



Public Safety  
Canada

Sécurité publique  
Canada

BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**



## Federal Provincial Territorial Collaboration to Protect Canadians and Critical Infrastructure from Cyber Threats

Public Sector Chief Information Officer's Council  
(PSCIOC)

February 25, 2016



- Update on collaborative work accomplished to date under *Canada's Cyber Security Strategy*
- A new approach to cyber security at the federal level
  - Cyber Review in Minister's Mandate Letter
  - Plans at the federal level to protect Vital Cyber Systems
- Deputy Minister Federal Provincial Territorial Table on Cyber Security
  - Composition of Membership
  - Action Plan for Collaboration
- The Way Forward

# Canada's Approach and Accomplishments



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

## Canada's Cyber Security Strategy

- Three pillar framework to guide the Government of Canada's efforts:
  1. Secure Government of Canada systems
  2. Partner to secure vital cyber systems outside the federal government
  3. Help Canadians be secure online
- Launched in 2010, initial \$244M investment, additional investment of \$142.6M announced in July, 2015
- Most investment has been focused under pillar one – shored up and secured Government networks and systems, now initiate work in other spheres
- Partnering with provinces, territories, and critical infrastructure sectors
- Strengthening the Canadian Cyber Incident Response Centre (CCIRC)
- Promoting public awareness, education, and engagement



# Prime Minister's Mandate Letter Direction



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

***“Lead a review of existing measures to protect Canadians and our critical infrastructure from cyber-threats in collaboration with the Minister of National Defence, Infrastructure and Communities, Public Services and Procurement, Innovation, Science and Economic Development, and the President of the Treasury Board.”***

## **Objectives for the Review**

- Conduct a credible, comprehensive stakeholder consultation process
- Identify needs and associated solutions and innovations
- Take cyber security in Canada to the next level: move from a responsive to proactive strategy, positioning Canada as a global leader in cyber security
  - Create a new national framework for cyber security



# Framework for a Renewed Approach to Cyber Security



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

## *Guiding Principles*

- Protect the safety and security of Canadians and critical infrastructure
- Defend fundamental rights and freedoms online
  - Foster economic growth and prosperity
  - Collaborate to grow capabilities
  - Foresee emerging technologies and the future of cyber security

## **Resilience**

- Public Awareness
- Accreditation Programs
- Incentives/Standards

## **Innovation**

- Innovation Centres
- Data & Analytics Strategy
- Curriculum Development
  - R&D Projects

## **Capability**

- Workforce Development
- National Cybercrime Coordination Centre
  - Cyber Fusion



# Review Process



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

- Publish a consultation paper with principles and key areas for action (March)
- Consult with industry, provinces/territories, academia, civil society (March – June)
- Gather consultation feedback and develop a new framework to be announced with early initiatives through a white paper (fall 2016)
- There will be further opportunities for consultation and feedback on the areas for action after the Framework is announced
  - Cyber is not a 'single fix' issue – initiatives will need to evolve and adapt



# Consultative process



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

## Consultations

- Seeking input through various mechanisms:
  - Opportunity for Public submissions - on-line consultations
  - Targeted Roundtables with provincial-territorial officials
  - Leverage key engagement vehicles including FPT (working groups, councils, committees, etc)

## Seeking PT Perspectives on:

- Pressing cyber challenges that need to be addressed to promote and protect Canada's digital infrastructure
- Gaps that still remain in protecting Canada's critical infrastructure and Canadians from cyber threats
- Agreeing to a baseline of cyber security approaches and discussing how these benchmarks may be adopted across Canada



# Early Action: Protecting Canada's Vital Cyber Systems



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

- In parallel with the Review, work to take immediate action to address gaps
  - Developing legislation to protect vital cyber systems per Budget 2015 announcement
- Current gap: No mechanism to ensure that vital cyber systems maintain a baseline level of security despite risks to Canada's national security, public safety, and economy.
  - Impedes ability of government to support vital cyber system operators
- Need to develop a collaborative approach between private sector operators and all levels of government.
  - Enhance collective defence to benefit national security and the economy
  - Establish a foundation for sharing information and expertise





# Protecting Canada's Vital Cyber Systems



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

## Context

- No legal authority to identify or protect vital cyber systems
- Limited ability to support operators, protect economy, national security
- Many countries examining legislative approaches
- Budget 2015: Announced legislation to protect vital cyber systems





## IDENTIFY

- Designate vital cyber systems and their owners

## PROTECT

- Cyber Security Plans
- Incident reporting
- Direction in emergencies
- Criminal penalties for attacks on vital systems

## COLLABORATE

- Support for crises
- Expertise and tools
- Actionable intelligence
- Real-time and longer-term analysis

# DM FPT Table on Cyber Security



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

## Context

- Initiated following July 2013 meeting of the Clerk and Cabinet Secretaries
- Two meetings each year, most recent in June 10, 2015
- Provide a forum to exchange information and practical examples on strengthening cyber security, formulate common definitions for cyber security terms, provide strategic direction, and identify key FPT activities and deliverables

## Challenges

- Jurisdictions have different capacities and various levels of maturity in relation to cyber security
- Jurisdictions differ in their approach to cyber security – IT security, infrastructure, or public safety focus
- Cyber Security is complex and dynamic that requires holistic consideration and multi-faceted involved strategy



# Action Plan for Collaboration



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

## Four agreed upon areas of work that merit FPT collaboration:

1. Information sharing and incident response (Public Safety facilitated);
2. Public awareness (British Columbia and PS lead);
3. Cyber security standards and best practices (Alberta, Ontario and PS lead); and
4. Education and talent management (New Brunswick and PS lead).

## Revisions proposed by NCSD and endorsed by NCSIP in Fall 2015 included:

- Two activities migrated to NCSIP for action
- Agreement on priorities that comprise Action Plan, however persistent resource challenges
- Need to identify FPT leads in areas of expertise beyond IT security

# The Way Forward



BUILDING A **SAFE AND RESILIENT CANADA**  
BÂTIR UN **CANADA SÉCURITAIRE ET RÉSILIENT**

## Action Plan Items

- Who within your PT (primary and an alternate) would be well positioned to sit on the DM FPT Table on Cyber Security?
- How can we advance the priorities identified in the Action Plan?

## Review Process

- What are the pressing cyber challenges that this government should tackle in order to promote and protect Canada's digital infrastructure?
- What do you see as the policy and operational gaps that still remain in protecting Canada's critical infrastructure from cyber threats?
- How do we position Canada as a global leader in cyber security and make this one of our competitive advantages?





## NCSD, Public Safety Canada:

Mark Matz, Director, Policy and Issues Management  
[mark.matz@canada.ca](mailto:mark.matz@canada.ca)