Communications Security Establishment
Centre de la sécurité des télécommunications

CYBER JOURNAL

EDITION 10 | AUGUST 2016

IN THIS EDITION

PROTECTING CLASSIFIED INFORMATION

In the fall of 2012, CSE published the first edition of the Cyber Journal to further our commitment to providing Information Technology Security advice and guidance to the Government of Canada (GC). It is now four years later, and I am pleased to present the special 10th edition of the Cyber Journal.

As the GC's centre of expertise on cyber security, CSE continues to build upon our relationships with our colleagues across the government to help protect GC networks and the information they contain. It is important that we work together to ensure that GC classified information is protected.

Not all information is created equal, and classified information represents the GC's most valuable and sensitive information. Every day, departments face the risk of their information being compromised. When GC employees accept the privilege of accessing classified information, they are also accepting the responsibilities that accompany this privilege.

Our 10th edition of the Cyber Journal will highlight the importance of protecting classified information by providing insight on the importance of security categorization for "open-government" initiatives, as well as providing key actions departments should take to protect classified information.

Originally signed by

Scott Jones
Deputy Chief, IT Security

cse-cst.gc.ca

Canada

CYBER JOURNAL

10th EDITION

AUGUST 2016

5 TIPS FOR PROTECTING CLASSIFIED INFORMATION

Classified information, if compromised, could reasonably cause injury to the national interest of Canada. Threat actors apply substantial resources and take significant risks to obtain this sensitive information.

Consequently, information systems which process classified information require specialized safeguards that departments must implement to protect their information.

Here are five steps GC departments can take to protect their classified information systems.

1 DEPARTMENTAL SECURITY PLAN

Prioritize and carefully monitor classified information within your department. As part of your Departmental Security Plan (DSP), integrate all aspects of security, including physical, personnel and operational security. In addition, get to know your Departmental Security Officer (DSO).

2 APPLY ITSG-33

Design, build, operate and maintain your classified information systems according to the risk management framework described in ITSG-33.

ITSG-33 Annex 4A provides a starting point for a system security profile supporting SECRET confidentiality, MEDIUM integrity and MEDIUM availability.

Consult CSE early in the development of your classified information systems to ensure that your approach will provide adequate protection.

3 SEGREGATE SENSITIVE INFORMATION

UNCLASSIFIED, designated (i.e., PROTECTED A, B or C) or Internet-connected information systems present a large and attractive attack surface, and expose information to a high risk of compromise.

Process, store or transmit classified information using only appropriately classified systems (e.g., the Canadian Top Secret Network (CTSN) or the GC Secret Infrastructure (GCSI)).

Remember, removing a classification marking from a document does not declassify the information in the document.

4 USE CSE-APPROVED COTS SOLUTIONS

In order to assure that Commercial Off-The-Shelf (COTS) products provide the necessary protection, GC departments should consult CSE to validate any claims by vendors that particular products or solutions are suitable to serve a security function as part of a classified system.

COTS solutions are not all created equally and, alone, they do not provide adequate protection for classified information.

5 REPORT SECURITY INCIDENTS

As identified in Tip #1, report all security incidents as per your DSP. DSOs must report security incidents to the GC Computer Incident Response Team (GC CIRT) at Shared Services Canada (SSC), in accordance with the GC Cyber Security Event Management Plan (GC CSEMP).

Examples of security incidents include those compromises affecting classified information systems, and those where classified information is present on a system of a lower security level.

THE CANADIAN TOP SECRET NETWORK MODERNIZATION PROJECT

The Canadian Security and Intelligence (S&I) community comprises a number of distinct but interconnected communities: intelligence, law enforcement, defence, security and foreign affairs. The efficient and effective functioning of this community relies on the right information getting to the right people securely and at the right time in order to take timely and decisive action.

In 1996, the Mandrake network was stood up to share information at the Top Secret (TS) level across the Canadian S&I community. In 2012, Mandrake was officially renamed the Canadian Top Secret Network (CTSN) and ownership of the network was transferred from the Privy Council Office (PCO) to CSE.

In 2012, Treasury Board of Canada Secretariat (TBS) approved a 5-year CTSN Modernization Project with funding from April 2013 to March 2018. The project is modernizing the CTSN by offering new and improved collaboration, information sharing and security services. The new services will greatly improve communication and collaboration at the TS level both domestically within Canada as well as with our international allies.

If you would like more information on the CTSN or the CTSN Modernization Project please contact: CTSN-client-services@cse-cst.gc.ca.

DID YOU KNOW?

There are 20+ Government of Canada Departments and Agencies in the CTSN community.

CTSN
CANADIAN TOP SECRET NETWORK

CSE'S TOP 10 VIDEOS NOW AVAILABLE!

Visit the ITS Web site to view our new videos and learn more about the first four of the Top 10.

MODERNIZING OUR SECRET INFRASTRUCTURE

Contributed by Shared Services Canada

GC departments are faced with the challenge of communicating classified information securely across the GC enterprise and with other levels of government. To help them meet this challenge, SSC is in the process of transitioning various existing communication solutions to an enterprise-level service referred to as the GC Secret Infrastructure (GCSI). SSC is assessing the current state of legacy secret infrastructures in the GC and planning for their transition into the GCSI.

The establishment of a modern, integrated and secure set of IT solutions is critical to the GC's ability to effectively conduct day-to-day operations and to address threats in an increasingly hostile environment. The table below further articulates the challenges as well as the approach the GCSI program intends to take in order to lead the deployment of accessible, adaptable, and scalable services.

KEY CHALLENGES	SSC APPROACH
Maintain aging and disparate legacy environments	Build one common infrastructure to which all users and applications migrate over time.
Seamlessly deploy diverse types of services	Leverage investments in enterprise data, voice, video services, networks and data centers. Offer integrated, secure, and accessible services.
Respond to stakeholders demands for new applications and partnerships	Increase the flexibility of current offerings. Adapt current solutions to meet requirements.

The planned approach is to augment and expand the GCSI, an existing SECRET-level network for SECRET Canadian Eyes Only (CEO) data, followed by important enhancements and the introduction of new services. These services will require solutions to be integrated that support video, secure voice (classified VoIP, vIPer, etc.), remote access and secure mobile device connectivity. All these services are being developed in collaboration with other partners including PCO, CSE and TBS. The future infrastructure will be hosted by SSC enterprise data centres and will be incorporated into an overall enterprise service strategy.

For additional information on the GCSI, contact SSC at infoforsecret@canada.ca.

SECURITY CATEGORIZATION FOR AN OPEN GOVERNMENT

Contributed by Treasury Board of Canada Secretariat

The GC's current emphasis on openness and transparency, using concepts such as "open-by-default", is intended to better serve the needs of Canadians. While increasing accountability to the public is important, there are risks to being too open. Openness and transparency initiatives have inherent business needs, but they also have security risks that need to be mitigated.

To find the right balance, security categorization activities need to be undertaken. This process identifies the Confidentiality, Integrity, and Availability (CIA) needs of your business activities, and qualitatively or quantitatively categorizes the impact associated with the disruption or compromise of one of these elements. Moreover, security categorization adds valuable intelligence on how to manage the security risks related to business activities and their related system, information, and asset inventories.

From a broader perspective, security categorization also helps with cost-effective security management, effective business continuity planning, and the Security Assessment and Authorization (SA&A) process. It is also a key enabler for open-data and open-information initiatives.

Initiatives to identify information and system resources that can be deemed "open" also create a parallel requirement to identify those that are sensitive and to justify their ongoing protection. In this scenario, security categorization has a dual benefit: it promotes openness and transparency by identifying resources that are non-sensitive in nature, while simultaneously supporting the legislative framework that outlines the principles for maintaining the confidentiality of information, namely the Access to Information Act and the Privacy Act.

> *"Security categorization allows your department to identify and prioritize what measures are reasonable for each business activity".*

When the government makes information and services available to the public and businesses, this also comes with an inherent responsibility to ensure that the integrity of the data is not compromised, and that the information and services remain available. Security categorization allows your department to identify and prioritize what measures are reasonable for each business activity.

Security categorization is fundamental to effective security risk management. From a policy perspective, greater emphasis is needed on assessing business impacts resulting from compromises in terms of the overall value of the business activity, rather than simply the cost of the assets that support it.

For more information, refer to Annex 1 of CSE's ITSG-33 - IT Security Risk Management: A Lifecycle Approach.

GO AHEAD...THIS LINE IS SECURE

Smartphone for Classified (SPfC) is an innovative CSE-developed solution that will enable GC employees to communicate using secure mobile voice, e-mail and instant messaging. SPfC uses readily-available COTS products, which, when properly configured, are capable of securing classified communications up to and including the SECRET level. Using COTS products, rather than government-supplied and developed equipment, offers many advantages such as shorter time to market, user friendliness and ease of operations.

In the spring of 2015, Proof-of-Concept (POC) testing was undertaken and demonstrated sufficient promise. SSC then decided to proceed with a Technical Proof of Service (TPOS) project using UNCLASSIFIED data. The TPOS goals were to evaluate the technical feasibility, verify the operational effectiveness and determine the value of pursuing an operational deployment.

During November 2015, approximately 100 employees from several government departments participated in the TPOS by testing out the functionality. Participants provided positive feedback, and many users commented that if the solution was approved for use, they would use it in their daily operations. The technical feasibility and operational effectiveness were also confirmed.

Work is currently underway to advance the SPfC to an expanded pilot phase wherein a larger group of GC employees, requiring up to SECRET-level communications, will use the phones in their daily working lives within predetermined security parameters. As the solution proves its stability in day-to-day use, the plan is to progressively grow the deployment until it is generally available for use in the GC within a couple of years or less.

NEWLY RELEASED PUBLICATIONS

These are the first two from our new publication series. Stay tuned for more information!

ITSAP.00.001
Using your Mobile Device Securely

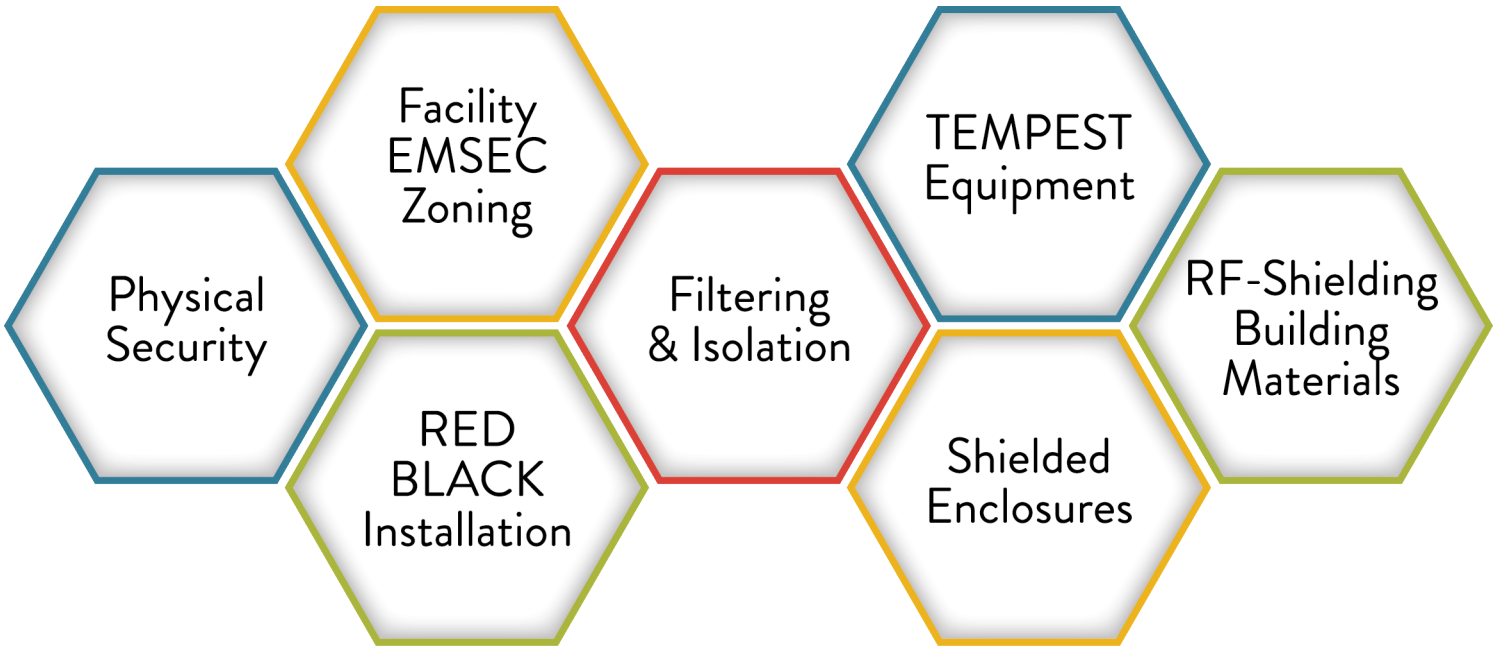
ITSE.80.001
Mobile Security Securing the GC V6

ELECTROMAGNETIC EMISSIONS...SHOULD I BE WORRIED?

Did you know that your IT equipment (e.g., your computers, laptops and printers) may be leaking sensitive information over the air or across signal and power lines that can be intercepted by threat actors?

The computers and electronic equipment we use today radiate electromagnetic (EM) emissions which can contain unintentional traces of the data being processed. If your IT system is processing sensitive or classified data, a motivated threat actor can try to intercept and analyze these emissions in an attempt to reveal the data.

To help protect your data against this kind of threat, CSE has recently published ITSG-11A – Emission Security (EMSEC) Guidance to assist you with the planning, construction and installation of IT systems processing classified information. This document reviews the characteristics of the electromagnetic emissions of IT equipment, and recommends the following seven security controls that can be implemented within your facility to reduce the risk of emission compromise:



EMSEC is just one of the many aspects of security you need to consider when building a secure classified IT system. GC departments need to take a balanced approach in understanding EM related risks and selecting the best cost-effective EMSEC controls to protect classified data.

For more information, please contact ITS Client Services to find out how we can help.

SUPPLY CHAIN INTEGRITY

The Supply Chain Integrity (SCI) process provides additional security measures for equipment, software or services procured by SSC. The SCI process is used to assess the impact of supply chain threats and aims to protect the integrity, availability and confidentiality of Canada's data and communications. The level of review is often dependent on the trust relationship between the vendor and the GC, and assessments are based on the sensitivity of information stored on government networks.

Under Mandate B of Canada's National Defence Act, CSE provides best practices and guidance for all GC departments and agencies on supply chain threats and vulnerabilities. This includes recommendations and mitigation measures against potentially vulnerable technologies used throughout GC networks and IT infrastructure. CSE receives SCI requests from departments and agencies under SSC authority to assist in the acquisition of new equipment and services by providing a second opinion and advising against products with known security issues.

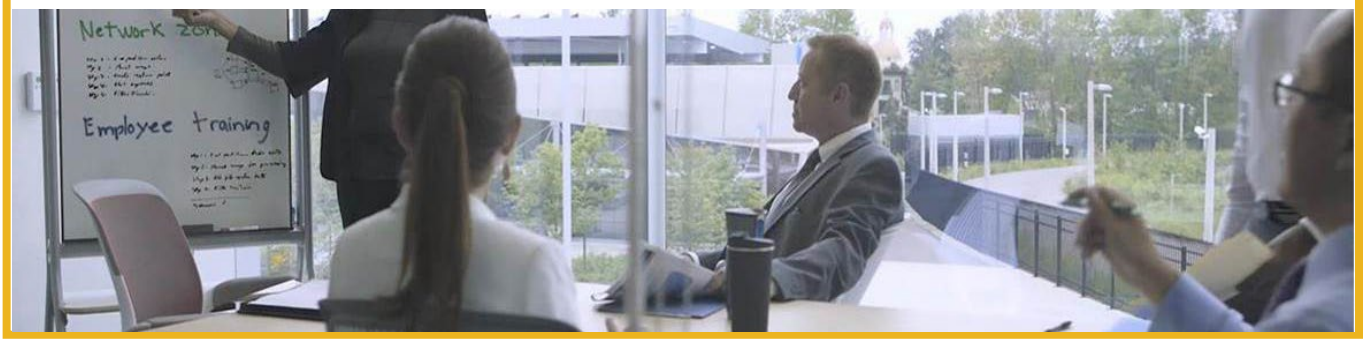
Departments and agencies must be aware of the evolving threats targeting government systems in order to mitigate the supply chain risks to GC equipment and services. Threat actors probe GC networks for exploitable vulnerabilities in order to gain access and disrupt operations crucial to the GC. The SCI process helps secure the supply chain against malicious attacks from sophisticated foreign state actors, hacktivists, criminals and terrorists. CSE's advice and guidance provides an additional layer of defence in the protection of Canada's IT infrastructure and guards government networks against evolving threats.

Additional information can be found at: Supply Chain Technology.

GROUP TRAINING AT YOUR SITE!

CSE's IT Security Learning Centre (ITSLC) works with many Government departments to provide tailored group training solutions. Our courses range from introductory to advanced topics in the areas of cyber/IT security and communications security (COMSEC). Courses such as *COMSEC in the GC*, *Cryptographic Security in the GC and Cyber Security in the GC* are all introductory courses that can be customized and taught to a large audience.

Our knowledgeable staff would be happy to work with you in addressing your specific training needs. To explore customized training options, contact the ITSLC at its-education@cse-cst.gc.ca or 613-991-7110.



NEW ITSLC COURSES

ITSLC 105 INFORMATION SYSTEMS SECURITY IMPLEMENTATION PLAN (ISSIP)

ITSLC 105 explains to participants what the ISSIP is, why it is required and where the ISSIP is situated within the IT Security Risk Management (ITSG-33) process. It describes all the ISSIP activities, and gives participants the ability to complete key ISSIP activities within their GC departments.

Participants will also be able to identify the GC roles that are involved in the ISSIP and their related responsibilities. This course is critical to an effective understanding of cyber/IT system security requirements in basic, medium or high assurance environments.

ITSLC 107 CYBER SECURITY IN THE GC

ITSLC 107 is intended for non-IT security professionals who are in supporting cyber security roles. This course provides participants with a basic comprehension of cyber/IT terminology which will help them apply key security principles in their day-to-day functions.

In addition, participants will be able to describe basic cyber/IT security protection measures and identify the threat context for their GC department. This course will also explain the exploitation cycle and describe in general terms the GC reporting process for cyber/IT security activities.

To register, log into your ITSLC Learning Account.

ABOUT THIS NEWSLETTER

Cyber Journal has been prepared for GC IT practitioners and stakeholders and is published on a periodic basis. This publication reflects the CSE IT Security commitment to share information, advice and guidance with the broader GC community to help departments and agencies better protect themselves from cyber threats. The aim is to highlight key security issues and stimulate discussion about security within your department. In addition, the newsletter profiles key products and services offered by CSE with information on how you can leverage them to help your GC organization. Security awareness throughout an organization is an essential element to improving the GC's security posture. As such, we encourage you to share this information within your organization.

SUBSCRIBE

To be notified of future releases, contact: itsclientservices@cse-cst.gc.ca

CONTACT US

For general advice and security guidance support, contact:

✉ itsclientservices@cse-cst.gc.ca **General Inquiries: (613) 991-7654**

To contact the Cyber Threat Evaluation Centre:

✉ ctec@cse-cst.gc.ca

For planning, support or any issues regarding COMSEC devices, contact COMSEC Client Services:

✉ comsecclientservices@cse-cst.gc.ca

General Inquiries: (613) 991-8495

COMSEC custodians can contact the Crypto Material Assistance Centre (CMAC):

✉ cmac-camc@cse-cst.gc.ca

General Inquiries: (613) 991-8600

For education and training services, contact the IT Security Learning Centre:

✉ its-education@cse-cst.gc.ca

General Inquiries: (613) 991-7110