Communications Security Establishment
Centre de la sécurité des télécommunications

Cross Domain Security Primer

IT Security Bulletin for the Government of Canada

ITSB-120 **January 2016**

1 Introduction

The need to securely access or move information between networks with different security classifications is an ongoing operational necessity within the Government of Canada (GC). Accessing or moving data from one network to another enables business operations, information sharing and decision making.

Any movement of information across networks has the potential of introducing new threats to the networks and jeopardizing the security of the information holdings. While several methods can be considered for moving information across networks (a.k.a. security domains), only Communications Security Establishment (CSE)-approved Cross Domain Solutions (CDS) should be used for information at security levels above Protected B.

2 Purpose

This bulletin will illustrate the two most common types of CDS and identify security considerations associated with them. It is intended for use by executives, business managers and IT stakeholders who are collectively engaged in assessing the information-sharing requirements for their respective department.

3 What are CDS?

CDS are defined as Information Technology (IT) solutions that provide the ability to access or transfer information between two or more security domains. Each solution varies in functionality, components and processes, but enforces security controls to minimize risks and offer benefits such as:

- ✓ Access control mechanisms;
- ✓ Protection against network intrusion; and
- ✓ Data-flow enforcement.

A fully deployed system must be complemented with departmentally developed policies, processes and user training. The two main types of CDS are: **Access CDS** and **Transfer CDS**.

3.1 Access CDS

Access CDS allow users to view information that resides in various security domains with different security policies using a single workstation where appropriate physical and IT security exists. They do not, however, allow information to be transferred between security domains (i.e., cutting and pasting from one window to another is not allowed).

While Access CDS will not solve the proliferation of multiple isolated networks in the GC, it will allow for the consolidation of desktop systems and improved user experience. Desktop consolidation usually results in reduced acquisition and support costs (i.e., total cost of ownership (TOC)), minimized space requirements and reduced power consumption.

3.2 Transfer CDS

Transfer CDS allow users to securely transfer information between different security domains. There are three categories of transfer CDS:

- **High-to-Low Transfer:** In the high-to-low transfer category, users transfer data from a domain with a higher security classification (high domain), to a domain with a lower classification (low domain) through a CDS. An example of this type of transfer would be Access to Information and Privacy (ATIP) requests that can require classified, sensitive or private information to be sanitized before being transferred to an unclassified system.
- **Low-to-High Transfer:** In the low-to-high transfer category, users transfer data from a low domain to a high domain through a CDS. An example of this type of transfer would be a requirement to transfer a weather report from an unclassified system to an operational dashboard.
- **Manual Data Transfer:** Users transfer data manually using removable media such as a USB memory stick, CD-R or DVD. An example of this type of transfer would be a requirement to transfer a software patch or anti-virus update from a removable media device to an isolated security domain.

4 Security Considerations

When attempting information transfers across security domains with different security policies, or when displaying multiple security domains on a single workstation, there are inherent threats, some of which are briefly explained below:

- **Data Leakage:** The primary threat to a high-to-low transfer CDS is data leakage where classified information is unintentionally transferred from a more highly classified security domain to a lower classified security domain.
- **Malicious Code:** The primary threat to a low-to-high data transfer CDS is the proliferation of malicious code or other unauthorized software across security domains.
- **Inappropriate User Behavior:** Some users may decide to circumvent the proper transfer procedures and manually transfer information using removable media, or attempt to use other inappropriate and unauthorized methods to transfer data.

GC Departmental Authorizers are responsible for clearly understanding that while CDS will improve security, there will always be some level of residual risk that must be assessed before they grant security waivers or an Authority to Operate (ATO). This is especially true when moving information is deemed an operational imperative that may outweigh the security risks.

5 Considering Your Requirements

When planning, selecting, or implementing a CDS, it is important to:

- ✓ Assess your business requirements and determine your business needs;
- ✓ Understand your threat and risk environment (threat and risk assessment);
- ✓ Develop strong security and information management (e.g., data tagging) policies, procedures and safeguards; and
- ✓ Identify and understand the current best IT security practices based on operational requirements, and select appropriate security controls.

Implementing a solution that will reduce the risk (to an acceptable level) of transferring data between different security domains requires considering the design and security requirements of the department’s enterprise architecture.

6 Removable Media

Some departments may find that implementing a CDS may not be a viable business decision and that transferring information using removable media may become an operational necessity. Having a robust removable media policy is paramount and highlights multiple steps that must be followed to ensure threats are mitigated, as per ITSB-112 Security Considerations for the Use of Removable Media Devices for Protected C and Classified Information.

7 Contacts and Assistance

CSE recommends following the ITSG-33 IT Security Risk Management: A Lifecycle Approach security risk management framework. Additionally, if your department has identified a CDS requirement based on business needs and would like more detailed information on any aspect of CDS, please contact CSE ITS Client Services.

ITS Client Services
Telephone: (613) 991-7654
E-mail: itsclientservices@cse-cst.gc.ca