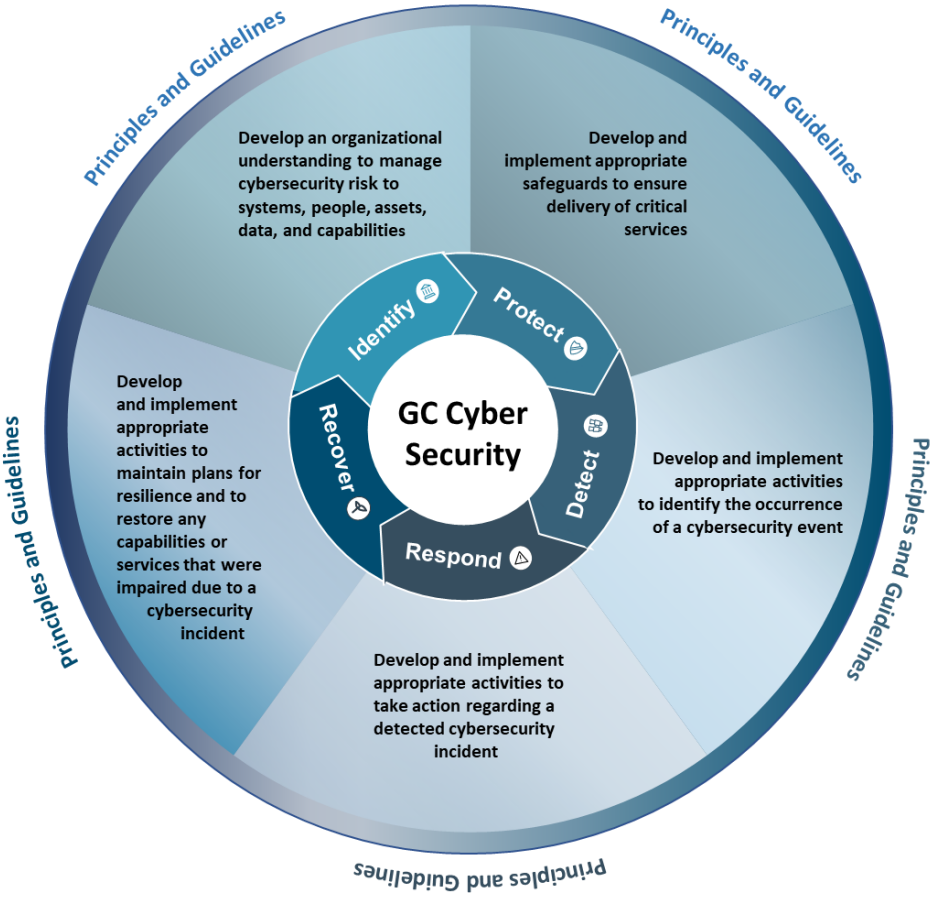
Guide for Cyber Maturity Self-Assessment (CMSA) Tool

Background

As per Section 4.4.4.1 of the Directive on Service and Digital[1], the Designated Official for Cyber Security (DOCS) is responsible for "ensuring that cyber security requirements and appropriate risk-based measures are applied continuously in an **identify, protect, detect, respond, and recover** approach to protect information systems and services."

To that end, a set of GC Cyber Security Management Guidelines has been established to support the DOCS in meeting this requirement.



It is expected that the DOCS work collaboratively[2] with the Departmental Chief Information Officer and Departmental Chief Security Officer in applying these principles and guidelines, with the aim of improving cyber security posture within a department or agency.

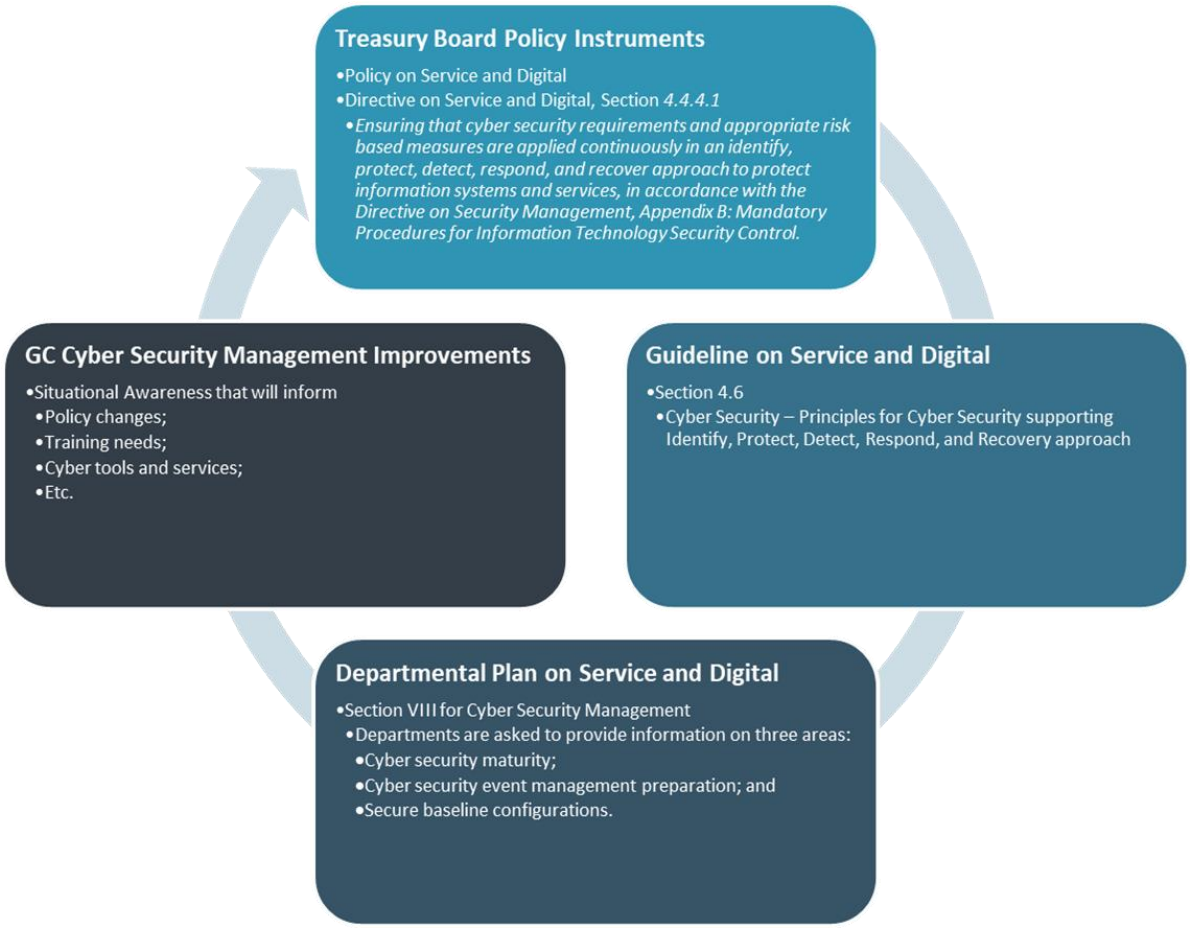
[1] As per the update to the Directive on Service and Digital targeting publication in early 2022.
[2] As per Section 4.4.4 of the Directive on Service and Digital.

Assessing Cyber Maturity

To understand the cyber security maturity posture across the Government of Canada (GC), a methodology to facilitate all GC institutions in assessing their cyber security maturity against recognized best practices has been established.

The GC Cyber Maturity Self-Assessment Tool (CMSA) aligns with the GC Cyber Security Management Guidelines, as depicted below. The goals of the tool are to:

- ensure that enterprise cyber risks are being adequately managed and to identify areas of improvement;
- increase response time to potential risks by ensuring a secure and resilient enterprise infrastructure that enables the trusted delivery of programs and services; and
- reduce the cost and time spent in assessing cyber security maturity through other means (e.g., third party assessors).



How to Access the CMSA Tool

The CMSA tool is hosted in the **Cyber Security Application Portal** of the **TBS Application Portal (TAP)**. Only users who are authenticated via GCpass (MyKey Login) and have been assigned a role within the Cyber Security Application Portal are granted access to the tool.

Roles

There are two roles that are assigned within the CMSA tool:

1. **Designated Official for Cyber Security** (DOCS), and
2. **Departmental Responder**.

The DOCS and Departmental Responder have equal access to the tool where they can: access, create and edit the CMSA report for their organization.

While the Departmental Responder will largely be responsible for responding to the CMSA, the DOCS will have access to the response information in order to review and approve of the GC organization's assessment.

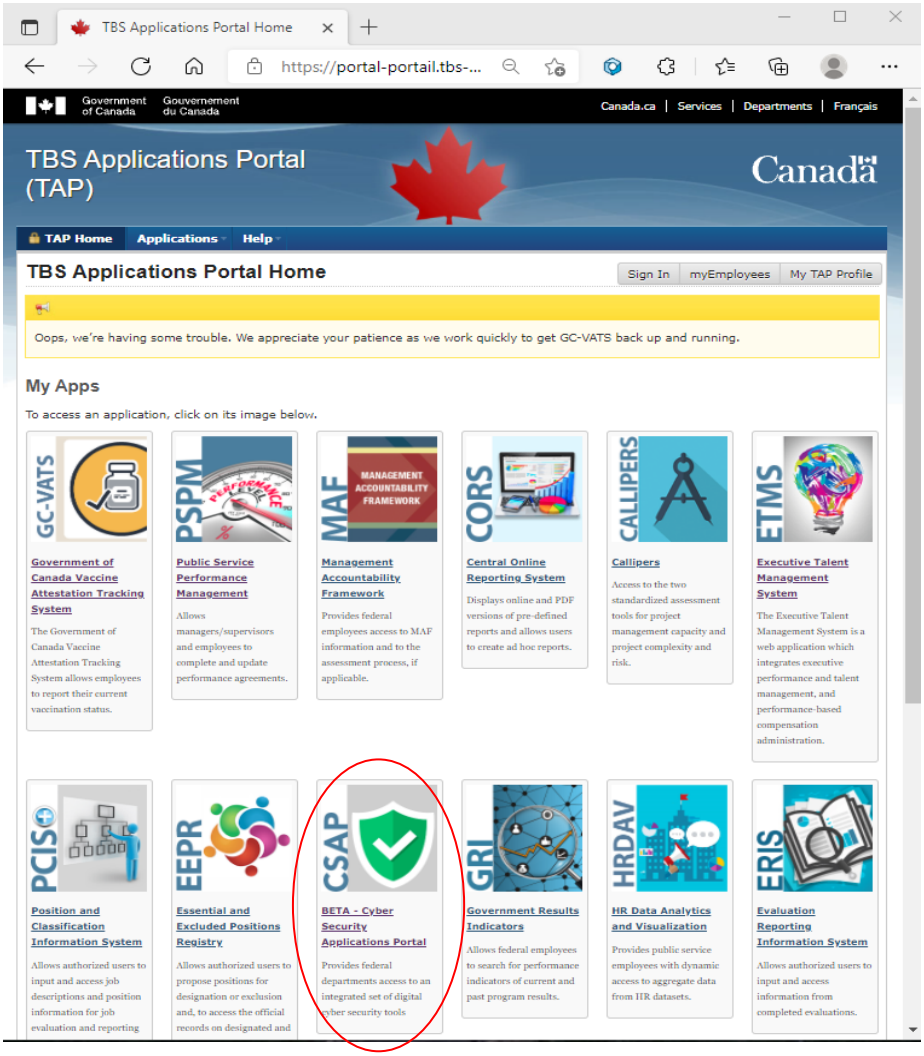
Only TBS has the authority to assign users to a role in the **Cyber Security Application Portal**. Please contact TBS-Cyber Security's DOCS Mailbox to identify and/or modify the DOCS or Departmental Responder roles to ensure representatives have access to the tool.

Steps to Accessing and Completing the Cyber Maturity Self-Assessment

Step 1:

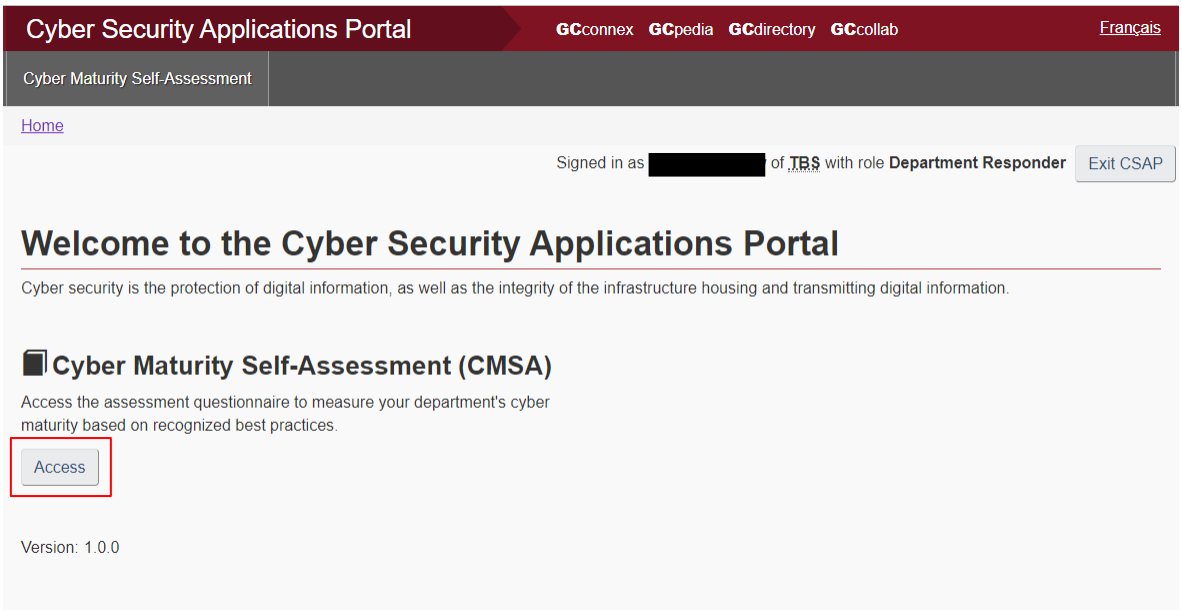
Access the TBS Application Portal at https://portal-portail.tbs-sct.gc.ca/home-eng.aspx.

Select the **Cyber Security Applications Portal** to access the CMSA tool.



Step 2:

Once on the homepage of the Cyber Security Applications Portal, select '**Access**' to access your organization's CMSA questionnaire.

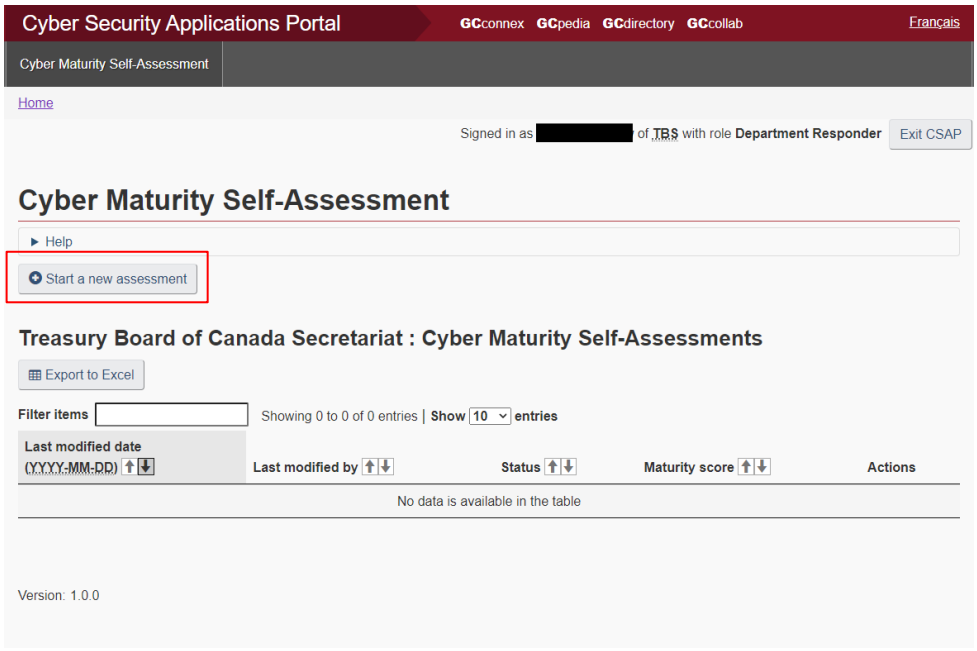


Step 3:

You will now land on your departmental CMSA page, which will identify assessments completed or in progress for your organization.

To begin a new assessment, select '**Start a new assessment**'.

It is not required that an assessment be completed in its entirety at once. You may save your work as you go and edit an existing assessment at any time.



Step 4:

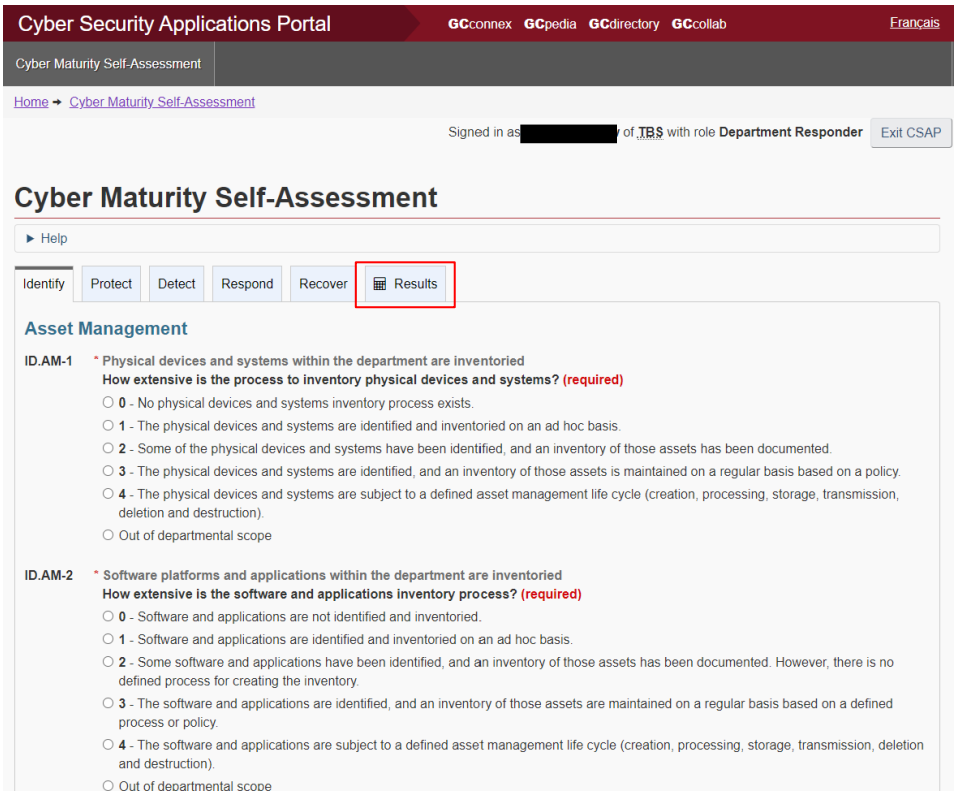
Once a new assessment has been started (or you wish to modify an assessment in progress), you will be brought to a survey that is broken down into five tabs corresponding to the **Cyber Security Management Principles**: 1) **Identify**; 2) **Protect**; 3) **Detect**; 4) **Respond**; and 5) **Recover**.

- *If you would like more information and guidance on the GC Cyber Security Management Principles, we encourage you to check out the GC Cyber Security Management guidelines on GCpedia*.

Departmental Responders must complete the survey by responding to **all** the questions under each of the tabs corresponding to the Cyber Security Management Principles.

Departmental Responders may select '**Out of Departmental Scope**' if the responsibility outlined in the survey question is overseen by another organization. If selected, a comment box will appear requesting that you list the organization responsible.

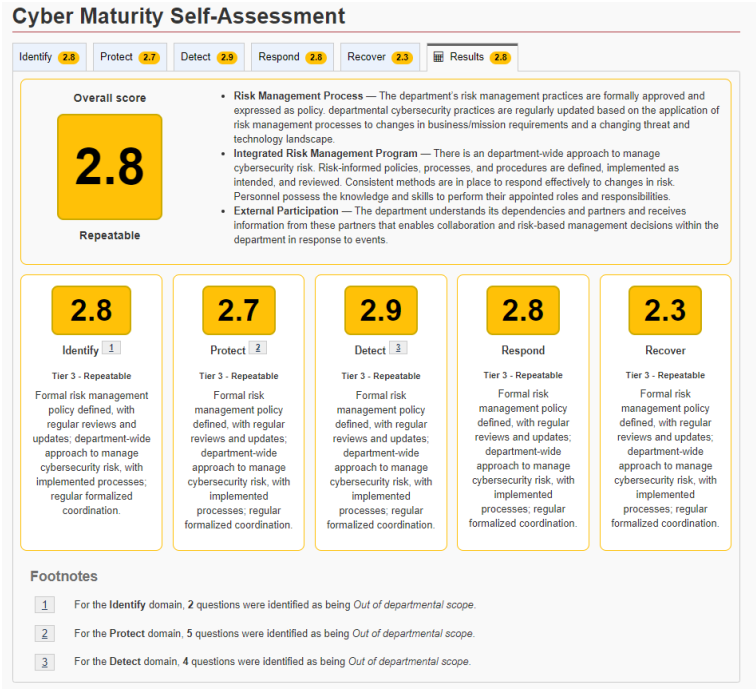
Following the completion of the survey, select '**Save**' at the bottom of the webpage, followed by selecting the '**Results**' tab.



Step 5:

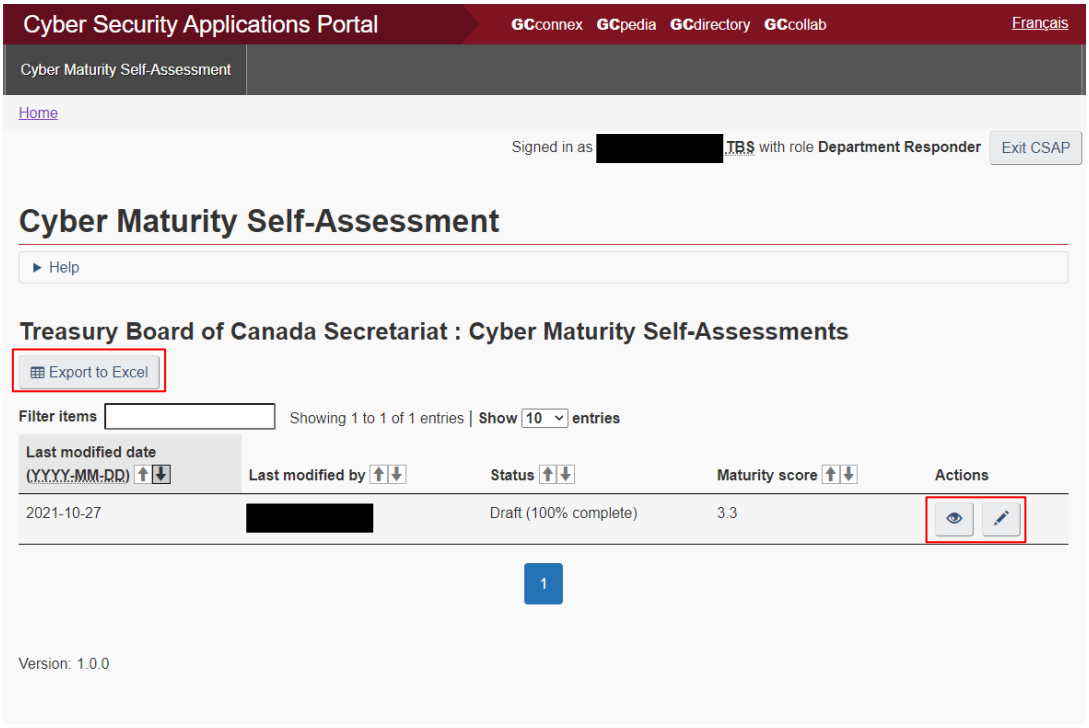
Based on the responses to the survey, the '**Results**' tab will summarize the organization's cyber maturity level.

Your organization will be given an overall score between 0-4, as well as scores broken down by each of the five Cyber Security Management Principles (i.e., identify, protect, detect, respond, and recover).



Following the completion of the CMSA, the history of the assessment will populate within the CMSA page with the options to:

- **view an assessment** by selecting the **'eye' icon**;
- **modify or complete an assessment** by selecting the **'pen' icon**; and
- **export the assessment to excel format** by selecting '**Export to Excel**'.



Contact Information

If you are having technical difficulties with the tool, please reach out to us at the following email address:

- DOCS / ADCS DOCS-ADCS@tbs-sct.gc.ca

If you have any general questions or would like more information, please reach out to us at the following email address:

- TBS-Cyber zztbscybers@tbs-sct.gc.ca