Communications Security Establishment
Centre de la sécurité des télécommunications

# Security Considerations for the Use of Removable Media Devices for Protected C and Classified Information

IT Security Bulletin for the Government of Canada

**ITSB-112** **August 2014**

## 1 Purpose

Government of Canada (GC) departments rely on information systems to support their business activities. Many departments and agencies use removable media devices to easily store or share information between computers or networks. However, removable media poses a threat to the GC's information assets due to their small size, portability, storage capacity, and capability to run device-unique applications. Departments and agencies must ensure that removable media devices have adequate safeguards to prevent unauthorized access to GC information.

This bulletin is in support of the Treasury Board of Canada Secretariat (TBS) *Information Technology Policy Implementation Notice 2014-01* (ITPIN: 2014-01). The notice, released in May 2014, describes the risks posed by, and the possible mitigations for, removable media devices that are used to temporarily store GC information. The intended audience for this bulletin includes executives, those responsible for IT security risk management activities, and information system security practitioners.

## 2 Impact

Removable media devices are typically used to temporarily store information or transfer data electronically from one system to another. While data transfers enable collaboration between employees and among departments, the improper use of removable media devices poses significant risks to the confidentiality of departmental information assets. Without proper management of these devices, there is an increased likelihood that GC information could be exposed to unacceptable risks (e.g. loss or theft of a device, a device being used as a means to insert malicious code).

## 3 Mitigation Strategies

When applied together, the following safeguards frame CSE's recommendation of devices for the storage of Protected C and classified information in support of ITPIN 2014-01:

- The device must be encrypted using a Cryptographic Module Validation Program (CMVP) validated module **operating in Federal Information Processing Standards (FIPS) mode**.
- The device must be handled with the same sensitivity as the highest classification of information that has been, is, or will be stored on the device **prior to encryption**. The

device must also be handled with the same sensitivity as the highest classification of network **to which the device has or will be connected**.

# 4 Implementation

Although some aspects for solutions in this domain will be left to departments as risk management decisions, the specification of encryption or other safeguards for the electronic handling of Protected C and classified information is the responsibility of CSE, in accordance with the TBS *Operational Security Standard: Management of Information Technology Security (MITS)*, section 16.4.4.

## 4.1 Cryptographic Security

Devices must be encrypted with a CMVP-validated implementation, operating in FIPS mode only. Validation has not been performed on encryption modules operating outside of FIPS mode. The encryption of any GC information on removable media using CMVP modules outside of FIPS mode is not recommended by CSE. In addition to CMVP-validated solutions, there are also high-assurance (HA) products suitable for handling Protected C and classified information. The use of HA products reduces the number of safeguards required for the storage and handling of information. Further details on HA products can be obtained by contacting comsecclientservices@cse-cst.gc.ca.

## 4.2 Physical Security

Departments must have adequate physical handling policies and procedures in place for Protected C and classified information. For further details concerning marking, storing, and transporting of removable media devices, refer to the Royal Canadian Mounted Police (RCMP) *G1-001: Security Equipment Guide* and *G1-009: Transport and Transmittal of Protected and Classified Information*.

## 4.3 Cross Domain Considerations

GC departments and agencies required to transfer data electronically between two different security domains should always use an authorized Cross-Domain Solution (CDS). However, in the event that a CDS is not available, manual data transfer using removable media may be required. Depending on the classification levels of the networks involved as well as the direction of the transfer, several specific security controls should be considered and implemented as part of a departmental IT policy for manual data transfer. The selection of safeguards is particularly important when transferring data out of classified networks to prevent leakage of classified information, or transferring data into classified networks to prevent the introduction of malware and viruses that could compromise the classified environment.

CSE can provide additional guidance to assist departments to develop a robust CDS policy. For more information, contact itsclientservices@cse-cst.gc.ca.

## 5 Conclusion

It is essential that GC departments implement protective measures to secure the confidentiality, availability and integrity of their IT information and assets. In order for commercial removable media products to satisfy the recommendations of CSE, the devices must be CMVP-validated, operate in FIPS mode, and be handled with the same physical safeguards that are required to protect the information that will be or has been held on the device. For further clarification on this bulletin, or queries on the CMVP and other assured products, contact itsclientservices@cse-cst.gc.ca.

## 6 Contacts and Assistance

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