Canadian GNSS Activities

Advisory Board Meeting

Boulder, Colorado

October 30 – 31, 2015

Jina MacEachern

GNSS Coordination Office

GNSS and Critical Infrastructure

- Similar to most developed nations, the use of GNSS in Canada's critical infrastructure sectors is pervasive.
- There are risks associated with the use of GNSS.
  - Considerable attention is being focused on the risk of signal disruption:
    - Use of "eBay" jammers is becoming more common.
    - Solar activity can distort the GNSS signals.
    - Spoofing and Cyber are issues of concern.
- There will be inconvenience and economic impact should a significant disruption of GNSS occur.

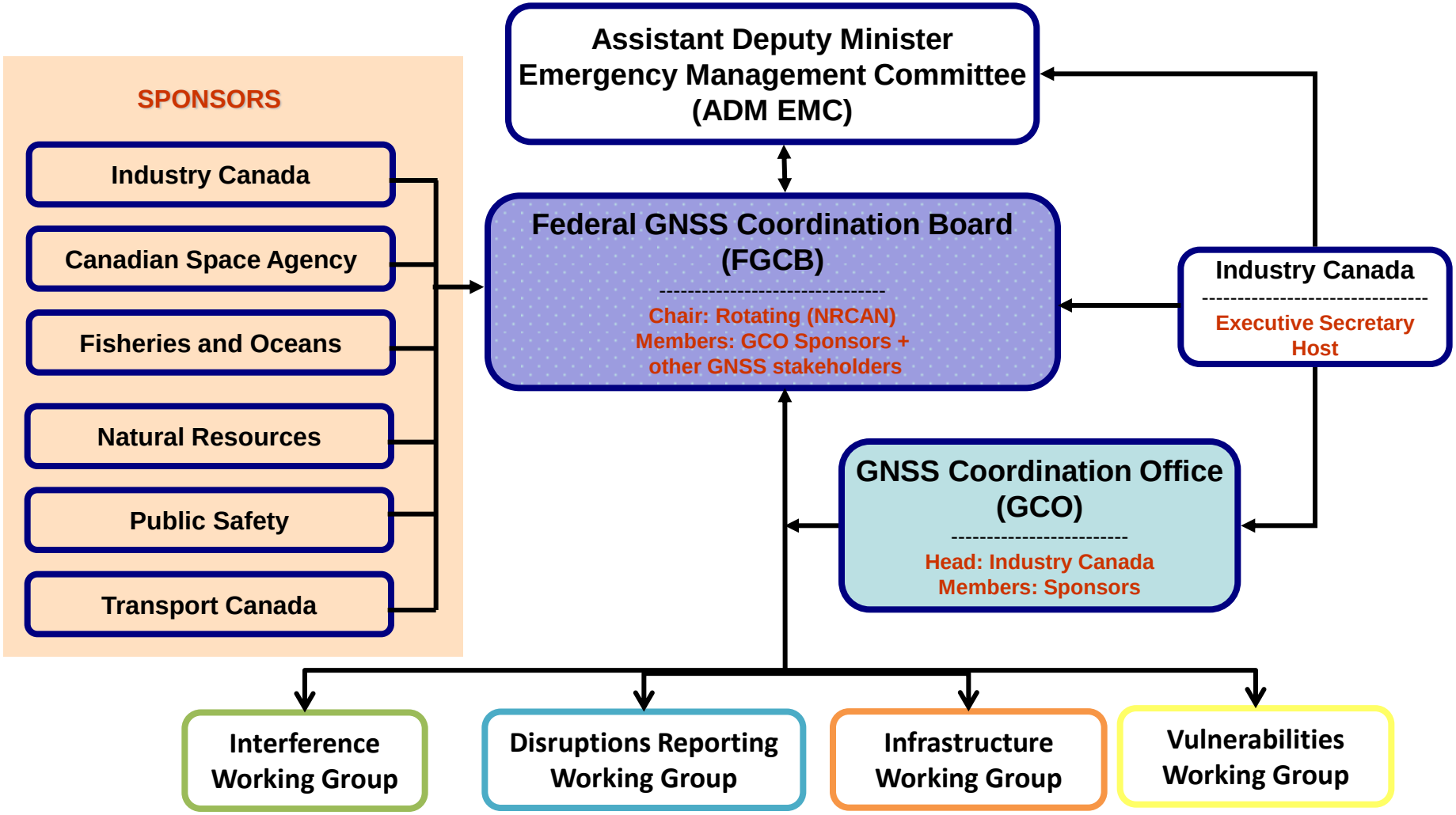
GNSS and Critical Infrastructure

The ICT Sector is composed of both physical and cyber infrastructure and may be divided into the following sub-sectors:

- Telecommunications including cable, wireless and satellite infrastructures
- Information Technology
- Broadcasting

"Critical infrastructure refers to processes, systems, facilities, technologies, networks, assets and services essential to the health, safety, security or economic well being of Canadians and the effective functioning of government. Critical infrastructure can be stand-alone or interconnected and interdependent within and across provinces, territories and national borders. Disruptions of critical infrastructure could result in catastrophic loss of life and adverse economic effects." ***National Strategy for Critical Infrastructure (2010)***

FGCB Governance Structure



Responsibilities and Functions

FGCB

- Advise the Canadian government and coordinate GNSS matters among its members as well as international bodies
- Collaborate, share information/expertise, and provide advice
- Present annual objectives and priorities to ADM EMC

GCO

- Act as the federal point of contact for GNSS
- Provide support for the FGCB operations
- Develop an annual work plan consistent with objectives and priorities
- Provide catalyst/facilitator role for FGCB working groups
- Ensure reports and recommendations are prepared and presented

FGCB Working Group Activities

Interference Working Group

To develop a Canadian approach for GNSS interference monitoring, detection, reporting and mitigation (e.g. IDM, testing, legislations, enforcement).

Disruptions Reporting

To develop a GNSS disruption alerts and communicate GNSS problems within the Canadian government departments and GNSS users.

Infrastructure Working Group

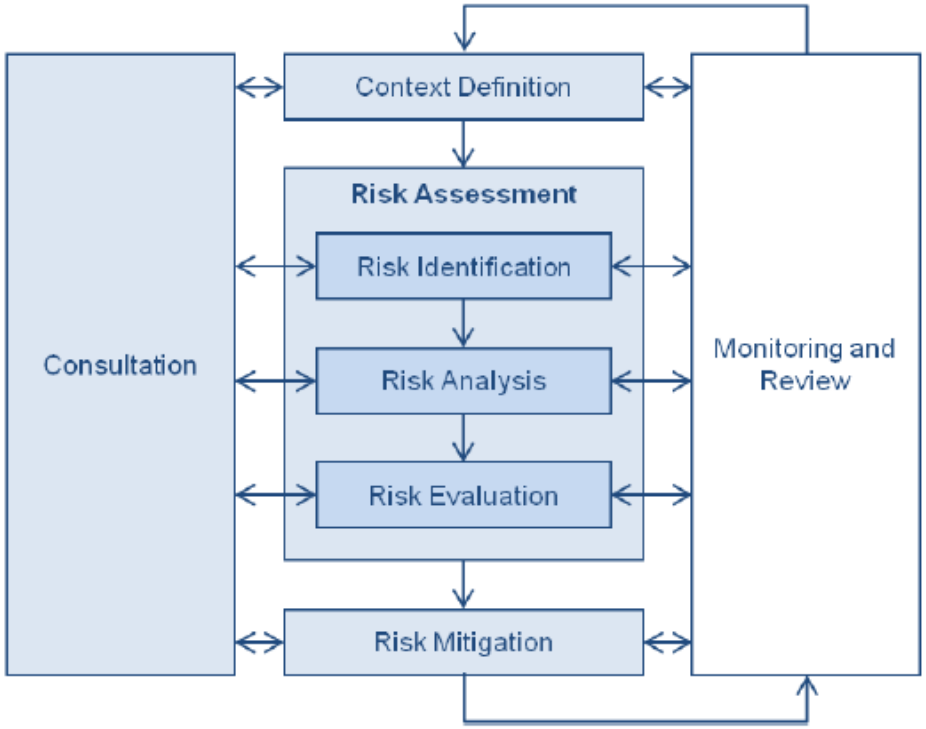
To develop a coordinated approach to GNSS infrastructure investment across the Government of Canada that considers life-cycle of instrumentation, the advent of new GNSS systems and technologies.

Vulnerabilities Working Group

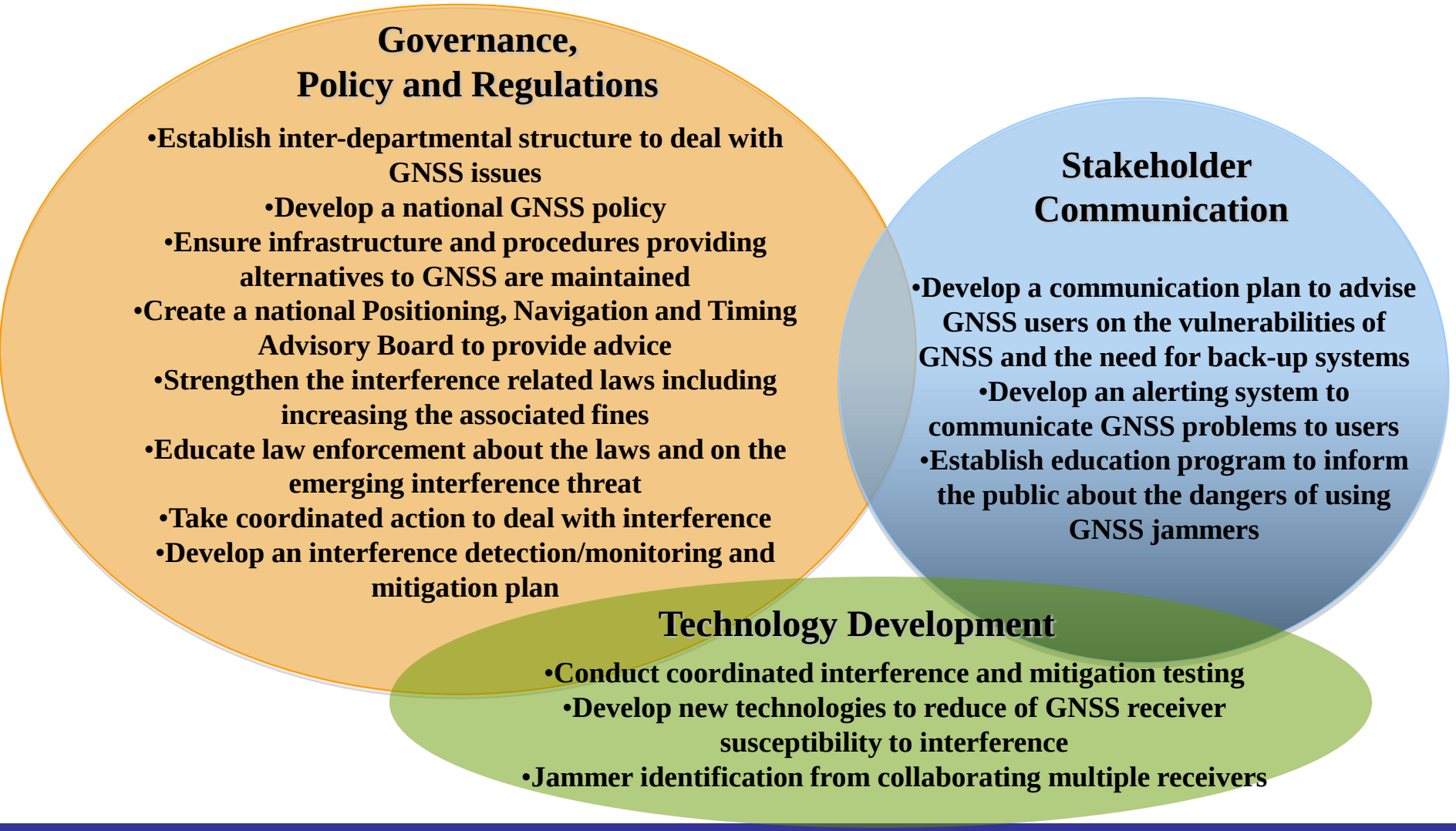
To develop an assessment of the risks and potential effects of GNSS disruptions on Canadian Critical Infrastructure and recommend measures to prevent and mitigate risks and vulnerabilities.

Progress to Date
GNSS Risk Assessment

1. Identify the critical infrastructures that would be affected by a GNSS signal disruption (e.g. Failure, unavailability, solar storms, interference, jamming)
   - **Air transportation**
   - **Marine Transportation**
   - **Timing & Synchronization**
   - **Safety**
   - **Government**
2. Determine the level of risk that exists using the following metrics:
   - Safety of life
   - Economic
   - Environmental
3. Recommend potential solutions to mitigate the potential impact.



Progress to Date
Risk Assessment - Recommendations



Progress to Date
Radiocommunications Act - Jammers Treatment

- **Broad definition of jammers:**
  - 4(4) “jammer” means any device or combination of devices that transmits, emits or radiates electromagnetic energy and is designed to cause, causes or is capable of causing interference or obstruction to radiocommunication other than a device or combination of devices for which standards have been established under paragraph 5(1)(d) or 6(1)(a) or for which radio authorization has been issued
- **Prohibition**
  - Installation, use, possession, manufacture, import, distribution, lease, offering for sale or sale of a jammer is prohibited

Radiocommunications Act - Jammers Penalties

- **Administrative Monetary Penalties**
  - Civil penalties
  - Up to $10 million ($15 million for subsequent violation) for companies, $25,000 ($50,000 for subsequent violations) for individuals
- **Regulatory Offence**
  - $5,000 fine and/or one year in prison for individual
  - $25,000 fine for companies

Progress to Date
More FGCB Accomplishments

- Enhancing collaborations among various government departments on GNSS
- Participating in inter-departmental and international committees dealing with GNSS
- Developing recommendations concerning responsibilities of Canadian departments with respect to GNSS ***I***nterference, ***D***etection and ***M***itigation issues
- Expanding cooperation on interference detection and mitigation, jammer enforcement, and geodetic network ground station coverage in Canada
  - Canada – U.S. Civil GNSS meetings
- Organizing FGCB Workshop on GNSS vulnerabilities
  - February 2014
  - April 2015

Next Steps

- Exploring options for improving communication of GNSS problems to users
- Developing a GNSS Risk Assessment taking threats (e.g. spoofing, cyber) and CI interdependencies into consideration
- Monitoring developments related to GNSS backup
- Developing a communication plan to advise GNSS users on the vulnerabilities of GNSS
  - Organize workshop(s) with private sector (telecom, finance, power, etc.) to understand the dependency on GNSS and impact of GNSS disruptions on these services.

THANK YOU

Jina MacEachern
Jina.MacEachern@Canada.ca