André Boucher
Assistant Deputy Minister, Operations
October 30, 2018
Background

2015
Minister of Public Safety is mandated by the Prime Minister to lead “a review of existing measures to protect Canadians and critical infrastructure from cyber threats.”

2016
Government consults Canadians and key cyber security stakeholders on the cyber security landscape in Canada.

2018
February
The Canadian Centre for Cyber Security is announced as part of Budget 2018

June
The new National Cyber Security Strategy is released

October
The Cyber Centre is
The New Cyber Strategy


National Cyber Security Strategy

Secure and Resilient Canadian Systems

Protect Canadians from cybercrime, respond to evolving threats, and help defend critical government and private sector systems.

An Innovative and Adaptive Cyber Ecosystem

Support advanced research, foster digital innovation, and develop cyber skills and knowledge.

Effective Leadership, Governance, and Collaboration

Collaborate with provinces, territories, the private sector, as well as international allies, to take a leadership role in advancing cyber security.
The Canadian Centre for Cyber Security

- A key initiative of the new Cyber Strategy
- Flagship cyber security authority for Canada, demonstrating Federal leadership and clarity to stakeholders across Canada
- Unites cyber security expertise across the Government of Canada into a single window for stakeholders

- Governments
- Critical Infrastructure
- Private Industry
- Academia
- Canadian Public
- International Partners
Program Integration

The Cyber Centre consolidates all GC cyber security operations into one unique, innovative, and forward-looking organization, as part of CSE.

- Canadian Cyber Incident Response Centre and GetCyberSafe (PS)
- Security Operations Centre (SSC)
- IT Security branch (CSE)
Functions

**Inform** Canada and Canadians about cyber security matters, including about cyber security threats.

**Defend** networks and systems that are within its purview.

**Protect** Canadian interests through advice, assistance, and collaboration with partners across the country and abroad.

**Develop** and enrich the knowledge, personnel, and skills needed to continually improve cyber security for Canadians.
Benefits

- Bring together federal operational cyber expertise from across the federal government under one roof.

- Result in faster, better coordinated, and more coherent Government responses to cyber threats.

- Provide Canadian citizens and businesses with a clear and trusted place to turn to for cyber security information.

- Advance partnerships and dialogue with other jurisdictions, the business community, academia and international partners.
Attributes of a Valued Partner

- STRIVES FOR IMPROVEMENT
  - Governance
  - Technology
  - Training and Education

- PROMOTES TRANSPARENCY
  - Information Sharing
  - Manufacturing and supply chain process management
  - Centre for transparency

- LOOKS TO COLLABORATE
  - Advanced notifications
  - Feedback
  - Cyber security research and/or projects
  - Resources, milestones and deliverables

- ACTS RESPONSIBLY
  - Cyber security investments
  - Organizational decision-making processes
  - Conferences and cyber security events
  - Senior-level executive
New Facility

- The Cyber Centre facility will be located at 1625 Vanier Parkway, occupying the 5th to 10th floors
- Separate, open, accessible, and collaborative-by-design facility
- Will enable innovation with industry partners
IM/IT Strategy

Modern, flexible and accessible IM/IT services will support the Cyber Centre.

- Protected B and below by default
- Public cloud services as the priority choice
- Software-as-a-Service (SaaS) solutions as the priority choice for corporate applications
- Infrastructure as a Service (IaaS) and Platform as a Service (PaaS)
- Mobility including remote access and Wi-Fi
- No data centre in the new facility; will leverage the CSE campus data centre and public cloud
Milestones

- **2018/2019**
  - IOC 1
    - Oct 2018
    - Virtual establishment of the Cyber Centre

- **2019/2020**
  - IOC 2
    - Oct 2019
    - Physical establishment of the Cyber Centre

- **2020/2021**
  - IOC 3
    - Oct 2020
    - New facility is functional and fully operational

- **2021/2022**
  - BOC
    - Oct 2021-22
    - Enhanced IM/IT functionality to enable Cyber Centre operations

- **2023/2024**
  - FOC
    - Oct 2023
    - Cyber Centre integration is complete

IOC - Interim Operating Capability  BOC - Basic Operating Capability  FOC - Full Operating Capability