Government of Canada | Gouvernement du Canada

Canadian Safety and Security Program

APCO Canada

May 20, 2014

700 MHz Public Safety Broadband Network

Capabilities – Recommendations for the PSBN

Claudio Lucente, P.ENG, M.ENG.
Senior technical advisor

Led by Defence R&D Canada – Centre for Security Science

Canada

About the Centre for Security Science…

- Canadian Safety & Security Programme
  - ⇨ *mission is to strengthen Canada's ability to anticipate, prevent/mitigate, prepare for, respond to, and recover from acts of terrorism, crime, natural disasters, and serious accidents through the convergence of S&T with policy, operations and intelligence.*
  - ⇨ *Provide technical advice and support to the public safety community on communications interoperability.*

Disclaimer

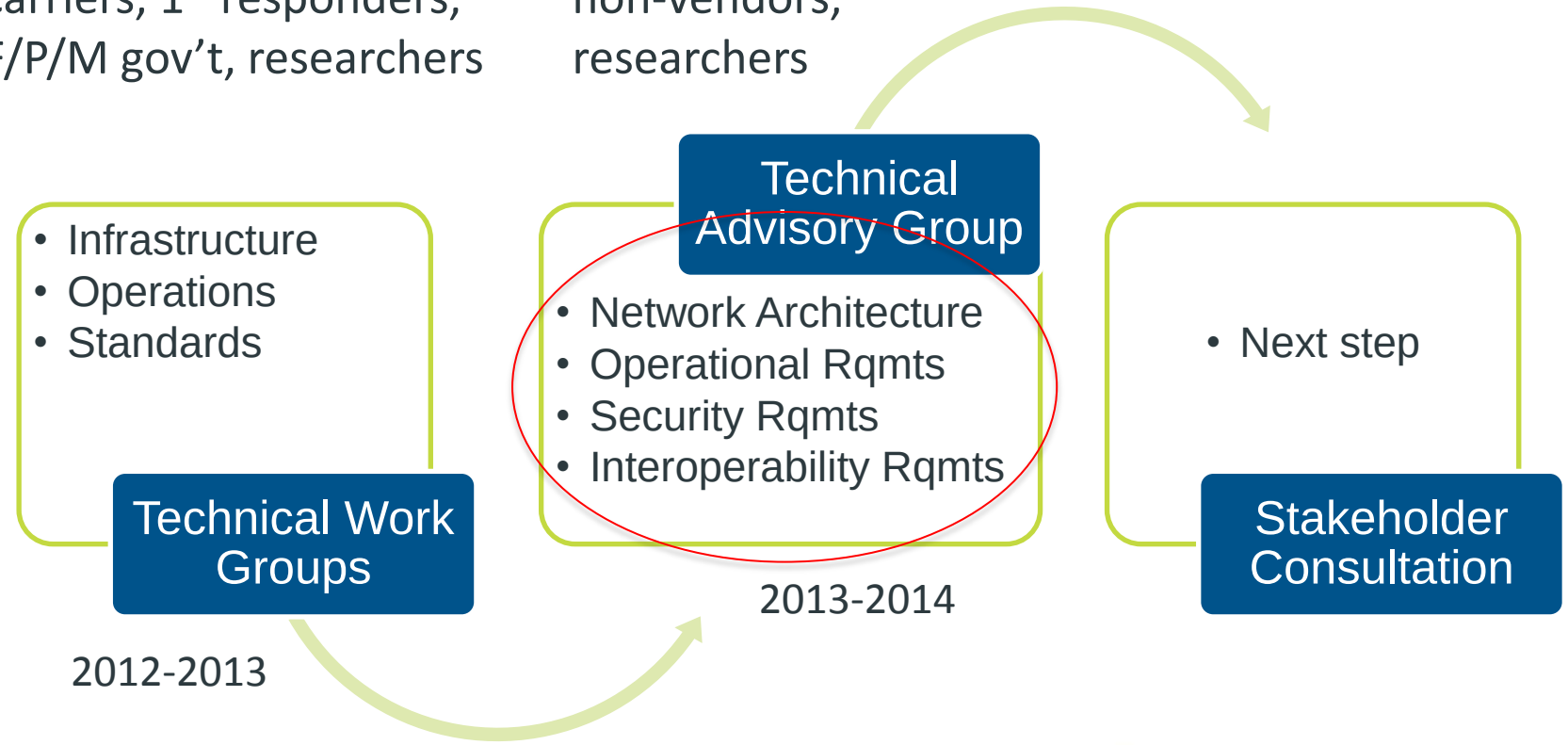
The statements contained in this presentation or communicated in the context of this presentation do not represent official statements by the Government of Canada. They are solely attributable to the author.

All or some of the contents in this presentation may change at any time. The author disclaims any obligation to inform the recipients of any changes.

Requirements development

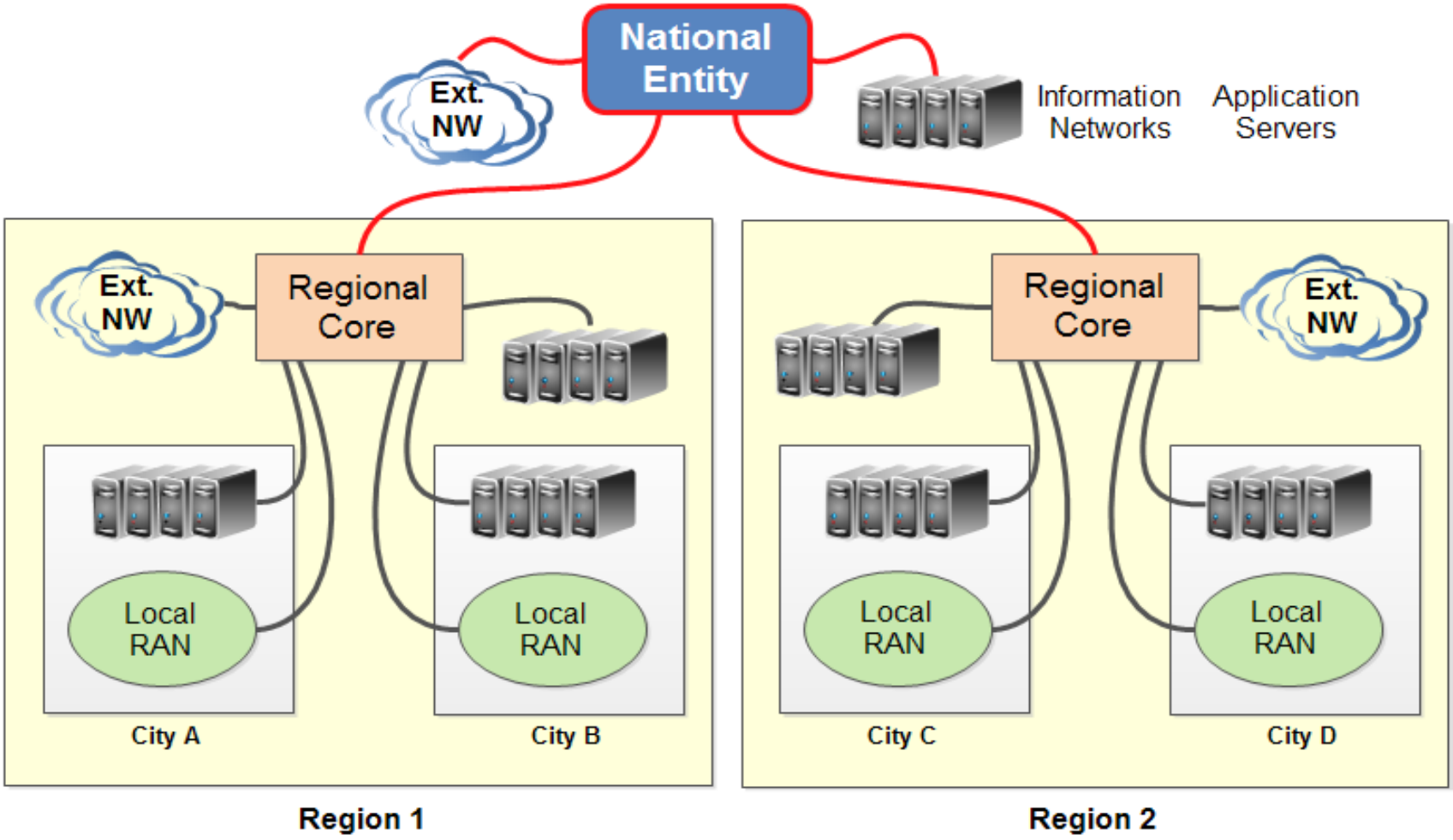
Open Consultation
Vendors, consultants, carriers, 1st responders, F/P/M gov't, researchers

Closed group
gov't, contractors, non-vendors, researchers



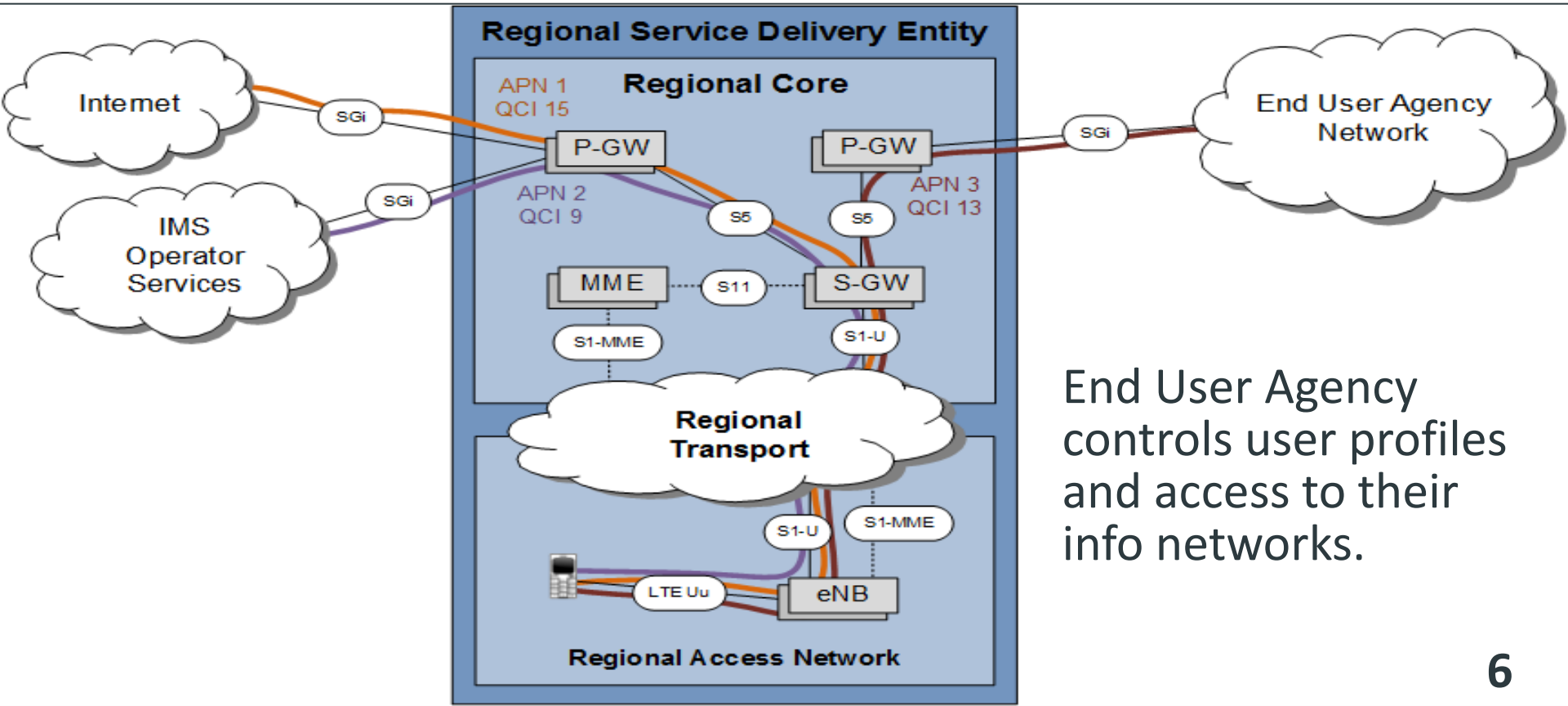
Canadian Safety and Security Program

Network Architecture - conceptual



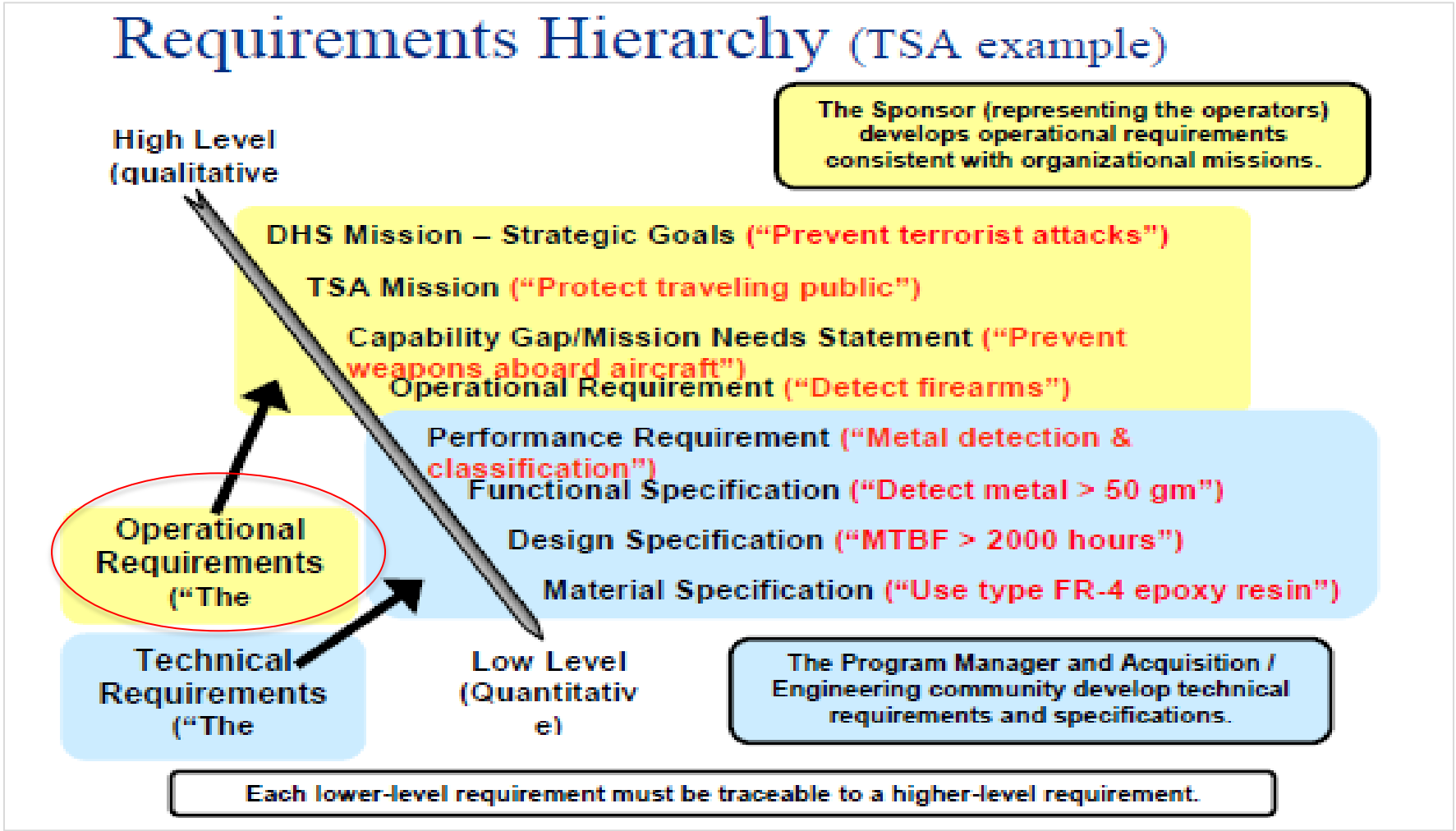
Accessing multiple services

- QoS: Multiple services and applications can be accessed simultaneously by a user. Each application would be accessible with its own QoS.
- Priority: Priorities for accessing applications can be set independently for each user and each application.



End User Agency controls user profiles and access to their info networks.

Operational Requirements



DHS, "Developing Operational Requirements – A Guide to the Cost-Effective and Efficient Communications of Needs", version 2.0, Nov. 2008.

Operational Requirements

1. Roaming between the PSBN, FirstNet, commercial carriers in Canada and international.
2. Traffic off-loading onto other 3GPP and non-3GPP networks.
3. Session persistence during hand-off and when transiting from one network to another.
4. Fixed and deployable components of the PSBN.
5. Operability with other systems and networks:
   - Land Mobile Radio
   - Public Switched Telephone Network (PSTN)
   - Public Warning Systems
   - NG 9-1-1
   - Internet

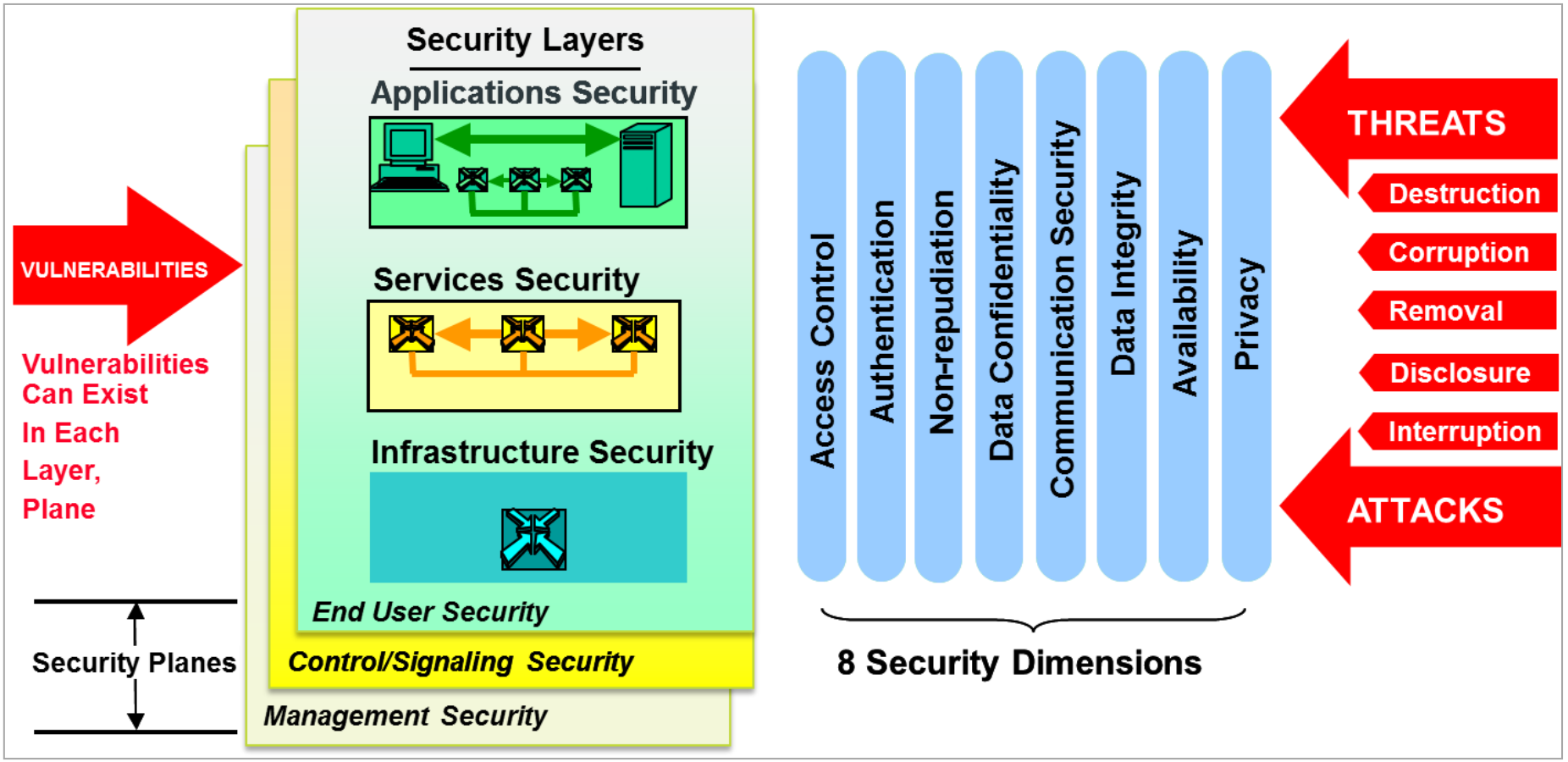
Operational Requirements

6. Device management:
   - Support for multiple users
   - Alternative access (WiFi, etc.)
   - Provisioning, updating, revoking access
7. Support applications:
   - Life-cycle management of apps – vetting & monitoring, launching, retiring.
   - Location-based apps
   - Messaging
   - Video
   - Voice services
   - MVPN
8. Congestion Management:
   - QoS and Prioritization – static and dynamic
   - Multicast capability

Operational Requirements

9. Network and Service management:
   - Service provisioning
   - Performance management
   - Fault management
   - Configuration and Inventory management
   - Billing and revenue assurance
   - Self-Organizing Networks
   - Compliance to Service Level Agreements
10. Resiliency:
   - Redundancy
   - Layered fall-back
   - Service availability

Security Requirements - Framework



ITU-T Recommendation X.805

"Security Architecture for Systems Providing End-to-End Communications".

Canadian Safety and Security Program

Security Requirements: Access Control

1. Physical access controls.
2. Assignment of radio resources to authorized users only.
3. Access to servers, logs, metadata.
4. User devices access to the PSBN.
5. Applications access to network services such as location information, billing records, etc.
6. Access to KPIs.
7. Authorized end-users, OAM users, and devices only.
   - Default deny security posture.

Security Requirements: Authentication

1. Identity Credentials and Access Management (ICAM) service to be hosted by PSBN (recommended).
2. Ascertain confidence in digital identities and use confidence level in access control.
3. Mutual authentication of machines/sensors and the PSBN.
4. Applications and machines to be authenticated prior to granting access to network services.

Security Requirements: Non-Repudiation

1. Log actions of end-users and OAM users:
   - Physical access,
   - Log-in / log-out actions,
   - Configuration changes,
   - Information access,
   - etc.
2. Time and location stamping of logs to use network reference.

Security Requirements: Data Confidentiality

1. Logs and metadata to be stored securely.
2. Information collected by users to be stored securely.
3. Logs, metadata, and user data should be usable as evidence in a court of law.
4. Secure disposal of User devices and network appliances.
5. Encryption of information.
6. Notification of users when session is not encrypted.
7. Confidentiality of user credentials.

Security Requirements: Communication security

1. Separate IP addressing spaces for user plane, control plane, signalling plane.
2. Network address translation.
3. Inter-domain security gateways (IPsec).
4. Certificate Validation service and Directory service for key management (ITU X.509).
5. Support user-defined cipher algorithms.

Security Requirements: Data Integrity

1. Monitor device OS for changes. Disable access to UE with compromised OS.
2. Retain images of prior configurations as fall-back.
3. Prevent power failures from corrupting data.
4. Upgrades to be active after code integrity check.
5. Malware detection and filtering.
6. Active monitoring of code integrity of applications. Disable applications with compromised code.
7. Only authorized applications can be installed.

Security Requirements: Availability

1. Geo-redundancy of critical information repositories, applications, network elements, etc.
2. Protection from DoS attacks.
3. Ability to isolate compromised (infected) portions of the PSBN.
4. Push virus definition files.
5. Active prevention of duplicate IP addresses.
6. Remote deactivation of compromised UE.
7. Re-start network services into a known operating state.
8. Separate ICAM for end-users and OAM users.
9. Secure backup and restoration service.

Security Requirements: Privacy

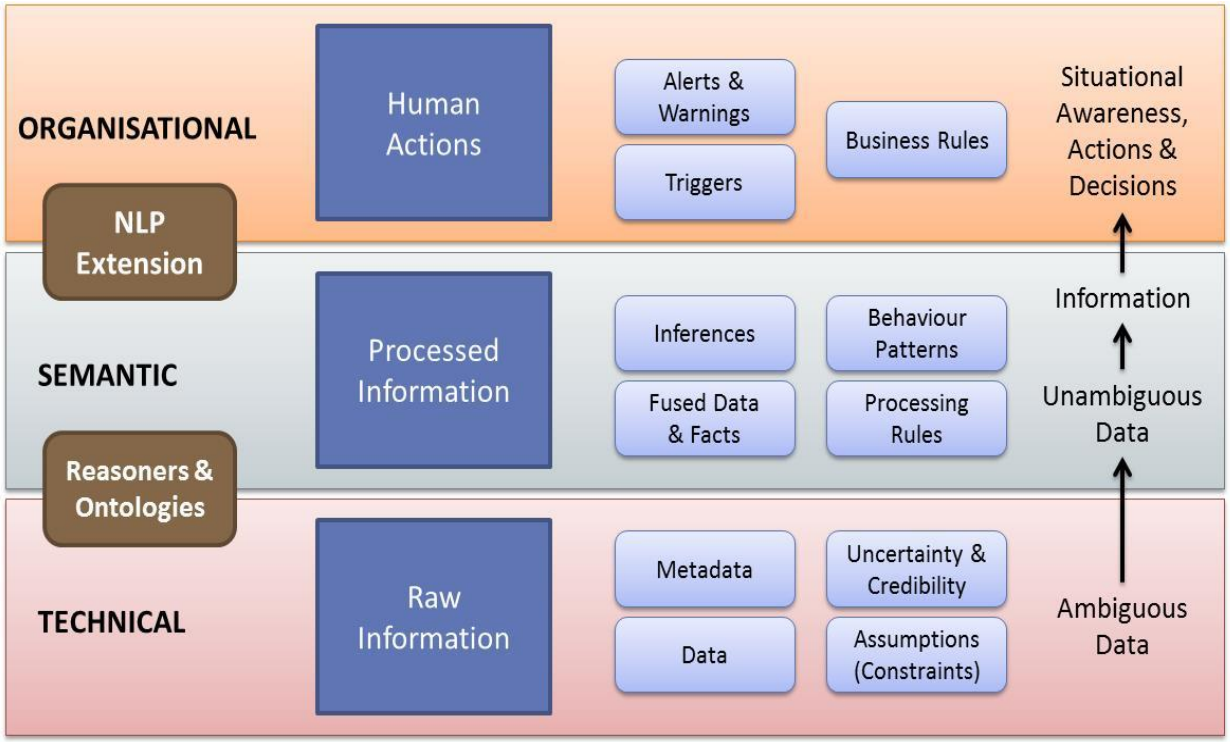
1. Comply with Gov't of Canada policies with respect to routing and ciphering of information, and key management.
2. IP addressing plan and network design to be protected.
3. Data transferred to removable media to be protected.
4. Black-listing and white-listing users wrt external messaging.
5. Confidentiality of location information.
6. Separation of business and personal information on dual-mode devices.
7. User-specific cipher keys for shared devices.
8. Access to Internet through security gateways.

Interoperability Requirements

1. PSBN mobile network based on LTE Rel.10; 3GPP standards.
2. Open standards for network APIs. Examples…
   - Device Management
   - File transfer
   - Identity Management
   - Image sharing
   - Multimedia streaming control
   - Presence services
   - User-profile Management
   - Order Management
   - Supply chain e-bonding
   - Element management system adaptors
   - Service Level Agreement
   - Trouble Ticketing

Interoperability Requirements

3. Information interoperability – common information model.



(Re-produced with permission from Pegasus Simulation Services Inc.)

Interoperability Requirements

4. System-level interoperability testing:
   - UE devices
   - eNB
   - EPC
   - Deployable systems
   - Applications
   - External networks
   - Life cycle management – change management
5. Interfaces between RSDE and National Entity:
   - Security Gateways
   - MVPN
   - IP Multimedia Subsystem (VoLTE)
   - eMBMS (Group Call, PTToLTE)

Interoperability Requirements

6. Interfaces between PSBN and external networks:
   - Inter-carrier roaming interfaces
   - IMS roaming interfaces
   - Interfaces with non-3GPP networks.
   - Wireless Public Alerting
   - Law Enforcement Monitoring facility
   - Land Mobile Radio networks
7. Interfaces between PSBN and deployable systems:
   - Extensions of the PSBN fabric
   - Augmenting the existing PSBN
   - Deployments in isolated areas
   - Self-Organizing Network

Interoperability Requirements

8. Interfaces with Operations Admin Maintenance
   - Integration Reference Points (3GPP)
9. Allocation of Network Identifiers.
10. Standards for access control, QoS, and priority applied in a consistent manner throughout the PSBN.
11. Identity, Credentials, and Access Management (ICAM) consistency throughout the PSBN.
    - Federated ICAM as a nationally-hosted service.
    - Common definition of confidence levels of digital signatures.

Thank you

Claudio Lucente

CLucente@Fiorel.com