Summary of the 2016-2017 Evaluation of Canada's Cyber Security Strategy (CCSS)

Background

- **Inception**: October 3, 2010.
- **Objectives:** Securing Government of Canada (GC) Systems, Partnering to Secure Vital Cyber Systems external to the GC, Helping Canadians to be Secure Online.
- **Participating organizations:** Public Safety Canada, Communications Security Establishment, Shared Services Canada, National Defence, Treasury Board of Canada Secretariat, Canadian Security Intelligence Service, Global Affairs Canada, Justice Canada, Royal Canadian Mounted Police.
- **Total Funding for five years**: More than $198 million over five years; and 60 million/year (ongoing).
- **Evaluation scope:** 2010-11 to 2015-16.

What We Examined

- The effectiveness of the governance structure in providing oversight.
- The implementation of the funded activities by partner departments.
- The extent to which the main objectives were achieved.

Evaluation Findings

Governance

- Oversight committees facilitated collaboration, coordination and information-sharing among participating organizations.
- However, given the absence of consistent meeting minutes, other documentation, the evaluation was unable to assess the extent to which oversight committees were able to fulfill their mandates.
- Although roles and responsibilities of various players have been clarified and information-sharing and level of collaboration have improved, there are still some lingering issues that would require further improvement.

Implementation

- Most of the Strategy-funded activities have been fully implemented as intended, with the exception of four activities.
- Three organizations have reported under-spending of the allocated funding, two organizations spent more, two the exact amount and one was unable to track its relevant expenditures; three organizations faced difficulty staffing certain technical positions, particularly in a secret and/or top secret environment.

Performance

- The GC has increased its capacity to prevent, detect, respond to, and recover from cyber-attacks.
- The numbers of data breaches has declined over the course of the Strategy.
- The GC now analyzes and contains breaches more quickly than had been possible in the past.
- These improvements were made despite an increase in state and no-state-sponsored cyber activities against GC's networks.
- Closer partnerships have been forged with critical infrastructure owners and operators and other private sector stakeholders.
- Despite public awareness activities undertaken it is unclear to what extent Canadians are safer online.

Recommendations

In collaboration with participating organizations, the Senior ADM of the National and Cyber Security Branch, Public Safety, should consider undertaking the following:

1. Strengthen horizontal governance of cyber security in the Government of Canada by:
    a) re-assessing the governance structure to determine the need and demand for the current committee configuration and to improve participation;
    b) improving the provision of secretariat support, including coordination, information management and other administrative services;
    c) ensuring that governance committees have terms of references that clearly define roles, responsibilities, and expectations from members;
    d) ensuring that the oversight committees fulfill their roles and responsibilities as outlined in each oversight committee's terms of reference; and
    e) keeping meeting minutes on a consistent basis.

2. Strengthen the Cyber Security related information-sharing practices by developing policies, procedures and tools to ensure timely and systematic exchange of information among partners and stakeholders.

3. Strengthen the Strategy's performance measurement and data collection practices by:
    a) collecting relevant, reliable and outcome oriented performance information, including information on program expenditures, on a regular and consistent basis; and
    b) providing performance and expenditure information collected to the appropriate oversight committees on a regular basis to support effective monitoring and accountability.