Department of National Defence (DND)

Information Technology (IT) Security Requirements Document

for

Contract W8482-168150

Protected B Information System (IS)

RELEASE HISTORY

VERSION	AMENDMENT DATE	AMENDMENT DETAILS	AMENDED BY
1.0	27/09/2019	Initial draft	R. Mongeon
1.1	21/10/2019	DIM Secur changes from 18 & 21 Oct 2019 implemented	R. Mongeon

TABLE OF CONTENTS

1. INTRODUCTION

1.1 This "Contract W8482-168150 Protected B IT Security Requirements Document" is being provided in accordance with the instructions for completion of Part C, Section 11.d of the Treasury Board Secretariat (TBS) Form 350-103 which states:

> "Will the supplier be required to use its IT systems to electronically process and/or produce or store PROTECTED and/or CLASSIFIED information and/or data? If Yes,. . . The client department and/or organization will be required to specify the IT security requirements for this procurement in a separate technical document. . ."

1.2 This document outlines the Department of National Defence's (DND's) IT security requirements for the electronic processing, production, and/or storage of this contract's Proprietary Information up to and including the level of Protected B.

1.3 Throughout this document the term "Proprietary Information" is defined as "any Protected (A and B) information provided or generated pursuant to this contract, regardless of form or type, including but not limited to scientific, technical, business and/or financial information, whether or not it is included in the Public Services and Procurement Canada (PSPC) Controlled Goods Program." Additional information on the PSPC Controlled Goods Program is available on the internet from "Controlled Goods Regulations (SOR/2001-32)" at https://laws-lois.justice.gc.ca/eng/regulations/SOR-2001-32/ and by email to dmc-cgd@tpsgc-pwgsc.gc.ca. For this contract, the contractor will require access to Controlled Goods.

1.4 In the event that the Information System (IS) used to electronically process, produce and/or store this Proprietary Information is required to electronically connect to DND's infrastructure (Security Requirements Check List (SRCL) Part C, Section 11.e is checked as "YES"), a separate IT Link "Connectivity Criteria" document will be completed by the Project Officer (PO) for the DND Project Management Office (PMO) and will require validation and authorization from Canadian Industrial Security Directorate (CISD).

1.5 Security is based upon layers of protection; in order for IT security requirements to effectively safeguard information they must be preceded and supported by other aspects of security and their associated policies. Contracted efforts should be preceded by the implementation of physical, personnel, procedural, information, and IT Security safeguards.

1.6 Additional security information is available on the internet from the Canadian Industrial Security Directorate (CISD) of Public Services and Procurement Canada (PSPC), the Communications Security Establishment (CSE), the Canadian Centre for Cyber Security (Cyber Centre), and the Royal Canadian Mounted Police (RCMP).

2. MANDATORY PREREQUISITES

2.1 PSPC Validation

2.1.1 The application of the IT security 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/or store Information up to and including Protected B information. Validation must be provided by PSPC/CISD.

2.1.2 The contractor must inform CISD and the DND PO of all physical sites where Proprietary Information will be processed, produced and/or stored (e.g. any applicable main and/or alternate contractor offices, construction sites, back-up storage locations, partners, all levels of sub-contractors offices, etc.). The contractor must inform the DND PO and officially register with CISD any partners and all levels of partnership and sub-contractors involved in this contract.

2.1.3 Every site used to electronically process, produce and/or store this contract's Proprietary Information must be granted a Facility Security Clearance (FSC) as well as either a Designated Organization Screening (DOS) or a Document Safeguarding Capability (DSC), as applicable. Every site must also be cleared by CISD prior to being authorized to electronically process, produce and/or store Proprietary Information.

2.2 Physical Security

2.2.1 Processing, production and/or storage of this contract's Proprietary Information must only be performed in facilities which have been authorized by CISD. All data must be processed, produced and/or stored in a secure manner that prevents unauthorized viewing, access, or manipulation.

2.2.2 In accordance with the RCMP's "*G1-026 Guide to the Application of Operations*", the IS (identified herein as the W8482-168150 Protected B IS) will be installed and operated in an Operations zone or in a temporary Operations zone.

2.2.3 Processing, production and/or storage of Proprietary Information must not be performed outside Canada.

2.2.4 Mobile computing/teleworking involving Proprietary Information may be authorized under this contract if required. 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. Safeguards must meet the requirements of CSE " ITSAP.10.016 - Telework Security Issues".

2.3 Personnel Security

2.3.1 All contractor personnel who have access to any Proprietary Information must:

2.3.1.1 hold - at minimum - a valid SECRET security screening level which must be granted and be tracked by CISD;

2.3.1.2 be assigned system privileges on the criteria of least privilege; this means applying the most restrictive set of privileges and the need-to-know principle (i.e. limiting access to information only to those whose duties require such access) necessary for the performance of authorized tasks.

2.3.2 No visitors, foreign nationals or unauthorized personnel shall have access to the Proprietary Information, the W8482-168150 PROTECTED B IS or the zone where the Proprietary

Information is being processed, produced and/or stored unless they possess a valid SECRET security screening level and are escorted by an authorized contractor employee.

2.3.3 All contractor personnel handling Proprietary Information must be provided training and/or a briefing session coordinated and delivered by the CSO or the ACSO. This training must, at minimum, make reference to the Government of Canada (GC) "Industrial Security Manual" (ISM) and other security information as determined by the DND PO as well as the IT Security Orders and Standard Operating Procedures (SOP) for the W8482-168150 PROTECTED B IS.

2.4 Procedural Security

2.4.1 The contractor must create System IT Security Orders and SOPs relating to the operation and maintenance of the W8482-168150 PROTECTED B IS. These documents must - at minimum - address:

2.4.1.1 roles and responsibilities (e.g. CSO, technical authority, and/or system administrator(s) for the IS);

2.4.1.2 access management for the Operations zone and the IS;

2.4.1.3 acceptable use of the IS;

2.4.1.4 incident management procedures; and

2.4.1.5 any other subject identified in this document.

2.4.2 All personnel having access to the IS must read the System IT Security Orders and sign an associated User Agreement Form, as produced and tracked by the CSO or ACSO. All changes to the System IT Security Orders, SOPs and/or User Agreement Form must be promulgated to all personnel having access to the IS.

2.4.3 The IS must be administered and maintained internally by individual(s) possessing - at minimum - a valid SECRET security screening level.

2.4.4 The contractor must continually monitor its overall security posture including physical, personnel, procedural, information and IT security. The contractor must inform CISD and the DND PO of any issues that could potentially impact the security of the Proprietary Information or the IS.

2.5 Information Security

2.5.1 All documents containing Proprietary Information must be marked with the appropriate security level (of the information contained in the document) and be afforded a unique identifier to ensure positive control and tracking.

2.5.2 The contractor must protect the security of the Proprietary Information at rest through physical and/or IT security measures:

2.5.2.1 When unattended, all hardcopy containing Proprietary Information (e.g. paper printouts, etc.) must be physically locked in approved secure containers.

2.5.2.2 When unattended all removable IT media used to process, produce and/or store Proprietary Information must be physically locked in approved secure containers or encrypted using GC-approved encryption technology appropriate for the sensitivity level of the Proprietary Information.

2.5.2.3 Only contractor personnel authorized to have access to the Proprietary Information will have the ability to unencrypt electronic documents and/or have access to the key/combination for the approved secure container(s).

2.5.3 When exchanging Proprietary Information between DND and all levels of contractors/sub-contractors via hard copy and/or removable IT media, all hard copy documents and removable IT media must be handled and transported/transmitted in accordance with GC guidelines as depicted in the ISM or the RCMP's "*G1-009 Transport and Transmittal of Protected and Classified Information*". When transported/transmitted, all electronic media must be encrypted using GC encryption technology approved for the sensitivity level of the information contained in the electronic media.

2.5.4 All hard copy documents and IT media must be packaged appropriately and transported/transmitted with a covering letter as well as a transmittal form or circulation slip which must indicate:

2.5.4.1 the highest sensitivity level of information contained in the media;

2.5.4.2 the date of transport/transmission;

2.5.4.3 the unique identifier for each document/IT media in the package;

2.5.4.4 the name and phone number of the originator;

2.5.4.5 the physical street address of the destination; and

2.5.4.6 the name and phone number of the recipient.

2.5.5 Exchange of Proprietary Information with partners, sub-contractors or DND can be done via authorized IT links. These IT links must first be validated, inspected, and authorized by CISD as well as recognized and authorized by the DND IT Security Authority and the DND PO.

2.5.6 All Proprietary Information (e.g. hard copy documents, IT media, and electronic documents, etc.) must be segregated from other contractual and corporate information in a way that allows all Proprietary Information to be securely destroyed or wiped, immediately upon request from CISD or the DND PO as indicated in the Cyber Centre's publication "*IT Media Sanitization (ITSP.40.006)*".

2.5.7 The contractor is ultimately responsible for ensuring that all security requirements and all relevant and/or associated security documentation relating to this contract are provided to the contractor's partners and all levels of sub-contractors.

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 IT Security Authority, DND retains the right to conduct inspections of every contractor's facility involved in this contract to ensure compliance with the IT Security requirements herein as well as compliance with GC standards and policies concerning the prevention, detection, response, and recovery requirements.

3.2 IT System Configuration

3.2.1 Basic system configuration: The anticipated basic system configuration will be a segment of the contractor's corporate network meeting Protected B requirements.

3.2.2 The W8482-168150 Protected B IS can be configured as a closed LAN or as a segment of the contractor's corporate network, meeting Protected B requirements.

3.2.3 The equipment used to process, produce and/or store the Proprietary Information can consist of COTS equipment and must be labelled commensurate with the highest sensitivity level of Proprietary Information to be processed on the equipment.

3.2.4 If 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. CSE and the Cyber Centre provide guidelines on this specific subject; see "*Network Security Zoning - Design Considerations for Placement of Services within Zones (ITSG-38)*" and "*Baseline Security Requirements for Network Security Zones in the Government of Canada (ITSG-22)*". Details on segregation methodology (i.e. topology diagram and other documents as deemed necessary) must be provided to CISD and the DND PO for evaluation. The contractor must also implement perimeter defence and network security safeguards for the IS to negotiate all traffic and to protect servers that are externally accessible.

3.2.5 Processing equipment must be configured with internal hard drives. Examples of processing equipment for this IS include workstations (e.g. PCs, laptops, tablets, etc.), servers, printers, scanners, etc.

3.2.6 Operating System. The IS must operate on a supported Operating System (OS); i.e. the vendor of the OS must be creating and providing current security patches for the OS. OS security patches must be installed regularly, at least monthly. The OS must be configured to disable unnecessary processes, services, and ports. The IS SOP must provide details on the OS configuration and identify the frequency and the method used to update the OS security patches.

3.2.7 Anti-virus/Anti-malware Software. A supported anti-virus/anti-malware application must be installed and operating on all workstations and servers (as applicable). Anti-virus/anti-malware definition files must be updated regularly, at least weekly. The W8482-168150 Protected B IS SOP must provide details on the configuration of the anti-virus application as well as identify the frequency and the method used to update the anti-virus/anti-malware definition files. Configuration of the anti-virus/anti-malware application must:

3.2.7.1 allow only changes made by the system administrator(s);

3.2.7.2 automatically scan all W8482-168150 PROTECTED B IS workstations/servers at power-on or on a set interval, at least weekly;

3.2.7.3 scan - for malicious code - every new file introduced to the IS workstations/servers;

3.2.8 Software and Applications. Only applications required under this contract must be installed on the IS. Application patches must be kept up to date and be managed through a defined configuration management process. The IS SOP must list every installed application and its version, as well as identify the application patch management process.

3.2.9 Logging and Auditing. OS logging must be active and the log files must be reviewed by the W8482-168150 PROTECTED B IS system administrator at least monthly. The review must consist of - but not be limited to - successful logins; unsuccessful login attempts; unauthorized changes to the system hardware, firmware, and software; unusual system behaviour; unplanned disruption(s) of systems and/or services; system errors; etc. Only the system administrator(s) shall be allowed to modify or delete log files and only after being authorized by the CSO or A/CSO. The IS SOP must identify the frequency and the method used to review OS log files.

3.3 IT Equipment

3.3.1 A list of all equipment forming the IS must be maintained by the contractor. This equipment list must contain - at minimum - the equipment's description, make, model, and quantity. If requested, this equipment list must be made available to CISD and the DND PO.

3.3.2 The contractor must inform CISD and the DND PO of any major change(s) to the W8482-168150 PROTECTED B IS IT equipment.

3.3.3 The use of wireless or Wi-Fi capabilities on the IS is strictly prohibited.

3.3.4 The use of "cloud" technology to store Proprietary Information is strictly prohibited.

3.3.5 All equipment interconnectivity must be controlled and monitored to prevent inadvertent or deliberate connection to any unauthorized equipment or infrastructure. (Anticipated to be a segment of existing corporate network).

3.3.6 A topology diagram of the W8482-168150 PROTECTED B IS must be provided, upon request, to CISD and/or the DND PO. The diagram must consist of a high-level system design and include any IT links to other entities and/or connections to other networks and/or systems, where applicable.

3.3.7 Maintenance and disposal of any IT equipment used to process, produce and/or store Proprietary Information (e.g. printers, plotters, scanners, photocopiers and/or Multi-Function Devices (MFDs)/Multi-Function Printer (MFPs), etc.) must follow the instructions provided in the "Disposal" section, below.

3.4 Authorization and Access Control

3.4.1 The contractor must maintain a list of authorized individuals who have access to the IS. This list must be updated whenever there is a change of personnel or an individual's information contained on the list. The list must contain:

3.4.1.1 the individual's name

3.4.1.2 the individual's clearance level; and

3.4.1.3 the type of access (e.g. user, power user, administrator, etc.).

3.4.2 The IS must not contain any:

3.4.2.1 generic accounts,

3.4.2.2 guest accounts,

3.4.2.3 temporary accounts, or

3.4.2.4 shared accounts of any kind.

3.4.3 An individual account must be created for each user. User accounts must be configured for limited privileges and must allow access only to the files and folders required by the user to perform their specific duties.

3.4.4 An individual Administrator account must be created for each system administrator. If an individual requires both administrator access and regular user access, the individual must have two separate accounts on the IS. Administrator accounts must not be used for standard day-to-day operations.

3.4.5 Each account must be protected by a password with an enforced minimum password complexity. The password complexity must include the following:

3.4.5.1 the password must contain a minimum of eight (8) characters;

3.4.5.2 the password must contain three of the following four criteria:

3.4.5.2.1 at least one uppercase letter (A through Z),

3.4.5.2.2 at least one lowercase letter (a through z),

3.4.5.2.3 at least one number (0 through 9), and

3.4.5.2.4 at least one special character (e.g. !, $, #, %);

3.4.5.3 password lifetime restrictions of minimum (1 day) and maximum (90 days);

3.4.5.4 password reuse is prohibited for the previous ten (10) passwords; and

3.4.5.5 the account will lock after four (4) consecutive failed logon attempts.

3.4.6 Any password used to access the IS must:

3.4.6.1 never be shared with anyone;

3.4.6.2 be changed at first login;

3.4.6.3 be changed every 90 days thereafter;

3.4.6.4 be changed whenever there is any suspicion of compromise; and

3.4.6.5 not be saved or remembered by the OS or any application accessed by the OS.

3.4.7 The local administrator password on all workstations/servers forming the IS must be changed; vendor default passwords must not be used. Each time a local administrator password is changed it must be written down and placed in a sealed envelope which has been signed over the flap by the CSO, ACSO or system administrator. The envelope must be safeguarded commensurate with the highest sensitivity level of data processed on the system and it must be locked in an approved container.

3.4.8 All network elements (physical and/or virtual) of the IS must be tracked and be accessible (e.g. via access control list (ACL), Active Directory, etc.) only to authorized personnel.

3.4.9 The IS SOP must include an Authorization and Access Control process depicting the procedures for adding, disabling, and deleting user accounts.

3.5 IT Media

3.5.1 Throughout the duration of this contract, all IT media used to process, produce and/or store Proprietary Information must be disposed of in accordance with the “Disposal” section of this document.

3.5.2 In the event that equipment requires maintenance, support or replacement, **no IT media containing any Proprietary Information** (e.g. internal hard drives, removable IT media, etc.) will be given or made available to any outside vendor, service provider or other unauthorized personnel.

3.5.3 All IT media (e.g. internal hard drives, removable hard drives, external hard drives, CDs/DVDs, USB sticks, etc.) used to process, produce and/or store Proprietary Information must:

3.5.3.1 be dedicated to this contract only;

3.5.3.2 be given a unique identifier to ensure positive control and tracking;

3.5.3.3 be identified and inventoried by:

3.5.3.3.1 the type of media (e.g. CD/DVD, USB stick, etc.);

3.5.3.3.2 the information sensitivity level,

3.5.3.3.3 the release-ability caveat (if applicable), and

3.5.3.3.4 the model and serial number (if applicable);

3.5.3.4 be labelled with:

3.5.3.4.1 the highest sensitivity level of the data it contains,

3.5.3.4.2 the government department (in this case DND),

3.5.3.4.3 the contract number, and

3.5.3.4.4 the IT media's unique identifier.

3.5.4 If a label cannot be affixed directly on the IT media, the label must be attached to the IT media by other means (e.g. string, etc.).

3.5.5 All IT media must be safeguarded commensurate with the highest sensitivity level of the data it contains. When not being used all removable IT media - including failed, life cycled and long-term use media (e.g. backup media, etc.) - must be locked in a secure container approved to the information sensitivity level of the data that it contains.

3.5.6 The location of all removable IT media must be tracked and controlled via the use of a log book. The log book must contain, at minimum:

3.5.6.1 the type of media (e.g. CD/DVD, USB stick, etc.);

3.5.6.2 the IT media's unique identifier;

3.5.6.3 the date and time it was removed;

3.5.6.4 the name or initials of the individual who signed it out;

3.5.6.5 the date and time it was returned; and

3.5.6.6 the name or initials of the individual who returned the media.

3.6 Document Printing and/or Reproduction

3.6.1 The contractor is:

3.6.1.1 authorized to print and/or reproduce any Proprietary Information within the contractor's premises; and

3.6.1.2 not authorized to use external printing and/or reproduction services.

3.6.2 Printers, plotters, scanners, photocopiers and/or MFDs/MFPs used to process Proprietary Information must not be equipped with removable hard drives.

3.6.3 Unless the IS is configured as a segment of the contractor's corporate network, all printers, plotters, scanners, photocopiers and/or MFDs/MFPs must only be connected to the IS. Connection to other devices or networks is strictly prohibited.

3.6.4 The connection of telephone lines to any MFD/MFP used to process Proprietary Information is strictly prohibited.

3.6.5 Reproduction of Proprietary Information must first be approved by the DND PO.

3.7 Recovery

3.7.1 The Proprietary Information must be backed up regularly, at least once a week; and must 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 DND PO. Backups safeguarded by another party must be addressed though a sub-contract. The IS SOP must include details on the back-up frequency, methodology and storage.

3.7.2 The contractor must develop, and document a Disaster Recovery Plan (DRP) for the IS. This DRP must include details on the recovery, restoration, tests frequency, and methodology.

3.8 Disposal

3.8.1 The disposal of all IT media used on this contract - including removable media, internal and external hard drives - must be authorized in advance by the DND PO and must be documented and tracked. This includes for example, IT media that has failed, is being life cycled, is no longer required, etc. If hard drives cannot be removed from devices used to process, produce and/or store Proprietary Information (e.g. tablets, etc.) then the devices must be returned to the DND PO.

3.8.2 Disposal of IT media on-site at the contractor's facility is authorized under the following conditions: Only with permission from the DND PO, disposal must be IAW CSE ITSP 40.006. If the contractor does not have the required disposal means, arrangements can be made with the DND PO for disposal of IT media.

3.8.3 The disposal of IT media must be tracked via the use of a "Certificate of Destruction" (if applicable) and a "Transit and Receipt Form"; the DND PO will provide templates for these documents. The contractor must retain a copy of all IT disposal documents as evidence that the

IT media has been properly disposed of. The contractor must make these IT disposal documents available to CISD and the DND PO upon request.

3.8.4 At the end of the contract all Proprietary Information (hard copies and electronic) must be returned to the DND PO. This includes all paper copies of documents as well as any IT media used to process, produce and/or store Proprietary Information (e.g. internal hard drives (used in workstations, laptops, servers, photocopiers, MFDs/MFPs, etc.); CDs/DVDs; USB sticks; SD cards; external hard drives; etc.). If hard drives cannot be removed from devices used to process, produce and/or store Proprietary Information (e.g. tablets, etc.) then the devices must be returned to the DND PO.

3.8.5 If maintenance and/or disposal of IT equipment is necessary, the following procedures must be applied prior to removing any IT equipment used to process, produce and/or store Proprietary Information; this process applies to all IT equipment containing IT media (e.g. servers, workstations, printers, plotters, scanners, MFDs/MFPs, etc.):

3.8.5.1 All non-volatile memory devices (internal, removable, and external hard drives, etc.) must be removed and be disposed of as indicated in this section

3.8.5.2 Volatile memory (e.g. RAM, DRAM, SRAM, etc.) must be sanitized by removing all power for a minimum of 24 consecutive hours. The contractor must ensure there is no power to the memory (e.g. internal batteries or through connection to another device).

3.8.5.3 Any stickers or security markings on the device - in connection with this contract or the IS - must be removed.