<= 120 s	<= 180 s	<= 300 s	<= 600 s
	0	4560	4566	4584	4597	4612	4627	4635	4667	4681	4721	4771	4829	4848
	0.00%	92.40%	92.50%	92.80%	93.10%	93.40%	93.70%	93.90%	94.50%	94.80%	95.60%	96.60%	97.80%	98.20%

Abd Thres 0.0% / 120 s	> 0 s	> 15 s	> 20 s	> 30 s	> 36 s	> 45 s	> 50 s	> 60 s	> 80 s	> 90 s	> 120 s	> 180 s	> 300 s	> 600 s
	47	39	37	35	33	32	31	30	28	26	**18**	8	5	1
	0.90%	0.80%	0.70%	0.70%	0.70%	0.60%	0.60%	0.60%	0.60%	0.50%	**0.40%**	0.20%	0.10%	0.00%

Details at Skillset Level

SvcArea	Service	Calls Hnd	Calls Hnd < Thres	% Calls Hnd < Thres	Hnd Avg Wait	Hnd Long Wait	Short Calls Hnd	Avg Talk Time	Avg Not Rdy Time	Calls Abd (Skset)	Calls Abd >= Thres (Skset)	Vol Pct
DOJ	DOJ_APPS	271	265	97.79%	7.3	362	5	372.07	132	2	0.73%	5.49%
DOJ	DOJ_APPS_FR	134	134	100.00%	2.4	107	1	385.25	148.29	2	0.74%	2.71%
DOJ	DOJ_EMAIL	612	595	97.22%	10.2	441	5	351.17	128.41	7	0.32%	12.40%
DOJ	DOJ_EMAIL_FR	210	204	97.14%	10.4	395	0	401.76	145.93	1	0.47%	4.25%
DOJ	DOJ_MSOFFICE	275	269	97.82%	8.8	332	2	393.63	154.58	2	0.00%	5.57%
DOJ	DOJ_MSOFFICE_FR	125	124	99.20%	4.1	131	0	444.9	166.32	0	0.00%	2.53%
DOJ	DOJ_OTHER_PWD	173	169	97.69%	7	253	1	330.45	121.09	1	0.00%	3.50%
DOJ	DOJ_OTHER_PWD_FR	46	44	95.65%	11.2	241	0	303.93	136.41	0	0.00%	0.93%
DOJ	DOJ_PASSWORD	605	581	96.03%	11.5	515	2	284.49	104.85	7	0.65%	12.25%
DOJ	DOJ_PASSWORD_FR	219	212	96.80%	8.7	276	0	284.36	105.64	4	0.90%	4.44%
DOJ	DOJ_REQUEST	1061	1036	97.64%	7.4	413	3	344.58	128.7	10	0.28%	21.49%
DOJ	DOJ_REQUEST_FR	256	250	97.66%	6.8	329	0	352.78	129.86	2	0.39%	5.19%
DOJ	DOJ_WORKSTN	646	630	97.52%	8.6	466	4	308.24	133.23	7	0.31%	13.08%
DOJ	DOJ_WORKSTN_FR	304	296	97.37%	7.9	251	3	289.89	121.54	1	0.00%	6.16%
	Total for DOJ	**4937**	**4809**	**97.41%**	**8.5**	**515**	**26**	**337.11**	**128.58**	**46**	**0.36%**	**100.00%**
	Total	**4937**	**4809**	**97.41%**	**8.5**	**515**	**26**	**337.11**	**128.58**	**46**	**0.36%**	**100.00%**

Call Volume by Interval for DOJ

Start Date: **2013-08-01**
End Date: **2013-10-15**

Timestamp	Calls Offered	Calls Handled	Calls Abandoned	Calls Handled > Thres	Perc Abandoned	Perc Less LCT
0:00:00	0	0	0	0	0.00%	0.00%
0:15:00	0	0	0	0	0.00%	0.00%
0:30:00	0	0	0	0	0.00%	0.00%
0:45:00	0	0	0	0	0.00%	0.00%
1:00:00	0	0	0	0	0.00%	0.00%
1:15:00	0	0	0	0	0.00%	0.00%
1:30:00	0	0	0	0	0.00%	0.00%
1:45:00	0	0	0	0	0.00%	0.00%
2:00:00	0	0	0	0	0.00%	0.00%
2:15:00	0	0	0	0	0.00%	0.00%
2:30:00	0	0	0	0	0.00%	0.00%
2:45:00	0	0	0	0	0.00%	0.00%
3:00:00	0	0	0	0	0.00%	0.00%
3:15:00	0	0	0	0	0.00%	0.00%
3:30:00	0	0	0	0	0.00%	0.00%
3:45:00	0	0	0	0	0.00%	0.00%
4:00:00	0	0	0	0	0.00%	0.00%
4:15:00	0	0	0	0	0.00%	0.00%
4:30:00	0	0	0	0	0.00%	0.00%
4:45:00	0	0	0	0	0.00%	0.00%
5:00:00	0	0	0	0	0.00%	0.00%
5:15:00	0	0	0	0	0.00%	0.00%
5:30:00	0	0	0	0	0.00%	0.00%
5:45:00	0	0	0	0	0.00%	0.00%
6:00:00	0	0	0	0	0.00%	0.00%
6:15:00	0	0	0	0	0.00%	0.00%
6:30:00	3	3	0	0	0.00%	100.00%
6:45:00	9	8	1	0	11.11%	100.00%
7:00:00	27	26	1	4	3.70%	84.62%
7:15:00	24	22	2	3	8.33%	86.36%
7:30:00	42	42	0	0	0.00%	100.00%
7:45:00	47	47	0	0	0.00%	100.00%
8:00:00	81	81	0	3	0.00%	96.30%
8:15:00	97	97	0	4	0.00%	95.88%
8:30:00	148	147	1	1	0.68%	99.32%
8:45:00	143	143	0	3	0.00%	97.90%
9:00:00	194	193	1	6	0.52%	96.89%
9:15:00	215	212	3	8	1.40%	96.23%
9:30:00	208	205	3	10	1.44%	95.12%
9:45:00	178	177	1	13	0.56%	92.66%
10:00:00	146	145	1	0	0.68%	100.00%
10:15:00	177	176	1	2	0.56%	98.86%
10:30:00	167	167	0	2	0.00%	98.80%
10:45:00	161	161	0	0	0.00%	100.00%
11:00:00	136	135	1	2	0.74%	98.52%
11:15:00	146	146	0	1	0.00%	99.32%
11:30:00	137	135	2	1	1.46%	99.26%
11:45:00	134	134	0	1	0.00%	99.25%
12:00:00	106	104	2	3	1.89%	97.12%
12:15:00	104	103	1	3	0.96%	97.09%

Call Volume by Interval for DOJ

Start Date: **2013-08-01**
End Date: **2013-10-15**

Timestamp	Calls Offered	Calls Handled	Calls Abandoned	Calls Handled > Thres	Perc Abandoned	Perc Less LCT
12:30:00	81	80	1	0	1.23%	100.00%
12:45:00	99	98	1	3	1.01%	96.94%
13:00:00	110	109	1	1	0.91%	99.08%
13:15:00	146	146	0	1	0.00%	99.32%
13:30:00	131	126	5	5	3.82%	96.03%
13:45:00	133	133	0	7	0.00%	94.74%
14:00:00	115	112	3	3	2.61%	97.32%
14:15:00	119	118	1	3	0.84%	97.46%
14:30:00	115	115	0	3	0.00%	97.39%
14:45:00	149	146	3	4	2.01%	97.26%
15:00:00	117	116	1	3	0.85%	97.41%
15:15:00	118	117	1	6	0.85%	94.87%
15:30:00	98	98	0	2	0.00%	97.96%
15:45:00	89	88	1	0	1.12%	100.00%
16:00:00	89	88	1	6	1.12%	93.18%
16:15:00	62	62	0	1	0.00%	98.39%
16:30:00	56	56	0	0	0.00%	100.00%
16:45:00	44	44	0	0	0.00%	100.00%
17:00:00	29	29	0	1	0.00%	96.55%
17:15:00	37	37	0	1	0.00%	97.30%
17:30:00	14	14	0	0	0.00%	100.00%
17:45:00	21	21	0	0	0.00%	100.00%
18:00:00	19	19	0	2	0.00%	89.47%
18:15:00	12	12	0	1	0.00%	91.67%
18:30:00	15	15	0	1	0.00%	93.33%
18:45:00	5	4	1	0	20.00%	100.00%
19:00:00	14	14	0	0	0.00%	100.00%
19:15:00	5	5	0	1	0.00%	80.00%
19:30:00	8	5	3	1	37.50%	80.00%
19:45:00	8	6	2	1	25.00%	83.33%
20:00:00	3	3	0	0	0.00%	100.00%
20:15:00	5	4	1	1	20.00%	75.00%
20:30:00	2	2	0	0	0.00%	100.00%
20:45:00	3	3	0	0	0.00%	100.00%
21:00:00	0	0	0	0	0.00%	0.00%
21:15:00	0	0	0	0	0.00%	0.00%
21:30:00	0	0	0	0	0.00%	0.00%
21:45:00	0	0	0	0	0.00%	0.00%
22:00:00	0	0	0	0	0.00%	0.00%
22:15:00	0	0	0	0	0.00%	0.00%
22:30:00	0	0	0	0	0.00%	0.00%
22:45:00	0	0	0	0	0.00%	0.00%
23:00:00	0	0	0	0	0.00%	0.00%
23:15:00	0	0	0	0	0.00%	0.00%
23:30:00	0	0	0	0	0.00%	0.00%
23:45:00	0	0	0	0	0.00%	0.00%

Number of Calls by Reported Source	
Reported Source	**Count of Contacts (12 month period)**
Direct Input	8
Email	12601
Mobility	20
Other	5
Phone	20459
Systems Management	890
Voice Mail	202
Walk In	3
Grand Total	**34188**

Number of Calls by Product	
Product	**Count of Contacts (12 month period)**
BIOS	1
Building	4
Enterprise	937
In-House Application	6430
Office	193
Peripheral	3315
Request	242
Telecom	8
Third-party software	21112
Workstation	1033
Grand Total	**33275**

Incidents by Regions and Level

Note: The data is accurate within + or - 1 incidents

Incident only	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13
B.C. Region	169	322	270	237	303	229	302	326	387	213	274	205	262
Resolved Help Centre 1ST Level	69	94	129	94	151	116	101	126	133	72	132	69	105
	41%	29%	48%	40%	50%	51%	33%	39%	34%	34%	48%	34%	40%
Escalated 2nd Level	81	201	110	119	121	89	174	175	224	118	114	116	131
	48%	62%	41%	50%	40%	39%	58%	54%	58%	55%	42%	57%	50%
Escalated Other Groups	19	27	31	24	31	24	27	25	30	23	28	20	26
	11%	8%	11%	10%	10%	10%	9%	8%	8%	11%	10%	10%	10%
NCR	1107	1235	1268	971	1273	1264	1433	1597	1296	1198	1336	1065	1292
Resolved Help Centre 1ST Level	454	451	625	463	742	567	627	721	563	616	595	492	570
	41%	37%	49%	48%	58%	45%	44%	45%	43%	51%	45%	46%	44%
Escalated 2nd Level	494	617	506	399	410	548	618	711	551	455	604	476	597
	45%	50%	40%	41%	32%	43%	43%	45%	43%	38%	45%	45%	46%
Escalated Other Groups	159	167	137	109	121	149	188	165	182	127	137	97	125
	14%	14%	11%	11%	10%	12%	13%	10%	14%	11%	10%	9%	10%
Northern regions	38	18	22	16	36	26	19	69	29	30	33	21	27
Resolved Help Centre 1ST Level	9	4	5	5	21	13	5	13	11	13	14	10	9
	24%	22%	23%	31%	58%	50%	26%	19%	38%	43%	42%	48%	33%
Escalated 2nd Level	13	7	2	4	3	1	6	34	10	11	10	6	12
	34%	39%	9%	25%	8%	4%	32%	49%	34%	37%	30%	29%	44%
Escalated Other Groups	16	7	15	7	12	12	8	22	8	6	9	5	6
	42%	39%	68%	44%	33%	46%	42%	32%	28%	20%	27%	24%	22%
Ontario Region	64	47	58	52	248	81	239	594	450	384	389	22	319
Resolved Help Centre 1ST Level	29	18	21	28	54	50	200	241	231	192	207	123	147
	45%	38%	36%	54%	22%	62%	84%	41%	51%	50%	53%	559%	46%
Escalated 2nd Level	6	4	3	2	173	4	8	315	190	156	157	85	150
	9%	9%	5%	4%	70%	5%	3%	53%	42%	41%	40%	386%	47%
Escalated Other Groups	29	25	34	22	21	27	31	38	29	36	25	18	22
	45%	53%	59%	42%	8%	33%	13%	6%	6%	9%	6%	82%	7%
Prairie Region	328	367	323	241	301	345	396	388	368	322	407	240	309
Resolved Help Centre 1ST Level	76	107	104	72	118	152	142	158	118	119	116	91	89
	23%	29%	32%	30%	39%	44%	36%	41%	32%	37%	29%	38%	29%
Escalated 2nd Level	212	232	171	129	153	161	222	189	219	160	225	114	187
	65%	63%	53%	54%	51%	47%	56%	49%	60%	50%	55%	48%	61%
Escalated Other Groups	40	28	48	40	30	32	32	41	31	43	66	35	33
	12%	8%	15%	17%	10%	9%	8%	11%	8%	13%	16%	15%	11%
Quebec Region	200	230	226	166	193	315	242	245	206	226	223	223	246
Resolved Help Centre 1ST Level	72	68	87	44	88	125	84	108	84	67	84	92	80
	36%	30%	38%	27%	46%	40%	35%	44%	41%	30%	38%	41%	33%
Escalated 2nd Level	105	136	115	107	82	165	139	117	100	131	113	116	148
	53%	59%	51%	64%	42%	52%	57%	48%	49%	58%	51%	52%	60%
Escalated Other Groups	23	26	24	15	23	25	19	20	22	28	26	15	18
	12%	11%	11%	9%	12%	8%	8%	8%	11%	12%	12%	7%	7%
Atlantic Region	16	15	18	21	23	20	22	143	127	133	129	92	121
Resolved Help Centre 1ST Level	2	2	5	4	7	8	8	72	47	37	45	41	29
	13%	13%	28%	19%	30%	40%	36%	50%	37%	28%	35%	45%	24%
Escalated 2nd Level	0	1	1	1	0	2	3	51	69	87	68	44	76
	0%	7%	6%	5%	0%	10%	14%	36%	54%	65%	53%	48%	63%
Escalated Other Groups	14	12	12	16	16	10	11	20	11	9	16	7	16
	88%	80%	67%	76%	70%	50%	50%	14%	9%	7%	12%	8%	13%
DLSU	229	242	314	327	287	295	344	319	252	215	275	238	289

Incidents by Regions and Level

Note: The data is accurate within + or - 1 incidents

Incident only	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13
Resolved Help Centre 1ST Level	123	122	220	208	177	193	217	181	145	122	161	136	151
	54%	50%	70%	64%	62%	65%	63%	57%	58%	57%	59%	57%	52%
Escalated 2nd Level	29	47	42	67	31	47	59	69	53	42	45	47	82
	13%	19%	13%	20%	11%	16%	17%	22%	21%	20%	16%	20%	28%
Escalated Other Groups	77	73	52	52	79	55	68	69	54	51	69	55	56
	34%	30%	17%	16%	28%	19%	20%	22%	21%	24%	25%	23%	19%
Total	2151	2476	2499	2031	2664	2575	2997	3681	3115	2721	3066	2310	2865
Resolved Help Centre 1ST Level	834	866	1196	918	1358	1224	1384	1620	1332	1238	1354	1054	1180
	39%	35%	48%	45%	51%	48%	46%	44%	43%	45%	44%	46%	41%
Escalated 2nd Level	940	1245	950	828	973	1017	1229	1661	1416	1160	1336	1004	1383
	44%	50%	38%	41%	37%	39%	41%	45%	45%	43%	44%	43%	48%
Escalated Other Groups	377	365	353	285	333	334	384	400	367	323	376	252	302
	18%	15%	14%	14%	13%	13%	13%	11%	12%	12%	12%	11%	11%

Incident History by Hardware and Software	
	Number of Incidents (12-month Period)
Hardware	**5268**
Adaptive Technology	**228**
Other Adaptive Technology Hardware	228
Bus Adapter	**7**
Other Bus Adapter	7
CD Drive	**14**
Other CD Drive	14
CD Writer	**5**
Other CD Writer	5
CMOS	**6**
Other CMOS	6
Desktop	**598**
GX270	1
GX280	3
Other Desktop Workstation	562
P4	32
Docking Station	**25**
Other Docking Station	25
DVD Drive	**29**
Other DVD Drive	29
DVD Writer	**7**
Other DVD Writer	7
Hard Drive	**31**
Other Hard Drive	31
Keyboard	**140**
Other Keyboard	140
KVM Switch	**1**
Other KVM Swtich	1
Laptop	**386**
4600	1
EVON610C	1
Other Laptop Workstation	381
S3	3
Memory	**121**
Bio Clip	50
Other Memory	27
Outbacker MXP	1
Stealth MXP	43
Monitor	**407**
Other Monitor	407
Mouse	**150**
Other Mouse	150
PDA	**49**
Blackberry	47
Other PDA Workstation	2
Port replicator	**3**
Other Port Replicator	3
Printer	**1996**
Braille Printer	1
Bubble Jet	3
Color Laser Jet	3
DeskJet	3
InkJet	2
Label	24
LabelWriter Duo	110
LaserPrinter	1441
MFP	1
Other Peripheral Printer	406
Plotter	2
Router	**18**
Other Peripheral Router	5
Other Telecom Router	8
WRT54G - wireless	5
Scanner	**108**
Flatbed	5
Other Scanner	103

Incident History by Hardware and Software	
	Number of Incidents (12-month Period)
UNIX	**1**
Other UNIX Server	1
Video Adapter	**27**
Other Video Adapter	27
Virtual	**312**
Other Virtual Server	312
Wintel	**599**
Other Wintel Server	50
PowerEdge	474
ProLiant DL360	15
ProLiant DL380	54
ProLiant DL580	1
ProLiant ML370	4
ProLiant ML570	1
Software	**27869**
Adaptive Technology	**3**
Other Third-party Adaptive Technology	3
Application support	**25**
Other Third-party Application Support	25
Backup	**322**
Other Enterprise Backup	322
Business Application	**3775**
Antidote Prisme	11
CCM Mercury Plus (Domus)	1
ccmMercury	2
EES (Estimate of Elective Service) from PWGSC	1
E-Forms	1
Entrust	360
Folio Views (LSB)	2
IFMSSAP	40
Individual Learning Plan (ILP)	6
Internet Site	3
Intranet Site	28
iRims	45
Java	252
JUSTIN	2
Litigation/Ringtail	35
Online Pay	1
Other In-House Business Application	3
Other Third-party Business Application	2565
PeopleSoft	303
PKI Certificate	1
RDIMS (EDMS)	60
RIMS	20
SAP	1
SAS	1
Secure Remote Access	1
Summation/Supertext	2
Thin Client	4
VDI	24
Database application	**3**
Other Third-party Database Application	1
SQL Server	2
Email	**4610**
Other Third-party Email	76
Outlook	4534
Internet Browser	**1024**
Internet Explorer	1008
Other Third-party Internet Browser	16
Malware Anti-virus protection	**2**
Other Enterprise Malware Anti-Virus Protection	2
Monitoring	**2**
Other Enterprise Monitoring	2
Network Application	**1794**
Citrix Program Neighborhood Client	65
Other Third-party Network Application	1729

12. Incidents by Product

Incident History by Hardware and Software	
	Number of Incidents (12-month Period)
Office application	**2235**
Access	5
Acrobat Reader	519
Acrobat Writer	21
CD Burner Software	7
Excel	207
Frontpage	1
Mailfrontier	311
McAfee Antivirus	92
Office Suite	46
Other Third-party Office Application	11
Outlook Web Access	279
Powerpoint	103
Publisher	1
Quickview	2
Scanner Software	4
SnagIt	1
Start Stop Universal Transcription System	1
Visio	4
Windows Media Player	15
Winzip	3
Word	602
Operating System	**7354**
Blackberry OS	1074
Other Third-party Operating System	10
Windows	126
Windows 2000	2
Windows 2003	2790
Windows XP	3352
Security Application	**449**
Antigen	2
Other Third-party Security Application	39
SecureDoc Hard Drive Encryption	401
SecureDocs	7
Systems Management	**1**
Systems Management Server	1
Virtual Server	**1**
Hyper-V Virtual Machine	1
VPN	**1**
Other Third-party VPN	1
Web Application	**6268**
Aboriginal Research Network	1
CWA (Compensation Web Application)	1540
EFormsXpress	61
Firefox	2
Flash	45
GEDS (web500)	2
Icase	2590
Internet DOJ	2
Intranet JUSnet	6
JUSaccess	1959
LOPORS	1
Other In-House Web Application	3
Other Third-Party Web Application	8
Ringtail Casebook	2
Ringtail Viewer	23
Travel AcXess Voyage	7
Webex	16
Grand Total	**33137**

Incident History by Service Type	
	Number of Incidents (12-month Period)
Application Management	17
Account Mgmt.	**6**
Create ID	1
Permissions	**5**
Administration	7
Configuration	**7**
Breakfix	2
Configuration	**1**
Connectivity	1
Improvement initiative	**1**
N/A	1
Remedy ITSP	**1**
Training	1
Email Management	1
Service Change	1
Client related	1
End-User Computing	**56**
Application	4
Error	**3**
Performance Issues	1
Breakfix	**1**
Configuration	1
Configuration	**9**
Password reset	1
Workstation	**8**
End-User Training	2
Onsite Coaching	**2**
IMAC - Ontario	1
Generic Request	**1**
Maintenance/Corrective	39
Clean	39
Network Management / Data	5
Maintenance/Corrective	5
Configure	**5**
Printing Support	2
IMAC - NCR	2
Configure Printer	2
Reporting	2
Customized report	**2**
N/A	2
Server Management	**912**
Breakfix	9
Failure	**9**
Mission Critical	801
Abnormal termination	487
Breakfix	**312**
(blank)	2
Non Mission Critical	**102**
Abnormal termination	96
Breakfix	6
Service Desk	33193
Error	2745
Configuration	185
Password reset	8
Service desk Coaching	3
Troubleshooting	2549
Other	27568
Configuration	5131
Password reset	2010
Request for Information	**1183**
Service desk Coaching	895
Troubleshooting	18349
OUTLOOK - Calendar	305
Configuration	**61**
Service desk Coaching	46
Troubleshooting	198

Incident History by Service Type	
	Number of Incidents (12-month Period)
OUTLOOK - Delegation	**130**
Configuration	24
Service desk Coaching	**64**
Troubleshooting	42
OUTLOOK - PST	**394**
Configuration	78
Service desk Coaching	**182**
Troubleshooting	134
Performance Issues	393
Configuration	33
Request for Information	2
Service desk Coaching	3
Troubleshooting	355
Printer	1657
Configuration	237
Request for Information	**3**
Service desk Coaching	1
Troubleshooting	**1416**
(blank)	1
(blank)	**1**
Grand Total	**34188**

8581-008 Hardware Break/Fix PC's Laptops & Printers:	Counts	Counts compared to Previous Month (+/-)
Hardware Break/fix PC's (NCR)	1917	-
Hardware Break/fix Laptops (NCR)	629	8.00
Hardware Break/fix Printers (NCR)	618	13.00

Incidents vs. Service Requests

All types/ Tous les types	Sep-12	Oct-12	Nov-12	Dec-12	Jan-13	Feb-13	Mar-13	Apr-13	May-13	Jun-13	Jul-13	Aug-13	Sep-13
Atlantic	18	16	23	26	25	22	24	216	199	229	212	173	210
Incidents	16	15	18	21	23	20	22	143	127	133	129	92	121
	89%	94%	78%	81%	92%	91%	92%	66%	64%	58%	61%	53%	58%
Service requests	2	1	5	5	2	2	2	73	72	96	83	81	89
	11%	6%	22%	19%	8%	9%	8%	34%	36%	42%	39%	47%	42%
B.C.	292	427	382	332	431	361	448	469	519	318	403	433	447
Incidents	169	322	270	237	303	229	302	326	387	213	274	205	262
	58%	75%	71%	71%	70%	63%	67%	70%	75%	67%	68%	47%	59%
Service requests	123	105	112	95	128	132	146	143	132	105	129	228	185
	42%	25%	29%	29%	30%	37%	33%	30%	25%	33%	32%	53%	41%
DLSU	303	285	362	386	363	349	385	378	330	272	344	311	357
Incidents	229	242	314	327	287	295	344	319	252	215	275	238	289
	76%	85%	87%	85%	79%	85%	89%	84%	76%	79%	80%	77%	81%
Service requests	74	43	48	59	76	54	41	59	78	57	69	73	68
	24%	15%	13%	15%	21%	15%	11%	16%	24%	21%	20%	23%	19%
NCR	1633	1818	1860	1443	1951	1862	1986	2341	1990	1909	1932	1694	2088
Incidents	1107	1235	1268	971	1273	1264	1433	1597	1296	1198	1336	1065	1292
	68%	68%	68%	67%	65%	68%	72%	68%	65%	63%	69%	63%	62%
Service requests	526	583	592	472	678	598	553	744	694	711	596	629	796
	32%	32%	32%	33%	35%	32%	28%	32%	35%	37%	31%	37%	38%
Northern	46	39	35	24	45	40	27	88	53	48	54	40	46
Incidents	38	18	22	16	36	26	19	69	29	30	33	21	27
	83%	46%	63%	67%	80%	65%	70%	78%	55%	63%	61%	53%	59%
Service requests	8	21	13	8	9	14	8	19	24	18	21	19	19
	17%	54%	37%	33%	20%	35%	30%	22%	45%	38%	39%	48%	41%
Ontario	77	74	79	80	300	107	254	634	562	510	532	377	456
Incidents	64	47	58	52	248	81	239	594	450	384	389	226	319
	83%	64%	73%	65%	83%	76%	94%	94%	80%	75%	73%	60%	70%
Service requests	13	27	21	28	52	26	15	40	112	126	143	151	137
	17%	36%	27%	35%	17%	24%	6%	6%	20%	25%	27%	40%	30%
Prairies	528	605	530	374	441	552	559	580	580	556	564	383	491
Incidents	328	367	323	241	301	345	396	388	368	322	407	240	309
	62%	61%	61%	64%	68%	63%	71%	67%	63%	58%	72%	63%	63%
Service requests	200	238	207	133	140	207	163	192	212	234	157	143	182
	38%	39%	39%	36%	32%	38%	29%	33%	37%	42%	28%	37%	37%
Quebec	279	356	318	225	278	385	313	330	330	310	282	306	348
Incidents	200	230	226	166	193	315	242	245	206	226	223	223	246
	72%	65%	71%	74%	69%	82%	77%	74%	62%	73%	79%	73%	71%
Service requests	79	126	92	59	85	70	71	85	124	84	59	83	102
	28%	35%	29%	26%	31%	18%	23%	26%	38%	27%	21%	27%	29%
Total	3176	3620	3589	2890	3834	3678	3996	5036	4563	4152	4323	3717	4443
Incidents	2151	2476	2499	2031	2664	2575	2997	3681	3115	2721	3066	2310	2865
	68%	68%	70%	70%	69%	70%	75%	73%	68%	66%	71%	62%	64%
Service requests	1025	1144	1090	859	1170	1103	999	1355	1448	1431	1257	1407	1578
	32%	32%	30%	30%	31%	30%	25%	27%	32%	34%	29%	38%	36%

Service Request Types		Number of Service Requests (12 Month period)
***Starting November 2012 to October 2013		
Install - Hardware		
	Dongle Device Request	3
	Non-Supported Hardware Installation (NCR)	2
	$URGENT$ - Supported Hardware Installation (NCR)	1
	Supported Hardware Installation (NCR)	1881
	Install Supported Hardware - Atlantic	9
	Install Supported Hardware - BC	49
	Install Supported Hardware - NR/Iqaluit	1
	Install Supported Hardware - NR/Whitehorse	1
	Install Supported Hardware - NR/Yellowknife	1
	Install Supported Hardware - Ontario	35
	Install Supported Hardware - Prairie	92
	Install Supported Hardware - Quebec	66
Install - Wireless Device		
	Aircard Installation, Transfer or Disposal (BCRO)	2
	Blackberry Installation, Transfer or Disposal (BCRO)	9
Install - Printer		
	Install Label Printer (NCR)	22
	Install Local Printer (NCR)	2
	Install Network Printer (NCR)	11
Install - Software		
	BSAS Supported Software Installation	2
	Supported Software Installation (DOJ-Desktop Install)	1
	Supported Software Installation (IMACRR Install)	249
	Supported Software Installation (REGIONS)	1
	Non-Supported Software requires BSAS approval rev 2	53
	Install Non-Supported Software (Atlantic)	2
	Install Non-Supported Software (BC)	12
	Install Non-Supported Software (Iqaluit)	1
	Install Non-Supported Software (Ontario)	5
	Install Non-Supported Software (Prairie)	21
	Install Software (Atlantic)	1
	Install Software (Quebec)	84
	Install Supported Software (Atlantic)	2
	Install Supported Software (BC)	48
	Install Supported Software (Iqaluit)	2
	Install Supported Software (Ontario)	12
	Install Supported Software (Prairie)	91
	Install Supported Software (Yellowknife)	1
	Install Secure Software Entrust - Regional	20
	Install Secure Software Entrust - NCR	78
Install/Reimage - Laptop		
	Install Laptop (NCR)	3
	Installation or Re-image of Laptop Computer (REGIONS)	8
	Re-image Laptop Only (NCR)	1
Install/Reimage - Desktop		
	Reimage Computer Only (NCR)	1
	Reimage Desktop (BC)	1
Move		
	Move (Atlantic)	3
	Move (BC)	36
	Move (Ontario)	16
	Move (Prairie)	68
	Move (Quebec)	4
Move - Relocating Operating CI		
	Computer Equipment Single Move (BC) - J. Lau	1
	Large Move 6 users or more (NCR)	5
	Small Move 5 users or less (NCR)	92
Change - Wireless Device		
	Aircard Installation, Transfer or Disposal (ARO)	8
	Aircard Installation, Transfer or Disposal (BCRO)	12
	Aircard Installation, Transfer or Disposal (NCR)	65
	Aircard Installation, Transfer or Disposal (ORO)	10
	Aircard Installation, Transfer or Disposal (PRO)	21

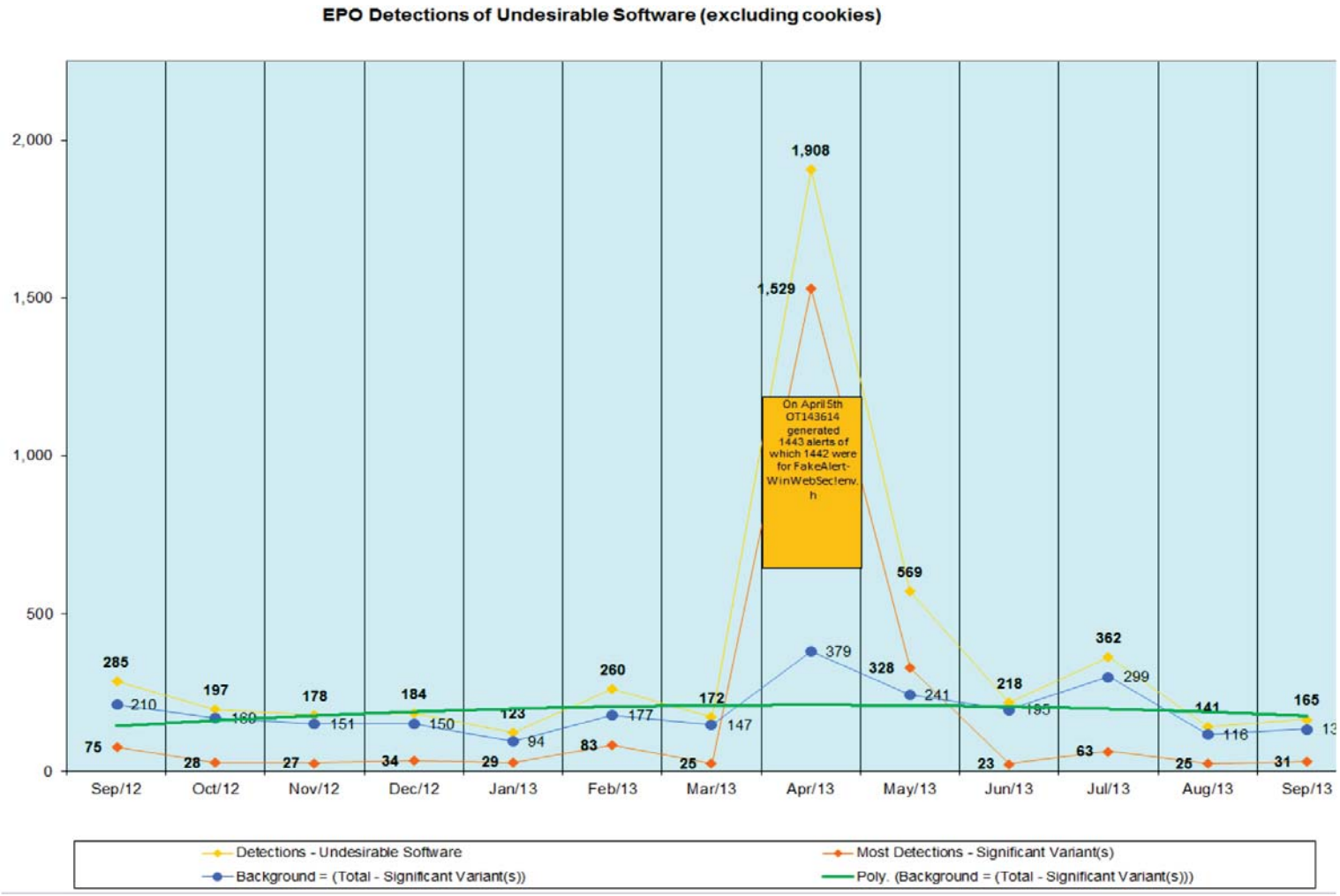
Service Request Types		Number of Service Requests (12 Month period)
	Aircard Installation, Transfer or Disposal (QRO)	2
	Blackberry Installation, Transfer or Disposal (ARO)	18
	Blackberry Installation, Transfer or Disposal (BCRO)	100
	Blackberry Installation, Transfer or Disposal (Iqaluit)	6
	Blackberry Installation, Transfer or Disposal (NCR)	503
	Blackberry Installation, Transfer or Disposal (ORO)	128
	Blackberry Installation, Transfer or Disposal (PRO)	79
	Blackberry Installation, Transfer or Disposal (QRO)	99
	Blackberry Installation, Transfer or Disposal (Whitehorse)	3
	Blackberry Installation, Transfer or Disposal (Yellowknife)	5
	Request for Wireless	76
Create NT Account		
	Create NT Account for Crown Agent	4
Create ID-Quebec		
	Create IFMS Access	1
	Create JusAccess (Quebec Region rev 2)	21
	Create People Soft Access	1
	Create Ringtail JusAccess	1
Create ID-Prairie		
	Create JusAccess (Prairie rev 2)	19
	Create LOPORS JusAccess	2
	Create PeopleSoft JusAccess	2
	Create Ringtail JusAccess	2
Create ID-Ontario		
	Create JusAccess (Ontario Region rev 2)	23
	Create Ringtail JusAccess	1
Create ID-North/Yellowknife		
	Create JusAccess (NR/Yellowknife rev 2)	1
Create ID-North/Whitehorse		
	Create IFMS Access	1
	Create JusAccess (NR/Whitehorse rev 2)	4
	Create PeopleSoft JusAccess	2
Create ID-BC		
	Create IFMS Access	1
	Create JusAccess (BC Region rev 2)	32
	Create People Soft Access	2
Create ID-Atlantic		
	Create JusAccess (Atlantic Region rev 2)	4
	Create JusAccess (Atlantic)	1
Create ID (NCR)		
	Create IFMS Access	38
	Create JusAccess NCR/DLSU/Crown Agent	397
	Create LOPORS Access	9
	Create People Soft Access	59
	Create RIMS Access rev 2	66
	Create Ringtail Access	49
Create ID (DLSU)		
	Create IFMS Access	95
	Create JusAccess NCR/DLSU/Crown Agent	291
	Create LOPORS Access	17
	Create PeopleSoft Access	64
	Create Ringtail Access	97
	Enable Remedy Profile	239
Create ID (Crown Agent)		
	Create JusAccess (Crown Agents)	153
	Enable Remedy Profile	140
Create ID		
	Create Non-Standard Email Account	42
	Create Remedy Account	13
	Provide Admin Privilege to Account	1
	Provide Local Admin Account	8
	Provide x_account info	7
New Employee - NCR		
	Create IFMS Account rev 2	44
	Create LOPORS Access	7

Service Request Types		Number of Service Requests (12 Month period)
	Create PeopleSoft Access	127
	Create RIMS Access rev 2	44
	Create Ringtail Account rev 2	36
	Enable Remedy Profile	376
	Install NEW Desktop PC (w/ monitor, keyboard, mouse)	117
	New Account (NCR)	454
	Send Welcome Email - DOJ	433
New Employee		
	Create IFMS Account	18
	Create LOPORS Access	7
	Create PeopleSoft Access	63
	Create RIMS Access (NR/Yellowknife)	1
	Create Ringtail Access	7
	Enable Remedy Profile	124
	Enabled Remedy profile	83
	New Account (Atlantic)	18
	New Account (BC)	42
	New Account (NR/Iqaluit)	9
	New Account (NR/Whitehorse)	6
	New Account (NR/Yellowknife)	21
	New Account (Ontario)	26
	New Account (Prairie)	100
	New Account (Quebec)	4
	Send Welcome Email - DOJ	218
Modify Account/ID		
	Blackberry Transfer/Setup-Request to transfer to another user NCR	5
	Modify Remedy Account	102
	Transfer & Setup Blackberry (BC)	1
	Modify Account-Quebec	189
	Modify Account-Prairie	292
	Modify Account-Ontario	122
	Modify Account-NCR	3359
	Server Infra to perform the move - NCR	1
	Account Modification Administration (BC)	508
	Create Generic Request for BC	1
	Modify Account-Atlantic	37
	Account Modification Administration (NCR)	3
	Modify RIMS Account	1
Create/Modify Distribution List		
	Create Distribution List (NCR)	47
	Create Distribution List (REGIONS)	44
	Modify Distribution List (NCR/DSLU)	102
	Modify Distribution List (REGIONS)	95
Account Transfer		
	Server Infra to perform the move	28
Account termination		
	Delete Accounts - BC	67
	Delete Accounts - North/Iqaluit	5
	Delete Accounts - North/Yellowknife	10
	Delete Accounts - Ontario	9
	Delete Accounts - Prairie	98
	Delete Network Accounts -NCR	128
	Delete Accounts - Atlantic.	14
Delete ID		
	Delete Remedy Account	6
Remove - Hardware		
	Remove Hardware - Atlantic	1
	Remove Hardware - BC	2
	Remove Hardware - Ontario	1
	Remove Hardware - Prairie	7
	Remove Hardware - Quebec	3
	Remove PC	36
Remove - Printer		
	Remove Printer (NCR)	2
Printer		

16. Service Request by Type

Service Request Types		Number of Service Requests (12 Month period)
	Request for Printer Toner (Prairie)	20
	Request for Printer Toner (Quebec)	1
Management Template		
	Create / Modify Request Management Template	1
Secure Data Destruction		
	Secure Data Destruction - NCR	1
SSM		
	SSM Request - NCR	20
Lan Jack Activation		
	Lan Jack Activation	10
Backup		
	Data Backup / CD burning (NCR)	3
	Data Backup / CD burning (REGIONS)	10
Bioclips		
	Non Standard Bioclip 2 or 4 GB (NCR)	4
	Non Standard Bioclip /USB devices (+2GB)	31
	Non Standard Bioclip /USB devices (+8GB)	3
	Standard Bioclip/USB storage less than 2GB	28
	Standard Bioclip/USB storage less than 8GB	97
Generic Request		
	Create Generic Request for Atlantic	426
	Create Generic Request for NR/Iqaluit	25
	Create Generic Request for NR/Whitehorse	10
	Create Generic Request for NR/Yellowknife	29
	Create Generic Request for Ontario	435
	Create Generic Request for BC	679
	Create Generic Request for Prairies	1092
	Create Generic Request for Quebec	547
	Generic Request NCR	1136
Equipment Loan		
	Request to borrow IT equipment (BC Region)	3
	Request to borrow IT equipment (NCR)	3
	Request to borrow IT equipment (Other Regions)	1
	Request to borrow IT equipment (Prairie)	10
	Request to borrow IT equipment (Quebec)	5
Training Request		
	Request for Training on Remedy ITSP	2
RDIMS ID		
	RDIMS New Account or Training/Coaching Request	158
	RDIMS Account Termination	22

Security Operations



Encryption Statistics	GB/Hour
SecureDoc full disk encryption rate	10

ATTACHMENT 3
MANDATORY BID EVALUATION CRITERIA

1. Mandatory Evaluation Criteria

(a) Approach Document

Criteria ID	Requirement	Bidder's Response
M1	The Bidder must provide with its bid a *Help Desk and Support Services Solution Approach Document* in which it must demonstrate its understanding of the Work and how it will meet the requirements outlined in the Statement of Work. The *Help Desk and Support Services Solution Approach Document* must describe the Bidder's: (a) Approach and methodology for the pre-transition, implementation, and the poste-implementation activities; (b) Overall solution architecture; (c) Maintenance and Support Concept of Operations, including how it will deliver on-going services during the entire Contract Period; (d) Value-added elements that it will include as part of its services, not identified in the Statement or Work; (e) Implementation milestone schedule, in chronological order; (f) Strategies to mitigate risks that could adversely affect the implementation timeline and the quality of service delivery; (g) Approach to formulate and enforce work and quality standards, and how the service will be continually improved during the entire Contract Period; and (h) Strategies to retain and train its resources, and how it will train its On-Site Support Services resources in the regions. The Bidder is asked to ensure its responses to each element above are segregated, where possible, by Service Domain (i.e. Service Desk Service, On-Site Support Service and Desktop Engineering Service). **Note to the Bidder:** The *Help Desk and Support Services Solution Approach Document* will be further assessed against the point-rated criteria in Attachment 4 of this bid solicitation.	

(b) Corporate Experience

Criteria ID	Requirement	Bidder's Response
M2	The Bidder must demonstrate its corporate experience delivering Service Desk Support, On-Site Support and Desktop Engineering Support services. To demonstrate its experience, the Bidder must reference a minimum of three projects, where: (a) each project: (i) included all of the following services: (A) Service Desk Support; (B) On-Site Support; (C) Desktop Engineering Support; (ii) was within the five years preceding the posting date of this bid solicitation; and (iii) was in support of a minimum of 2,500 users; (b) at least one project was in support of a minimum of 5,000 users; (c) at least one project was in support of a minimum of 500 printers; (d) at least one project was in support of a Canadian public sector organization; and (e) at least one project was for a customer requiring services in English and French. **Note to the Bidder:** internal projects within the Bidder's organization are accepted.	

(c) OEM Authorization

Criteria ID	Requirement	Bidder's Response
M3	The Bidder must certify that it is authorized by each Original Equipment Manufacturer (OEM) to provide Break/Fix services for the hardware listed in Appendix F to Annex A, Standard Hardware and Software, Table 2: Hardware List installed within Justice Canada.	

(d) Proposed Resources

Criteria ID	Requirement	Bidder's Response
M4	The Bidder must propose one resource to fulfil each of the following resource categories: (a) Project Manager; (b) Technology Architect; (c) Security Specialist; (d) Business Analyst; (e) On-Site Service Representative; (f) On-Site Service Team Leader; (g) Implementation Project Manager; (h) Solution Architect; (i) Security Architect; and (j) Service Manager. The Bidder must not propose the same resource for two or more categories. The Bidder must provide one résumé for each of its proposed resources.	

(e) Resource Experience

Criteria ID	Requirement	Bidder's Response
M6	**Project Manager** The Bidder must demonstrate that its proposed Project Manager has: (a) a minimum of 5 years of experience managing IT projects; and (b) one of the following project management certifications: (i) Project management professional PMP (Project Management Institute (PMI)) (ii) Certified associate in project management CAPM (PMI) (iii) CompTIA Project+ (iv) Master Project Manager MPM (American Academy of Project Management) (v) Certified Project Manager CPM (International Association of Project and Program Management) (vi) Project Management in IT Security PMITS (EC-Council)	

	(vii) Associate in Project Management APM (Global Association for Quality Management (GAQM)) (viii) Professional in Project Management PPM (GAQM) (ix) Certified Project Director (GAQM) The Bidder must provide a copy of each certification.	
M7	**Technology Architect** The Bidder must demonstrate that its proposed Technology Architect has a minimum of 5 years of experience architecting solutions in the Help Desk and Support domain.	
M8	**Security Specialist** The Bidder must demonstrate that its proposed Security Specialist has a minimum of 5 years of experience performing the following tasks: (a) Conducting security threat and risk assessments; and (b) Developing and enforcing IT security policies, standards, guidelines and procedures on the security aspects of IT facilities and application systems. **Note to the Bidder:** the minimum 5 years of experience is a cumulative total of the experience performing all tasks (e.g. 2 years of experience performing (a) and 3 years of experience performing (b) meets the minimum 5 years of experience).	
M9	**Business Analyst** The Bidder must demonstrate that its proposed Business Analyst has a minimum of 5 years of experience analyzing business requirements in IT projects.	
M10	**On-Site Service Representative** The Bidder must demonstrate that its proposed On-Site Service Representative has a degree, diploma or certificate in a relevant field of study. The Bidder must provide a copy of each degree, diploma or certificate.	
M11	**On-Site Service Representative** The Bidder must certify that its proposed On-Site Service Representative has the following qualifications:	

	(a) Fluent* in English and French; (b) Thorough knowledge of Help Desk and Support hardware (PC assembly, PC components) and Help Desk and Support software; and (c) Strong customer service and communication skills (both verbal and written). *To be considered fluent, the proposed resource must be able to communicate orally and in writing in English and in French without any assistance and with minimal errors.	
M12	**On-Site Service Team Lead** The Bidder must demonstrate that its proposed On-Site Service Team Lead has: (a) successfully completed a relevant training program from a recognized institution (e.g. relevant program at a community college); and (b) a minimum of 5 years of experience in a similar role. The Bidder must provide a copy of each degree, diploma or certificate.	
M13	**On-Site Service Team Lead** The Bidder must certify that its proposed On-Site Service Team Lead has the following qualifications: (a) Fluent* in English and French; and (b) Strong customer service and communication skills (both verbal and written). *To be considered fluent, the proposed resource must be able to communicate orally and in writing in English and in French without any assistance and with minimal errors.	
M14	**Implementation Project Manager** The Bidder must demonstrate that its proposed Implementation Project Manager has: (a) a minimum of 5 years of experience managing IT projects; (b) one of the following project management certifications: (i) Project management professional PMP (Project Management Institute (PMI)) (ii) Certified associate in project management CAPM (PMI)	

	(iii) CompTIA Project+ (iv) Master Project Manager MPM (American Academy of Project Management) (v) Certified Project Manager CPM (International Association of Project and Program Management) (vi) Project Management in IT Security PMITS (EC-Council) (vii) Associate in Project Management APM (Global Association for Quality Management (GAQM)) (viii) Professional in Project Management PPM (GAQM) (ix) Certified Project Director (GAQM) The Bidder must provide a copy of each certification.	
M15	**Solution Architect** The Bidder must demonstrate that its proposed Solution Architect has a minimum of 5 years of experience architecting solutions in the Help Desk and Support domain.	
M16	**Security Architect** The Bidder must demonstrate that its proposed Security Specialist has a minimum of 5 years of experience performing the following tasks: (a) Conducting security threat and risk assessments; and (b) Developing and enforcing IT security policies, standards, guidelines and procedures on the security aspects of IT facilities and application systems. **Note to the Bidder:** the minimum 5 years of experience is a cumulative total of the experience performing all tasks (e.g. 2 years of experience performing (a) and 3 years of experience performing (b) meets the minimum 5 years of experience).	
M17	**Security Architect** The Bidder must demonstrate that its proposed Security Architect has a certification from an internationally recognized security professionals organization (e.g. International Information Systems Security Certification Consortium $(ISC)^2$). The Bidder must provide a copy of each certification.	
M18	**Service Manager**	

	The Bidder must demonstrate that its proposed Service Manager has a minimum of 5 years of experience in a similar role in the Help Desk and Support domain.	

ATTACHMENT 4

POINT-RATED BID EVALUATION CRITERIA

1. Point-Rated Evaluation Criteria

(a) Approach Document

Criteria ID	Requirement	Point Allocation Scheme	Bidder's Response
R1	**<u>Approach and methodology for the pre-transition, implementation, and the poste-implementation activities</u>** The Bidder's *Help Desk and Support Services Solution Approach Document* should include the following elements: Element 1 information that demonstrates the Bidder's understanding of the requirement and the technical concepts defined in the Statement of Work, and that demonstrates a successful strategy to deliver quality services and achieve the objectives; Element 2 Evidence of Bidder-specific approaches, methods and techniques for completing	Points will be awarded in accordance with the following: a) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 1 = 10 points; b) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 2 = 5 points; and c) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 3 = 5 points. **Maximum Points = 20**	

	the pre-transition, implementation and post-transition activities; and Element 3 Information regarding the Bidder's ability to address anticipated potential problem areas in the handover activities, and roles and responsibilities of key stakeholders.		
R2	**<u>Solution Architecture in the Help Desk and Support Services Solution Approach Document</u>** The Bidder's *Help Desk and Support Services Solution Approach Document* should include the following elements: Element 1 Information to demonstrate the Bidder's understanding of the work, including creativity and thoroughness shown in its understanding of the objectives of the Statement of Work and specific tasks, and planned implementation of the Help Desk and Support Services; Element 2 Description of the Bidder's proposed Help Desk and Support Services including the name and capabilities of the Bidder's software and specifically the software's incident handling, escalation, and other minimum capabilities described in Statement of Work; Element 3 Description of the standard processes, procedures and resources that the Bidder will apply to proactively prevent and reduce the impact of security threats on the JUS Help Desk & support infrastructure and to facilitate recovery from security incidents, including any other processes and resources the	Points will be awarded in accordance with the following: a) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 1 = 3 points; b) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 2 = 3 points; and c) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 3 = 2 points. d) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 4 = 2 points. **Maximum Points = 10**	

	Bidder plans to use to identify and prioritize threats, and mitigate risks; and Element 4 Description of the key capabilities of the Service Delivery Portal the Bidder will provide and an explanation of how it will be employed to meet the requirements in Statement of Work.		
R3	**<u>Maintenance and Support Concept of Operations in the Help Desk and Support Services Solution Approach Document</u>** The Bidder's *Help Desk and Support Services Solution Approach Document* should include the following elements: Element 1 The Bidder's maintenance and support concept of operations plan to demonstrate its understanding of all aspects of the on-going services described in the SOW; Element 2 Description of the extent to which the Bidder's normal service management and delivery practices and procedures conform to a recognized best practices framework such as the Information Technology Infrastructure Library (ITIL) and how it has applied best practices such as Incident, Problem, Change, Configuration, Asset, Software License, Release and Service Operations Management; and a description of how the Bidder proposes to apply these practices and related methodologies	Points will be awarded in accordance with the following: a) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 1 = 10 points; b) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 2 = 10 points; and c) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 3 = 5 points. d) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 4 = 5 points. **Maximum Points = 30**	

	(e.g. Continual Service Improvement) and tools to ensure the consistent delivery of high quality services; Element 3 Description of how the Bidder proposes to manage the relationship with Canada, including proposed regular meetings, presentations, issue escalation and dispute resolution process, other major processes and reports; Element 4 A list of the roles and responsibilities for key stakeholders involved in steady state operations.		
R4	**<u>Value Added Elements in the Help Desk and Support Services Solution Approach Document</u>** The Bidder's *Help Desk and Support Services Solution Approach Document* should include five additional services, enhanced services, service methodologies or other items that are not identified as part of the on-going services in the Statement of Work; and the nature of these additional services, enhanced services, service methodologies or other items and their potential value or benefit to Canada.	The Bidder will obtain 2 points per service, enhanced service, service methodology or other item. **Maximum Points = 10**	
R5	**<u>Milestones in the Help Desk and Support Services Solution Approach Document</u>** The Bidder's *Help Desk and Support Services Solution Approach Document* should include the following elements: Element 1 Descriptions of the implementation milestones in chronological order; and	Points will be awarded in accordance with the following: a) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 1 = 6 points; b) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 2 = 4 points; and	

	Element 2 Evidence that all contractual deliverables are included in the milestones.	**Maximum Points = 10**	
R6	**Risk Management in the Help Desk and Support Services Solution Approach Document** The Bidder's *Help Desk and Support Services Solution Approach Document* should include the following elements: Element 1 A list of key risks to the timelines and quality of the Pilot service delivery; and Element 2 A list of mitigation for each identified key risk.	Points will be awarded in accordance with the following: a) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 1 = 5 points; b) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 2 = 5 points; and **Maximum Points = 10**	
R7	**Quality Assurance and Continuous Improvement Plan in the Help Desk and Support Services Solution Approach Document** The Bidder's *Help Desk and Support Services Solution Approach Document* should include the following elements: Element 1 Information of Bidder-specific methods and techniques to ensure quality assurance and continuous improvement related to processes for Service Delivery and Service Management; and Element 2 Description of the Bidder's approach and methodologies for measuring Quality Assurance and how it plans on applying these methodologies.	Points will be awarded in accordance with the following: a) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 1 = 5 points; b) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 2 = 5 points; and **Maximum Points = 10**	
R8	**Organizational Plan in the Help Desk and Support Services Solution Approach Document**	Points will be awarded in accordance with the following:	

	The Bidder's *Help Desk and Support Services Solution Approach Document* should include the following elements:
	
	Element 1 An organization chart showing the key roles and their organizational relationship to one another in the management and delivery of services; and a description of the main responsibilities and authorities of each of these roles;
	
	Element 2 Description of profiles and minimum qualifications the Bidder will apply for original or replacement personnel fulfilling each of the roles listed in Element 1 above;
	
	Element 3 The Bidder's plan to address strategies for staff retention and training to ensure its personnel have the required skill sets and are kept up-to-date on new and changing technologies; and
	
	Element 4 The Bidder's plan to address how Government of Canada On-site and Break/Fix Support personnel in the regions will be trained.
		a) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 1 = 4 points;
		
		b) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 2 = 2 points;
		
		c) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 3 = 2 points; and
		
		d) The Bidder's *Help Desk and Support Services Solution Approach Document* includes Element 4 = 2 points.
		
		Maximum Points = 10	

		Available Technical Points	**110**
		Bidder's Score (A)	

(b) Corporate Experience

Criteria ID	Requirement	Point Allocation Scheme	Bidder's Response
R9	**Service Desk Support in Canada**	Points will be awarded in accordance with the following:	

	The Bidder should demonstrate its corporate experience delivering Service Desk Support services to support a minimum of 2,500 users in Canada.
	
	Each project referenced by the Bidder to demonstrate its experience must have had a minimum duration of 2 consecutive years within the 5 years preceding the posting date of this bid solicitation.
	
	Note to the Bidder: internal projects within the Bidder's organization are accepted.
		a) Project supporting between 2,500 and 4,999 users = 5 points;
		b) Project supporting between 5,000 and 7,999 users = 10 points;
		c) Project supporting 8,000 or more users = 15 points;
		d) 5 points if one of the projects was for a Canadian public sector organization; and
		e) 5 points if one of the projects was for a customer requiring services in both English and French.
		
		Maximum Points = 40
		Note: Only a maximum of 30 points will be awarded based upon a combination of projects from a, b and c above.	

R10	**<u>On-Site Support in Canada</u>**
	
	The Bidder should demonstrate its corporate experience delivering On-Site Support services to support a minimum of 2,500 users in Canada.
	
	Each project referenced by the Bidder to demonstrate its experience must have had a minimum duration of 2 consecutive years within the 5 years preceding the posting date of this bid solicitation.
	Note to the Bidder: internal projects within the Bidder's organization are accepted.
		Points will be awarded in accordance with the following:
		a) Project supporting between 2,500 and 4,999 users = 5 points;
		b) Project supporting between 5,000 and 7,999 users = 10 points;
		c) Project supporting 8,000 or more users = 15 points;
		d) 5 points if one of the projects was for a Canadian public sector organization; and
		e) 5 points if one of the projects was for a customer requiring services in both English and French.	

		Maximum Points = 40 Note: Only a maximum of 30 points will be awarded based upon a combination of projects from a, b and c above.	

R11	**<u>Desktop Engineering Support in Canada</u>**
	
	The Bidder should demonstrate its corporate experience delivering Desktop Engineering Support services to support a minimum of 2,500 users in Canada.
	
	Each project referenced by the Bidder to demonstrate its experience must have had a minimum duration of 2 consecutive years within the 5 years preceding the posting date of this bid solicitation.
	
	Note to the Bidder: internal projects within the Bidder's organization are accepted.
		Points will be awarded in accordance with the following:
		
		a) Project supporting between 2,500 and 4,999 users = 5 points;
		
		b) Project supporting between 5,000 and 7,999 users = 10 points;
		
		c) Project supporting 8,000 or more users = 15 points; and
		
		d) 5 points if one of the projects was for a Canadian public sector organization.
		
		Maximum Points = 25
		Note: Only a maximum of 20 points will be awarded based upon a combination of projects from a, b and c above.	

R12	**<u>Service Desk and On-Site Printer Support in Canada</u>** The Bidder should demonstrate its corporate experience delivering Service Desk and On-Site Support services to support a minimum of 200 printers in a network environment.	Points will be awarded in accordance with the following: a) Project supporting between 200 and 399 printers = 5 points;	

	Each project referenced by the Bidder to demonstrate its experience must have had a minimum duration of 2 consecutive years within the 5 years preceding the posting date of this bid solicitation. **Note to the Bidder:** internal projects within the Bidder's organization are accepted.	b) Project supporting between 400 and 599 printers = 10 points; and c) Project supporting 600 or more printers = 15 points. **Maximum Points = 20**	
		Available Technical Points	**125**
		Bidder's Score (B)	

(c) Resource Experience

Criteria ID	Requirement	Point Allocation Scheme	Bidder's Response
R13	**<u>Implementation Project Manager</u>** The Bidder should demonstrates that its proposed Implementation Project Manager has experience being the lead project manager on projects implementing Help Desk Support services. Each project referenced by the Bidder must have been in support of a minimum of 2,500 users and included one of the following services: (a) Service Desk Support; (b) On-Site and Break/Fix Support; or (c) Desktop Engineering Support. **Note to the Bidder:** internal projects within the Bidder's organization are accepted.	Points will be awarded in accordance with the following: a) 5 points per project, up to a maximum of 3 projects; b) 5 points if one of the projects included all services (i.e. Service Desk, On-Site and Break/Fix, and Desktop Engineering Support services); and c) 5 points if one of the projects was for a Canadian public sector organization. **Maximum Points = 25**	

R14	**Solution Architect** The Bidder should demonstrates that its proposed Solution Architect has experience being the lead solution architect on projects implementing Help Desk Support services. Each project referenced by the Bidder must have been in support of a minimum of 2,500 users and included one of the following services: (d) Service Desk Support; (e) On-Site and Break/Fix Support; or (f) Desktop Engineering Support. **Note to the Bidder:** internal projects within the Bidder's organization are accepted.	Points will be awarded in accordance with the following: a) 5 points per project, up to a maximum of 3 projects; b) 5 points if one of the projects included all services (i.e. Service Desk, On-Site and Break/Fix, and Desktop Engineering Support services); and c) 5 points if one of the projects was for a Canadian public sector organization. **Maximum Points = 25**	
R15	**Security Architect** The Bidder should demonstrates that its proposed Security Architect has experience being the lead security architect on projects implementing Help Desk Support services. Each project referenced by the Bidder must have been in support of a minimum of 2,500 users and included one of the following services: (g) Service Desk Support; (h) On-Site and Break/Fix Support; or (i) Desktop Engineering Support. **Note to the Bidder:** internal projects within the Bidder's organization are accepted.	Points will be awarded in accordance with the following: a) 5 points per project, up to a maximum of 3 projects; b) 5 points if one of the projects included all services (i.e. Service Desk, On-Site and Break/Fix, and Desktop Engineering Support services); and c) 5 points if one of the projects was for a Canadian public sector organization. **Maximum Points = 25**	
R16	**Service Manager**	Points will be awarded in accordance with the following:	

	The Bidder should demonstrates that its proposed Service Manager has experience being the lead service manager on projects implementing Help Desk Support services. Each project referenced by the Bidder must have been in support of a minimum of 2,500 users and included one of the following services: (j) Service Desk Support; (k) On-Site and Break/Fix Support; or (l) Desktop Engineering Support. **Note to the Bidder:** internal projects within the Bidder's organization are accepted.	a) 5 points per project, up to a maximum of 3 projects; b) 5 points if one of the projects included all services (i.e. Service Desk, On-Site and Break/Fix, and Desktop Engineering Support services); and c) 5 points if one of the projects was for a Canadian public sector organization. **Maximum Points = 25**	
		Available Technical Points	**100**
		Bidder's Score (C)	

Maximum number of points available	**335**
Required Minimum Pass Mark	**201**
Bidder's Overall Technical Score ((A)+(B)+(C))	
Note to Bidders: Bids that do not meet the above minimum score of 201 points will not be evaluated further.	