Presentation to the Armed Forces Communications & Electronics Association (AFCEA)

Mr. Raj Thuppal
A/Assistant Deputy Minister
Cyber and IT Security Branch
Shared Services Canada

May 5, 2015
Purpose

- Provide an overview of Shared Service Canada’s cyber security program for the Government of Canada
Fragmentation in the management of the Government’s IT infrastructure led to high costs, complexity and security risks

Mission-critical programs depend on IT infrastructure
- 2,100 mission-critical applications that span:
  - Key benefits programs;
  - Security;
  - Safety and health;
  - Farmers and students; and
  - Finance systems.

Departments managed their IT infrastructure independently
- In total, the Government of Canada (GC) was spending $1.9B/year on an unstructured and uncoordinated web of IT infrastructure and services:
  - 63 email systems;
  - Nearly 500 data centres of varying sizes, quality, security and energy efficiency; and
  - 50 wide area networks connecting over 3500 buildings and data centres – over 1,000 firewalls.

Status quo was complex, costly and less secure
- Current state of IT infrastructure is:
  - Vulnerable to cyber attacks, low availability and poor performance;
  - A long-term unfunded liability and a barrier to renewal, modernization and agility;
  - Using procurement practices that limit innovation;
  - Largely in-sourced; and
  - Not service-oriented.

"Without sufficient and timely investment to modernize or replace aging systems, the ability of departments to serve Canadians is at risk."
– Auditor General of Canada (2010)
SSC has developed detailed plans to transform the GC’s IT infrastructure and is moving to implementation.

SSC’s “Transformation Plan” sets out a phased approach to consolidating and modernizing the GC’s IT infrastructure over seven years (2013-2020).
Shared Service Canada’s Role in Cyber and IT Security

Shared Services Canada works closely with its federal partners, including Public Safety Canada, Communications Security Establishment Canada (CSEC), and Treasury Board Secretariat (TBS) as a “lead security agency” to:

1. Operate, enhance and transform IT security required for GC infrastructure (email, data centers, networks)

2. Evolve and transform GC Classified (up to Secret) Infrastructure

3. Implement on-going and future Cyber Security initiatives related to Canada’s Cyber Security Strategy

4. In collaboration with TBS and CSEC, develop enterprise Security Strategy, related policies, and reference Security Architectures for implementation across all GC partners
Shared Services Canada: The Cyber and IT Security Challenge

Today
- Complex Government of Canada (GC) IT Infrastructure
- IT Security as an “add-on”
- Reactive, Slow & Siloed Response to Cyber Threats

Future
- Rationalized, Standardized and Consolidated
- IT Security Integrated into the Design
- Coordinated Proactive Rapid Response & Recovery

Transforming the Government of Canada

Cyber and other IT security threats are constantly evolving and on-going effort is required to keep up
### Cyber and IT Security: Current State and End State Targets

<table>
<thead>
<tr>
<th>Current State</th>
<th>End State</th>
<th>Benefits</th>
</tr>
</thead>
<tbody>
<tr>
<td>• Various maturity level Security Operations Centres (SOCs), some with rudimentary services</td>
<td>• Standardized enterprise SOC with alternate site</td>
<td>• Integrated IT security risk management</td>
</tr>
<tr>
<td>• Reactive, slow &amp; siloed response to cyber threats</td>
<td>• Coordinated proactive rapid response and recovery</td>
<td>• Security through end-to-end design</td>
</tr>
<tr>
<td>• 27 perimeter/border defense services</td>
<td>• One enterprise Perimeter/Border Defense Services</td>
<td>• Enhanced information and system protection</td>
</tr>
<tr>
<td>• 22 different security remote access solutions</td>
<td>• One enterprise standard Secure Remote Access solution</td>
<td>• Real-time detection of security incidents</td>
</tr>
<tr>
<td>• 42 departments device security implementation with partial data loss prevention services</td>
<td>• One enterprise device security solution with data loss prevention</td>
<td>• Swift incident response and recovery</td>
</tr>
<tr>
<td>• 42 department specific IT security risk management approaches</td>
<td>• Enterprise robust IT security risk management</td>
<td></td>
</tr>
<tr>
<td>• IT security as an “add-on”</td>
<td>• IT security integrated into the design</td>
<td></td>
</tr>
<tr>
<td>• 32 isolated department specific secret networks</td>
<td>• One enterprise Secret network enabling collaboration</td>
<td></td>
</tr>
<tr>
<td>• 10,000 users</td>
<td>• Approximately 20,000 users</td>
<td></td>
</tr>
</tbody>
</table>
Cloud Security

- SSC is building an internal GC private cloud leveraging industry best practices to build cloud security by design to address security and privacy challenges.
- Cloud Security Principles and Cyber and IT security framework for the GC private cloud has been developed, and the services required for full suite of functions are in progress.
Cloud Security Principles

1. Trusted equipment and services through Supply Chain Integrity

2. Security and privacy by design to ensure all aspects of security are addressed as part of design, balancing service, security and savings

3. Gradual enhancement from network based security-model to include application and data centric security – apply security controls as close to data as practical

4. Privileged access to data will be maintained and multi-tenancy will be built into systems where sensitive data owned by one partner cannot be seen by another partner or by unauthorized individuals

5. Security breaches in one part of the infrastructure are quickly detected and contained without spreading to other parts of the infrastructure

6. Maintain and improve the security posture as part of moving to enterprise services (i.e. don’t reduce security)

7. Security lifecycle management with multiple vendors strategy
### Cloud Security Framework: Cyber and IT Security Functions

#### PREVENTION
- Trusted infrastructure products and services through supply chain integrity
- Cyber and IT Security (including Privacy) policies and standards
- Security awareness and training
- Infrastructure Protection Services
- Data Protection Services
- Identity, Credentials and Access Management Services
- Secret Infrastructure Services
- Business Continuity and Emergency Management

#### DETECTION
- Coordination of GC-wide monitoring, detection, identification, prioritization, and reporting of IT Security incidents
- Automated, real-time threat monitoring, security information and event management and analysis
- Log analysis and investigations
- Security and Privacy Assessment
- Vulnerability assessments

#### RESPONSE
- GC-wide coordination and remediation of IT Security incidents
- Threat assessment and situational reporting
- Coordination and distribution of GC product alerts, warnings and advisories
- Forensics
- Software integrity through security configuration or replacement
- Infrastructure integrity through configuration or replacement

#### RECOVERY
- Highly specialized IT Security incident recovery services
- Mitigation advice and guidance
- Vulnerability remediation
- Post incident analysis

#### SECURITY MANAGEMENT
- Governance
- Innovation
- Engagement
- Risk Management
Cloud Security Risk Management

**Process**
- SSC uses the IT Security Risk management process published by Communication Security Establishment of Canada (CSE) for delivering security-by-design
- A Canadian adaptation of the US’s National Institute of Standards and Technologies NIST-800-53 publication
- Provides a methodology and recommended security controls broken down into security profiles for various confidentiality, integrity and availability requirements

**Approach**
- Business Context
- Technical Context
- Threat Context
- Threat Assessment
- Driving Factors
- Security Profile for design of cloud services
Wrap Up and Open Discussion…