Department of National Defence (DND)

Information Technology Security Requirements

Data Transfer

For

Contract W8482-168150

RELEASE HISTORY

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

1. INTRODUCTION

1.1 This document outlines the Information Technology (IT) Security requirements for the Department of National Defence's (DND) current contract W8482-168150 for the transfer of electronic information between the Information System (identified herein as the W8482-168150 IS used to process, produce and/or store the contractual information up to and including the level of SECRET. The scope of this document is to state the minimum IT Security safeguards required to transfer electronic information to and from the W8482-168150 IS 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 W8482-168150 may require data inputs from untrusted sources, there is a need for an additional level of IT Security to mitigate the possibility of malware infection originating from untrusted sources. These extra steps are intended to protect not only the W8482-168150 IS but also, any other IS receiving information from the W8482-168150 IS. The transfer of all contractual information into the W8482-168150 IS will be required to transition through an Air Gap workstation.

1.3 As a part of selecting contractual IT Security safeguards and processes, Project Leads should carefully consider the impact of the selected IT security safeguards and processes 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 Description

2.1.1 A standalone workstation equipped with an up-to-date approved anti malware must be used for all electronic data transfer into the W8482-168150 IS. The transfer of electronic data into the W8482-168150 IS is only allowed from an IS of equivalent sensitivity level, or lower. The transfer of electronic data from the W8482-168150 IS must be authorized in writing by the DND Project Lead.

2.2 Terminology

2.2.1 The following terminology will be used in this section:

2.2.1.1 Source File is the file being transferred from an IS of equivalent or lower sensitivity level, to the W8482-168150 IS;

2.2.1.2 Source System is the IS with the equivalent or lower data sensitivity level from which, the source file is transferred;

2.2.1.3 Target System is the IS with the highest data sensitivity level, receiving the Source File;

2.2.1.4 Source Transfer Media is the physical media, in this case a dedicated memory stick, used to transfer the Source File from the Source System to the Air Gap workstation; and

2.2.1.5 Target Transfer Media is the physical media, in this case a dedicated memory stick, used to transfer the Source File from the Air Gap workstation to the Target System.

2.2.2 The W8482-168150 IS represents the "Target System".

2.3 IT System Description

2.3.1 The Air Gap workstation must consist of a stand-alone computer with no peripheral equipment other than a monitor, keyboard and mouse.

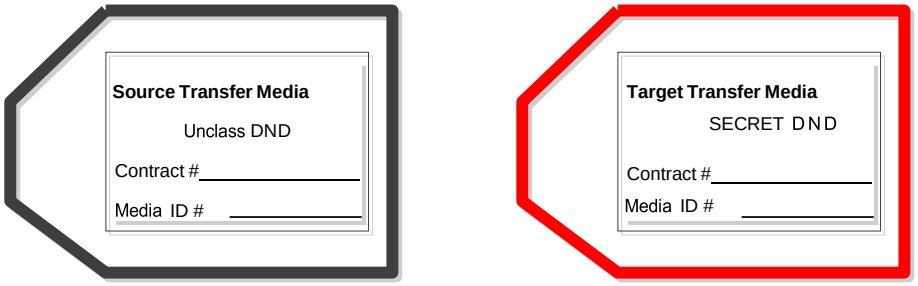
2.3.2 The Air Gap workstation must be equipped with a removable hard drive.

2.3.4 The Air Gap equipment must be labelled as follow:

2.3.4.1 Air Gap workstation and removable hard drive must be labelled as SECRET;

2.3.4.2 The Source Transfer Media must be affixed a large label (4 X 6 inches) with a black edge, containing: **Source Transfer Media**, source data sensitivity level, government department, contract number and the media unique identifier. See example below; and

2.3.4.3 The Target Transfer Media must be affixed a large label (4 X 6 inches) with a red edge, containing: **Target Transfer Media**, target system sensitivity level, government department, contract number and the media unique identifier. See example below.



2.3.5 The Air Gap workstation must be owned by the Contractor, be composed of COTS equipment, be installed / configured / be operational before being inspected by CISD

2.3.6 The Air Gap workstation must be installed and be operated in the **Security** zone or temporary **Security** zone where the W8482-168150 IS is installed but it must be located at least one meter away from any W8482-168150 IS equipment.

2.4 IT System Configuration

2.4.1 The Air Gap workstation 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 configure to disable unnecessary processes, ports and functionalities (i.e. network card and microphone). The update procedure must be documented in the W8482-168150 AIR GAP SOP.

2.4.2 Two different and supported antivirus applications must be installed on the Air Gap workstation. The antivirus definition files must be updated regularly; at least on a monthly basis and confirmed to be up-to-date before proceeding with the verification for malware. The update procedure must be documented in the W8482-168150 AIR GAP SOP.

2.4.3 Specific account(s) must be created for user(s) and administrator(s) responsible to operate and maintain the Air Gap workstation, OS and Antivirus definition files up-to-date. If an administrator is also required to operate the Air Gap workstation, a separate user account must be created for his operation of the Air Gap workstation. Generic accounts are not authorized on the Air Gap workstation.

2.4.4 User accounts must be configured for limited privileges and must be allowed access only to files and folder required by the users to perform their duties.

2.4.5 Every account must be protected by a password. The passwords must: never be shared, consist of at least 8 characters (composed of upper case, lower case and numerical value), be changed at first login, the OS remember option be disabled, be changed every 90 days and the last 10 password changes be remembered.

2.4.6 The system default administrator password must be changed, be written and be placed in a sealed envelope. The envelope must be safeguarded in an approved secure cabinet.

2.4.7 OS logs 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, unusual behaviour, system errors, etc.

2.4.8 The only applications allowed on the Air Gap workstation are the OS and the antivirus application. All other applications shall be deleted/uninstalled.

3 DATA TRANSGFER PROCEDURE

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

3.1.1 The Source file(s) must be copied from the Source System to the Source Transfer Media;

3.1.2 The Source Transfer Media must be connected to the Air Gap workstation and be scanned for malware/viruses using both antivirus applications;

3.1.3 If no virus is detected, the Source File(s) can be copied to the Air Gap workstation hard drive and the Source Transfer Media be removed from the Air Gap workstation;

3.1.4 The Target Transfer Media can now be connected to the Air Gap workstation and the Source File(s) be copied from the Air Gap workstation to the Target Transfer Media. The Source File(s) can now be deleted from the Air Gap workstation hard drive;

3.1.5 The Target Transfer Media must be removed from the Air Gap workstation and can be connected to the Target System (W8482-168150 IS); and

3.1.6 The cleaned Source File(s) can be copied from the Target Transfer Media to the Target System (W8482-168150 IS). Upon the successful data transfer, the Source File(s) must be deleted from the Target Transfer Media and the target Transfer Media removed from the Target System (W8482-168150 IS).

3.2 The transfer procedure must be posted in proximity of the Air Gap workstation.