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

SOLICITATION AMENDMENT
MODIFICATION DE L'INVITATION

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

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

Comments - Commentaires

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

Issuing Office - Bureau de distribution
Clothing and Textiles Division / Division des vêtements et des textiles
11 Laurier St./ 11, rue Laurier
6A2, Place du Portage
Gatineau, Québec K1A 0S5

Title - Sujet Non-Operational Clothing & Footwear	
Solicitation No. - N° de l'invitation W8486-174014/C	**Amendment No. - N° modif.** 006
Client Reference No. - N° de référence du client W8486-174014	**Date** 2019-02-11
GETS Reference No. - N° de référence de SEAG PW-$$PR-756-75835	
File No. - N° de dossier pr756.W8486-174014	**CCC No./N° CCC - FMS No./N° VME**
Solicitation Closes - L'invitation prend fin **at - à 02:00 PM** **on - le 2019-03-06**	**Time Zone** **Fuseau horaire** Eastern Standard Time EST
F.O.B. - F.A.B. **Plant-Usine:** ☐ **Destination:** ☐ **Other-Autre:** ☐	
Address Enquiries to: - Adresser toutes questions à: Picco(PR Div.), Robert	**Buyer Id - Id de l'acheteur** pr756
Telephone No. - N° de téléphone (613) 410-1348 ( )	**FAX No. - N° de FAX** ( ) -
Destination - of Goods, Services, and Construction: **Destination - des biens, services et construction:**	

Instructions: See Herein

Instructions: Voir aux présentes

Delivery Required - Livraison exigée	**Delivery Offered - Livraison proposée**
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**	

This Amendment #006 is raised to:

1. At Annex A – Delete Appendix 4, Tab 1, and insert Appendix 4, Tab 1 here attached.
   This new list Appendix 4, Tab 1 addresses bidder's question#6 published on amendment 005.

2. In the RFP – Delete Total bid Price section 4.3.3.4 b. c. and Insert Total bid Price section 4.3.3.4 b. c. here below ;

3. To extend the Request for proposal closing date.

4. Publish bidder's questions and answers.

Accordingly the request for proposal is hereby amended as follows:

1. In Reference to Amendment 005 - question #6.

At Annex A, Appendix 4, Tab 1, section 2.2.4, our interpretation is that an employee such as a programmer or customer service agent could not work from home under the new contract if they have access to DND personnel information. Does this clause only pertains when the source code can be accessed, such as a programmer, but a customer service agent could still take calls, access profile and responds to question? Can you please clarify how this should be interpreted?
Answer:
Canada has reviewed the Information Technology Security Requirements, Annex A, Appendix 4, Tab 1, and amended the security requirements to allow for mobile computing, teleworking, and wireless capabilities.-see attached new Appendix 4, Tab 1.

---

2. Delete :

4.3.3.4 Total Bid Price

b. For the purpose of establishing a Total Bid Price for evaluation purposes only, each of the LIUC found in Appendix 1 of Annex B will be multiplied by the estimated quantity per year of each item. The Total Bid Price will be established by adding the (resultant total of all LIUC) and the (resultant total for all LIUC by twice the offered firm Line Item Mark-up (LIM), or Management Fee (MF)).

c. Formula: (All LIUC x Estimated quantity per year) x (1 + 2 MF) = Total Bid Price;

Insert:

4.3.3.4 Total Bid Price

b. For the purpose of establishing a Total Bid Price for evaluation purposes only, each of the LIUC found in Appendix 1 of Annex B will be multiplied by the estimated quantity per year of each item. The Total Bid Price will be established by adding the (resultant total of all LIUC) and the (resultant total for all LIUC by the offered firm Line Item Mark-up (LIM), or Management Fee (MF)).

c. Formula: (All LIUC x Estimated quantity per year) x (1 + MF) = Total Bid Price;

---

3. As of this amendment 006, the closing date of the solicitation # W8486-174014/C is extended to March 6th, 2019 @ 2pm ET.

---

4. Bidder's Questions & Answers:

Question #1:
RFP Section 4.5.2: Could Canada consider reducing the weight of the ITB/VP score to 10%?
Answer #1:
Canada has considered industry's request to change the ITB/VP rated criteria evaluation weighting and has determined that the requirement will remain unchanged. The bid evaluation methodology, including the evaluation weighting for the rated criteria, was established based on internal analysis of the proposed procurement and stakeholder engagement to ensure that the bid evaluation methodology is appropriate for a competitive procurement of this nature.

Question #2:
RFP Section 7.23.1: Could Canada consider decreasing the financial security requirement by $1 million per annum as start of year 3, keeping a minimum $1 million financial security for year 6 and the remaining term of the contract?
Answer #2:
Canada has considered industry's request to decrease the financial security requirement and has determined that the $5M Security deposit requirement will remain as is. This amount is considered to be fair and reasonable given the anticipated overall Contract value.

Question #3:
Annex A – Appendix 12 – Professional Services Classifications: In the Mandatory Technical Requirements section for each of the PM and the CM, could Canada expand the reference period for experience to cover the last 15 years?
Answer #3:
DND will not consider amending the experience to cover the last 15 years.

Question #4:
Annex B – Basis of Payment, Section 7.3.1: Could Canada accept basing the calculation of the average yearly consumption on the previous 36 months?
Answer #4:
DND has considered the request and will amend the calculation for the average yearly consumption to be based upon the previous 36 months, rather than 24 months, as previously stated in the Basis of Payment, Annex B, Section 7.3.1.
As such at the Basis of Payment, Annex B, Section 7.3.1. :

Delete: Canada's average yearly consumption will be based on the sales of the previous 24 months period commencing 6 months prior to:

Insert : Canada's average yearly consumption will be based on the sales of the previous 36 months period commencing 6 months prior to:

Question #5
Annex C – Appendix 1, Section 3.3.5.2.1 Experience: This risk area allows a bidder to earn a point for past practice or experience in ITB/VP as it applies to each of the two plans. The resulting multiplier effect actually yields a differential in score of 5 points. Given the evident lack of experience most bidders would have in this field, could Canada not remove this risk area from the evaluation in order to make it equally fair to all bidders?
Answer #5
For mandatory ITB requirement two, Canada has considered industry's request to change the ITB Plans risk assessment methodology and has determined that the requirement will remain unchanged.

The ITB Plans are assessed on the information provided by the Bidder which demonstrates how they propose to deliver on the ITB requirements of the contract. Should there be ITB Plan elements where the Bidder has little or no experience, it is expected that the Bidder includes an explanation detailing how they propose to manage and mitigate risk for that element to ensure that they are successfully able to complete the contract ITB Obligations.

Question #6:
Annex C – Appendix 1, Section 3.3.5 Evaluation of Requirement Two: Due to the lack of experience bidders have in responding to this ITB/VP requirement, could Canada consider limiting the two plans to being mandatory requirements as per section 3.3 and not rate them in terms of a pass or fail score?
Answer #6:
For mandatory ITB requirement two, Canada has considered industry's request and has determined that the requirement will remain unchanged. Bidders should note that in order to minimize the risk of non-compliant bids, Canada is conducting a Phased Bid Compliance Process for this requirement whereby a bidder evaluated as non-compliant will be offered an opportunity to submit additional or different information in order to be re-evaluated as compliant with respect to Eligible Mandatory Requirements. Bidders are encouraged to review the information on the bid evaluation process found at section 4.3 of the Request for Proposals.

All other terms and conditions of the Request for Proposal remain unchanged.

Department of National Defence (DND)

Information Technology Security Requirements

For

Contract W8486-174014

1. INTRODUCTION 7

2. MANDATORY PREREQUISITES 8

2.1. PUBLIC SERVICES AND PROCUREMENT CANADA (PSPC) VALIDATION FOR PHYSICAL SECURITY 8
2.2. PHYSICAL SECURITY 8
2.3. PERSONNEL SECURITY 9
2.4. PROCEDURAL SECURITY 10
2.5. INFORMATION SECURITY 10

3. MINIMUM IT SECURITY REQUIREMENTS 12

3.1. IT SECURITY POLICY COMPLIANCE AND MONITORING 12
3.2. IT EQUIPMENT 12
3.3. IT SYSTEM CONFIGURATION 12
3.4. AUTHORIZATION AND ACCESS CONTROL 13
3.5. IT MEDIA 14
3.6. DOCUMENT PRINTING / REPRODUCTION 15
3.7. RECOVERY 16
3.8. DISPOSAL 16

1. Introduction

1.1 This document outlines the Information Technology (IT) Security requirements for the Department of National Defence's (DND) Contract W8486-174014 for the processing, production and/or storage of sensitive information up to and including the level of Protected B. Considering the IT portion of the Security clearance being Contract specific, the intent of this document is to establish the minimum IT Security safeguards required for the processing, production and/or storage of sensitive information be approved by the DND Project Authority (PA).

1.2 Security is based upon layers of protection; that is, in order for the requirements of the IT Security (ITSEC) to effectively safeguard the information, they must be preceded and supported by other aspects of security and their associated policies. Prior to engaging in the contracted efforts, in accordance with the Policy on Government Security (PGS) and ITSEC related Policy, Directive and Standards, physical, personnel, procedural and information security safeguards, must exist prior to the implementation of ITSEC safeguards.

1.3 As a part of selecting contractual IT Security safeguards, Project Leads should carefully consider the impact of the selected IT security safeguards on cost, schedule and operational requirements. Project Leads should be looking for a reasonable trade-off between the incremental cost of security requirements and the risk mitigation that would result from their use. The DND DIM Secur can assist Project Leads with these decisions, when requested.

2. Mandatory Prerequisites

2.1. Public Services and Procurement Canada (PSPC) Validation for Physical Security

2.1.1 The application of the ITSEC safeguards listed in this document are based on the mandatory requirement that the physical premises have been inspected, assessed and authorized to process, produce and store Protected B information. Validation must be provided by the Canadian Industrial Security Directorate (CISD) and PSPC.

2.1.2 The Contractor must inform CISD and the PA of all physical sites where contractual information will be processed, produced and/or stored. This includes (as applicable), but is not limited to, the main/secondary Contractor's offices, construction sites, back-up storage locations, and partner's/Sub-Contractor's offices.

2.1.3 Upon validation, CISD will notify the PA, the Director Defence Security Operations (DDSO) Industrial Security Lead and the Directorate Information Management Security (DIM Secur) Operations of the successful completion of this requirement. Every site must be granted a Facility Security Clearance (FSC), a Designated Organisation Screening (DOS) or a Document Safeguarding Capability (DSC) as applicable, and be cleared for Reliability Status IT Security by CISD prior to be authorized to process, produce and/or store government sensitive information, up to and including Protected B.

2.1.4 IT Links must also be validated by CISD before it can be used to transfer any contractual Protected B information. The contractor's IS dedicated to transfer Protected B information must comply with the requirement for 128-bit encryption.

2.2. Physical Security

2.2.1 Processing, production and/or storage of contractual information must only be performed in the facility(s) which has been authorized by CISD.

2.2.2 The Order Management System (OMS) IS must be installed and be operated in an Operational zone.

2.2.3 Processing, production and/or storage of contractual information cannot be performed outside Canada. All data must be processed, produced and stored in a secure manner that prevents unauthorized viewing, access, or manipulation. Sensitive or restricted data includes, but is not limited to, user's personal information, Canada's In-Service Support contract information, suppliers' financial information and technical design information.

2.2.4 Mobile computing / Teleworking involving the OMS IS is authorised on this Contract. The remote location where the contractual information will be processed must be approved as an

Operational zone. The Contractor's personnel must use mobile computing device(s) equipped with VPN (Virtual Private Network) capability using a combination of dedicated connections and encryption protocols to generate virtual Peer-to-Peer (P2P) connections and enable secure tunnelled access to a segment of the Contractor's corporate network where contractual information will be processed. The Contractor must implement configuration management, device identification and authentication; use of up-to-date mandatory protective software; scanning devices for malicious code, critical software updates and patches as well as to conduct primary operating system integrity checks and disable unnecessary hardware.

2.2.5 A trusted thin client connection must be used via approved VPN communication encryption. Trusted thin client connection must be designed to lock down the hardware of the remote device(s) and disallow access to the devices' internal or external hard drives, CD-ROM/RW, other USB ports and interfaces with exception of the components required to establish secure access to segregated segment of the Contractor's corporate network that the administrators or agents may need to process contractual information.

2.2.6 An authorized user of the remote device must use decryption password to allow hardware-based system integrity validation and initiate secure VPN connection to dedicated segment of the Contractor's corporate network which will be used to save and transmit contractual information. All contractual information must be saved on this segregated segment of the Contractor's corporate network, not on the endpoint device.

2.3. Personnel Security

2.3.1 All Contractor personnel authorized to processed, produced or stored contractual Protected B information must each hold a valid personnel security screening at the Reliability Status level and have a "*need to know*". Contractor's security screening (Reliability Status) must be granted and tracked by CISD.

2.3.2 All Contractor personnel handling contractual sensitive information must be provided a training/briefing session coordinated and delivered by the Company Security Officer (CSO) or by the Alternate CSO (ACSO). This training must make reference to the Industrial Security Manual (ISM) and other security publications as determined by the PA.

2.3.3 No foreign national can have the capability to affect the Confidentiality, Integrity and Availability of the data without a valid personnel security screening at the Reliability Status level and the prior approval from the CISD International section and the PA.

2.3.4 Access to the zone where contractual information is being processed, produced and/or stored is prohibited to visitors, personnel not holding a valid personnel security screening at the Reliability Status level and personnel not previously authorised unless escorted at all times by an authorised Contractor.

2.4. Procedural Security

2.4.1 The Contractor must create System IT Security Orders and Standard Operating Procedures (SOPs) specifying, as a minimum, roles and responsibilities, access management, acceptable use, and incident management as it relates to the operation and maintenance of the OMS IS.

2.4.2 All personnel having access to the OMS must read the System IT Security Orders and sign a user agreement form.

2.4.3 The OMS IS must be administered and be maintained internally by individual(s) possessing, at a minimum, valid personnel security screening at the Reliability Status level.

2.4.4 The Contractor must continually monitor its overall security posture including physical, personnel, procedural, information, and IT security, and inform CISD and the PA of any changes that could potentially impact the security of the contractual information.

2.5. Information Security

2.5.1 Contractual information must be exchanged between the PA and all levels of Contractor/Sub-Contractor companies using hard copy documents, IT media, and/or an approved IT link. Hard copy documents and IT media must be handled and transported in accordance with Government of Canada guidelines (RCMP G1-009 "Operational Security Standard on Physical Security").

2.5.2 All hard copy documents and other media must be marked with the appropriate security designation or classification and be afforded a unique identifier to ensure positive control and tracking.

2.5.3 All hard copy documents and IT media must be packaged appropriately and transmitted with a covering letter and a transmittal form or circulation slip marked to indicate the highest level of designation or classification of the attachments as stated in the Contracts' Security Requirements Check List (SRCL) as well as the date of transmission, the document unique identifier, the originator, and the destination.

2.5.4 All contractual information must be segregated from other contractual and corporate information in a way which allows all contractual information to be immediately security wiped upon request from CISD or the PA.

2.5.5 Contractual Protected B information cannot be safeguarded on company`s workstations. It must be safeguarded onto a server dedicated to the OMS IS and must not be stored using external "cloud" technology.

2.5.6 IT links are not authorized between the contractor and any level of sub-contractors. The IT link between DND and the OMS IS must be inspected and be validated by CISD.

2.5.7 IT Connections are not authorized between the OMS IS and any other network, system, or equipment unless CISD and the PA have been made aware and have authorised it. An additional IT security inspection may be required to validate and authorize the IT connection.

2.5.8 The Contractor must use CSE approved encryption technology to ensure the contractual information's confidentiality, integrity, authentication, and non-repudiation. Encryption will be used to protect the contractual information during transport via IT Link and user session. At a minimum, Protected B information must be encrypted using 128-bit encryption.

3. Minimum IT Security Requirements

3.1. IT Security Policy Compliance and Monitoring

3.1.1 On a frequency and schedule to be determined by the DND ITSC, DND retains the right to conduct inspections of the Contractor's facility to ensure compliance with the IT Security Requirements herein as well as the Government of Canada standards and policies with respect to the prevention, detection, response, and recovery requirements as depicted in the TBS Operational Security Standard: Management of Information Technology Security (MITS).

3.2. IT Equipment

3.2.1 A list of all equipment forming the OMS IS must be maintained by the Contractor. The list of equipment must contain, but not limited to, equipment description, quantity, make, and model. If requested, the list of equipment must be made available to CISD and the PA.

3.2.2 The contractor must inform CISD and the PA of any major change to the OMS IT equipment.

3.3. IT System Configuration

3.3.1 The equipment used to process, produce and/or store the contractual information must consist of Commercial off the Shelf (COTS) equipment and must be labelled commensurate with the contractual information sensitivity Protected B level.

3.3.2 The OMS IS must be configured as a segment of the company`s corporate network. As the OMS IS will be configured as a segment of the Contractor's corporate network, the Contractor must segregate its corporate network into IT security zones and implement perimeter defence and network security safeguards. The OMS IS/zone must be segregated from the company's corporate network via firewall. The firewall must be configured to block access to the OMS IS/zone to all information and processes that are not absolutely required for the operation of the OMS IS. Access to the OMS IS/zone must be limited to authorized personnel only. CSE provides the ITSG-38 and ITSG-22 guidelines addressing network zoning. Network perimeter defence safeguards (e.g. firewalls, routers, etc.) must be used on the company's corporate network.

3.3.3 The OMS IS/zone must contain at least one server dedicated to the safeguard of all OMS Protected B information.

3.3.4 Details on the OMS IS/zone including the segregation methodology (i.e. topology diagram and other documents as deemed necessary) must be provided to CISD and the PA for evaluation. The topology diagram must consist of a high level system design and include any IT links to other entities and/or connections to other networks/systems.

3.3.5 All equipment interconnectivity must be using cat-5 or cat-6 cable, which must be identifiable from the corporate system wiring, and must be controlled and be monitored to prevent inadvertent or deliberate connection to any unauthorised equipment, network, or infrastructure.

3.3.7 The OMS IS must operate on a supported Operating System (OS). OS security patches must be updated regularly; at least on a monthly basis. The OS must be configured to disable unnecessary processes and ports. The OMS IS SOP must identify the frequency and the method used to update the OS security patches and provide details on the OS configuration.

3.3.8 A supported antivirus application must be installed and be operational on the OMS IS. The antivirus definition files must be updated regularly; at least on a monthly basis. The antivirus application must be configured to automatically scan the OMS IS at power-on or on a set interval. Every new file introduced onto the OMS IS must be scanned for viruses. The OMS IS SOP must identify the frequency and the method used to update its definition files as well as the configuration of the antivirus application.

3.3.9 Only applications required by the Contract must be installed on the OMS IS/zone. Application patches must be kept up to date and be managed through a defined configuration management process. The OMS IS SOP must list every installed application and identify the application patch management process.

3.3.10 OS log files must be active and be reviewed at least on a monthly basis. The review must consist of, but not be limited to, unsuccessful login attempts, unauthorised changes to the system hardware/firmware/software, unusual system behaviour, unplanned disruption of systems/services, system errors, etc. Only system administrators must be allowed to modify or delete log files. The OMS IS SOP must identify the frequency and the method used to review OS log files.

3.3.11. The use of wireless capabilities on the OMS IS is authorized and the Contractor must establish usage restrictions (access enforcement mechanisms) and implement configuration/connection measures to control the wireless emanations and prevent unauthorized wireless access to Contractual information. The OMS IS must be protected by using authentication of user and wireless device and WPA 2 encryption. Modification of the wireless setting must not be authorized at the user level (limited privileges).

3.4. Authorization and Access Control

3.4.1 The Contractor must provide the PA with a list of all individuals who have access to the contractual information. The list must also indicate the type of account set for each user.

3.4.2 Specific user accounts for company`s employees and DND personnel must be created for each user. Three types of accounts must be created for DND personnel: DND OMS

Administrators, Supply Technician Administrators and Authorized DND Members and Units. The DND OMS Administrators and Supply Technician Administrators will access the OMS IS via an IT Link while the Authorized DND Members and Units (also identified as clients) will access the OMS IS via a User web portal. User accounts must never be shared.

3.4.3 There are five user groups that will utilize the OMS which will require one of the three types of accounts. Each authorized DND Member and Unit must be linked to one of the five (5) user groups. The user groups are as following:

3.4.2.1 Regular and Primary Reserve Force Members;
3.4.2.2 Civilian Firefighters;
3.4.2.3 Canadian Rangers;
3.4.2.4 Canadian Cadet Organization; and
3.4.2.5 Junior Canadian Rangers.

3.4.4 Specific administrator accounts must be created for each system administrator. If an administrator is also required to operate the OMS IS, a separate user account must be created for his/her operation of the system. There must be no generic account on the OMS IS.

3.4.5 User accounts (all accounts other than administrator accounts) must be configured for limited privileges and must allow access only to files and folder required by the users to perform their duties.

3.4.6 Every account must be protected by a password. The passwords must never be shared, consist of at least 8 characters and be composed of a combination of a minimum of three of the following: upper case, lower case, numerical and special character. Passwords must be changed at first login and subsequently, every 90 days. The OS remember option must be disabled, and the last 10 password changes be remembered.

3.4.7 System default administrator passwords must be changed. The new administrator password must be written and be placed in a sealed envelope. The envelope must be safeguarded commensurate with the highest level of contractual information, Protected B, and be locked in an approved lockable container.

3.4.8 The OMS IS SOP must include an Authorization and Access Control process depicting the user addition and removal process.

3.5. IT Media

3.5.1 Every IT media (i.e. memory sticks), used to process, produce and/or store contractual information must be dedicated to this Contract only and be encrypted.

3.5.2 Every IT media must be afforded a unique identifier to ensure positive control and tracking.

3.5.3 Every IT media must be identified and itemized by Designation or Classification, release ability caveat, model and serial number (if applicable). A list of all IT media, must be maintained by the Contractor. The list of IT media must contain, but not be limited to, media description (CD/DVD, Memory stick ...), serial number if applicable, and unique identifier. If requested, the list of IT media must be made available to CISD and the PA.

3.5.4 Every IT media must be labelled. The label must contain the highest level of information sensitivity (Protected B) it contains, the Contract number and the IT media unique number. If a label cannot be affixed directly on the IT media (i.e. memory sticks), the label must be attached to it using a string or other means.

3.5.5 All IT media, must be safeguarded commensurate with the contractual information sensitivity level (Protected B). When not being used, all IT media (including failed, life cycled and longer required media) must be locked.

3.5.6 The location of all IT media must be controlled via the use of a log registry/tracking. The "IT media registry" must contain, but not be limited to, the media description, unique identifier, the date it was removed from and returned to the approved container, and the initials of the individual who took the media.

3.5.7 In the event that equipment requires maintenance, support or replacement, no IT media containing contractual information must be given or be made available to an outside vendor or service provider.

3.5.8 Throughout the duration of the Contract, IT media that failed, is being life cycled, or is no longer required, must be disposed of in accordance with the "Disposal" section of this document.

3.6. Document Printing / Reproduction

3.6.1 The Contractor is authorized to print and/or reproduce contractual sensitive documents within the Contractor's premises.

3.6.2 Printers, plotters, scanners, and/or Multi-Function Devices (MFD) used on Contract W8486-174014 can be equipped with internal hard drives but must be segregated from the corporate network (be within the OMS IS/zone).

3.6.3 The use of MFD is authorized if connected only to the OMS IS. Connection to other devices, network or telephone line is strictly prohibited.

3.6.4 For the maintenance and disposal of printers, plotters, scanners and/or MFD, instructions provided in the "Disposal" section herein must be applied.

3.7. Recovery

3.7.1 The contractual information must be backed-up regularly (at least once a week) and be safeguarded at a remote location. If the Contractor does not have a remote location to safeguard the backups, arrangements can be made with the PA. If backups are safeguarded with another Contractor, CISD and the PA must be informed, validate, and authorise the initiative. The OMS IS SOP must include details on the back-up frequency, methodology and storage.

3.7.2 The Contractor must elaborate and document a system disaster recovery plan. The OMS IS SOP must include details on the recovery, restoration, tests frequency, and methodology.

3.8. Disposal

3.8.1 The disposal of IT media (media that failed, is being life cycled or is no longer required), including all hard drives, used on Contract W8486-174014 must be authorized in advance by the PA and must be documented/tracked. The local disposal of IT media is prohibited.

3.8.2 The disposal of IT media must be tracked via the use of a certificate of destruction (DND PA will provide template) and a document Transit and receipt form (DND PA will provide template). The contractor must retain a copy of every IT disposal evidence document and if requested, must make the evidence available to CISD and the DND PA.

3.8.3 All IT media including workstation and server hard drives, containing contractual information must be given to the PA at the end of the Contract.

3.8.4 The following process must be applied prior to removing printers, plotters, scanners and/or Multi-Function Devices (MFD) used on Contract W8486-174014 for maintenance or disposal:

3.8.4.1 If the equipment contains an internal/external hard drive or any other non-volatile memory device, the hard drive and/or non-volatile memory must be removed and be disposed of as indicated above.

3.8.4.2 Volatile Memory (RAM, DRAM, SRAM) must be sanitize by removing all power for 24 hours. Ensure there is no internal power to the memory (e.g. internal batteries).
NOTE: If there is doubt concerning the removal of all internal power to Volatile Memory in highly sensitive equipment that is being decommissioned, consider removing the Volatile Memory (RAM, DRAM, SRAM).

3.8.4.3 Any stickers or security markings on the device must be removed.

Department of National Defence (DND)

Information Technology Security Requirements

Connectivity Criteria

For

Contract W8486-174014

RELEASE HISTORY

Serial	Date Release	Version	Amendments Details
1	Oct 2018	1.0	Initial Draft

SYSTEMS SECURITY ENGINEERING: AN INTEGRATED APPROACH TO BUILDING TRUSTWORTHY RESILIENT SYSTEMS

1. INTRODUCTION 20

2. MANDATORY PREREQUISITES 20

2.1 IT SYSTEM DESCRIPTION 20

3. DATA LINK ..... ERROR! BOOKMARK NOT DEFINED.

1. Introduction

1.1 This document outlines the Information Technology (IT) Security requirements for the Department of National Defence's (DND) Contract W8486-174014 for establishing IT links between DND and Contractor to process, produce and/or store contractual information up to and including the level of Protected B.
The scope of this document is to state the minimum Connectivity Criteria required to transfer electronic information to and from the Order Management System (OMS) in order that the process be approved by the Canadian Industrial Security Directorate (CISD), Public Services & Procurement Canada (PSPC) and the DND IT Security Coordinator (ITSC).

1.2 As contract W8486-174014 will require online data transfer, there is a need for an additional level of IT Security to ensure that data is not compromised (disclosed, interrupted, modified, destructed, and removed). The Connectivity Criteria are intended to protect not only the OMS but also, any other IS receiving information from the web-based OMS.

2. Mandatory Prerequisites

2.1 IT System Description

2.1.1 The OMS must be used exclusively for DND's purpose and must be clearly identified as the Canadian Armed Forces Non-Operational Clothing and Footwear Order Management System on the first page of the website.

2.1.2 The transfer of electronic data into the OMS is only allowed from an IS of equivalent sensitivity level, or lower. The IT link must be inspected and be authorized to operate by CISD.

2.1.3 The OMS IS must consist of a segregated segment of the corporate network and be composed of at least one server and workstations dedicated to the OMS IS. Remote devices which will be used for Mobile computing / Teleworking must be connected to the segregated network segment via secure thin client connection using approved VPN communication encryption.

The IT link to the OMS IS must be established using standard internet browser or the Defence Information Network (DIN).

3. DATA LINK

3.1 The transfer of electronic data shall be performed as per the following procedure:

3.1.1 The OMS will be accessed by DND personnel in two different ways:

3.1.1.1 Via an IT Link used by DND OMS Administrators and Supply Technician Administrators; and

3.1.1.2 Via a secured web portal for the Authorized DND Members and Units (also identified as clients).

3.1.2 The electronic data related to DND OMS Administrator and DND OMS Supply Administrators must be transmitted between DND and Contractor via IT links using standard internet browser. The IT link must be inspected and be validated by CISD. IT links are not authorized between the contractor and any sub-contractors.

3.1.2.1 The IT link must be owned and be controlled by the contractor and must be secured via the use of at least 128-bit encryption.

3.1.3 The electronic data transfer will be controlled by the Contractor using active OS logs reviewed at least on a monthly basis. The review must consist of but not be limited to: failed login attempts, online ordering activity, unusual behaviour, system errors, etc.

3.1.4 Specific accounts must be created for each DND OMS Administrators, Supply Technician Administrators, and Authorized DND Members and Units.

3.1.5 Every user account must be protected by user name and password; be configured for limited privileges and allowed access only to data required by the users to perform their duties.

3.1.6 Account permissions for DND OMS Administrators and Supply Technician Administrators must be limited to the OMS IS only.