
# CSIRT (CERT) Registry Authority Concepts

Jacques Latour

Director, Information Technology

Canadian Internet Registration Authority

Version 1.4
February 2011

# Overview

- What's the problem?
  - The Internet industry is trying to find a solution for handling global security issues, including the discussion around a global DNS CERT

- What's the real problem?
  - To start, there's no clear understanding of CERT (CSIRT) concepts

    - National / Government CERTs (Canadian CCIRC, US-CERT, etc…)
    - Coordination Center CERTs (CERT/CC, PCH)
    - TLD & ISP CERTs (CIRA, Bell, Rogers, Telus, Videotron, etc…)
    - Business CERTs (financial, medical, conglomerate, etc…)
    - Computer vendor CERTs (P CERTs) (Cisco, Oracle, etc…)
    - Analysis CERTs (DNS-OARC, Def. Intel., InternetIdentity, etc…)

**What the industry is asking for is a mean for securely reaching the right organization(s) at the right time when a security event occurs**

# CERT & CSIRT

- "CERT" and "CERT Coordination Center" are registered in the U.S. Patent and Trademark Office. Organizations who wish to use "CERT" in their team name must request permission, send email to cert@cert.org
- Industry terms for CERT:
  - CSIRT Computer Security Incident Response Team
  - CIRT Computer Incident Response Team
  - IPC Information Protection Center
  - IRC Incident Response Center
  - IRT Incident Response Team
  - SERT Security Emergency Response Team
  - SIRT Security Incident Response Team

→ CSIRT ←

# CSIRT Overview

- Computer Security Incident Response Team (CSIRT)
  - A group of experts responsible for dealing with computer security incidents

- There are different type of CSIRTs

**Coordination Center CSIRT**

- Responsible for assessing security incidents and coordinating information dissemination with other CSIRTs

**Internal CSIRT**

- Responsible for full spectrum security incident remediation within the organization (incident management operations framework)

**Vendor CSIRT**

- Responsible for security incident remediation within a product or service

**Analysis Centers CSIRT**

- Trend and pattern analysis by subject matter (DNS, spam, phishing, etc…)

# Top Level CSIRT Organizations

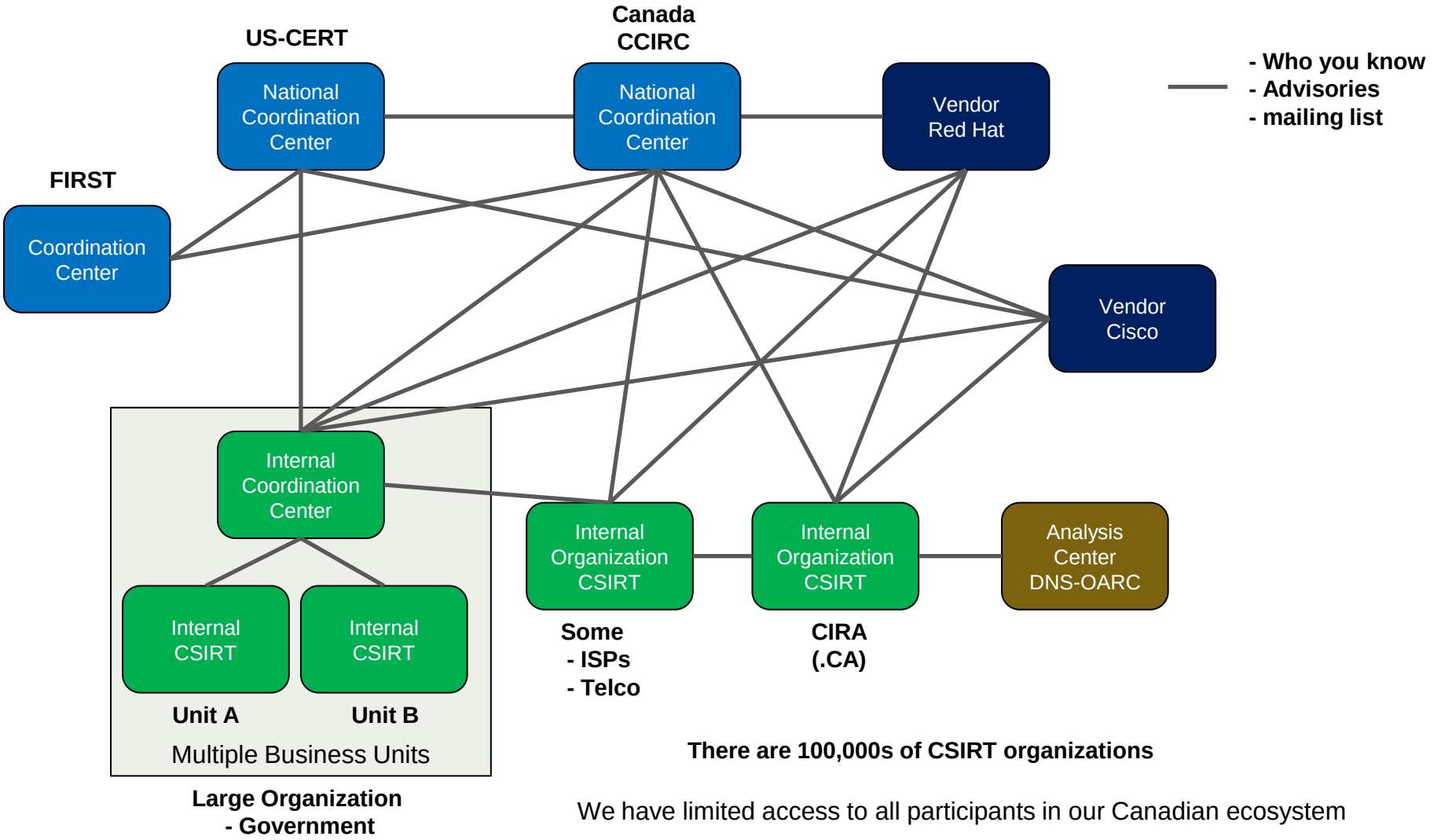
- The current framework for CSIRT is based on "who you know" and "who you trust"; there are a few organizations that act as "root registries" of trusted Coordination Center CSIRTs by geographic region. Internal CSIRTs are mostly excluded from these groups.

  FIRST is the Forum of Incident Response and Security Teams.
  - http://www.first.org/about/

  APCERT will maintain a trusted contact network of computer security experts in the Asia Pacific region
  - http://www.apcert.org/about/mission/index.html

  The Trusted Introducer (TI) maintains the European database of CSIRTs (also known as CERTs) and security teams.
  - http://www.trusted-introducer.nl/teams/

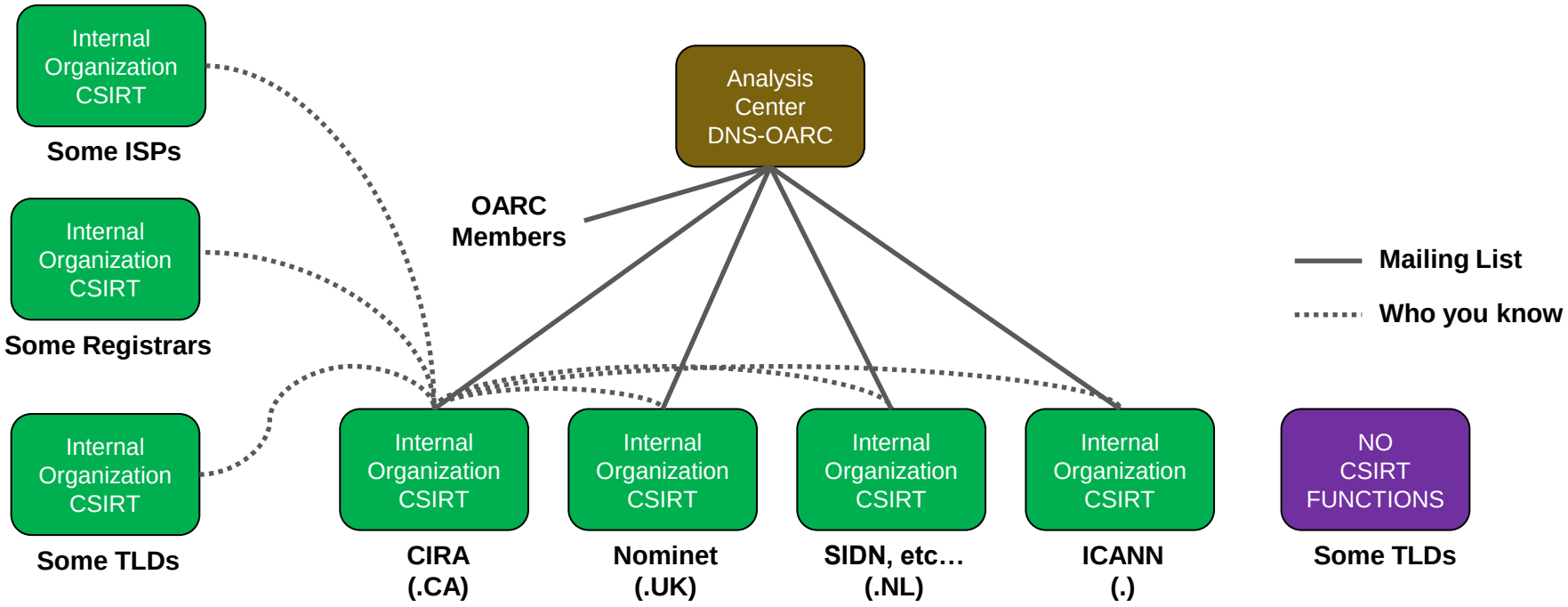
# Current CSIRT Operational Framework
# Ad-hoc




We have limited access to all participants in our Canadian ecosystem

# Current CSIRT Operational Framework DNS Related

- We have limited access to all participants in our global DNS ecosystem



# CIRA - Challenges

## Some of our challenges…

- Unable to contact all ISP CSIRTs in Canada
- Unable to contact all ccTLD / TLD CSIRTs in the world
- Unable to contact all .CA domain holder CSIRTs
- We need to subscribe for security advisories with every vendor
- We need to subscribe to National CSIRTs (CCIRC, CAN-CERT)
- We need to subscribe to subject matter analysis centers (DNS-OARC)
- Unable to contact individual organization CSIRTs in Canada
- Who do we tell if we discover a major incident?
- Who do we accept "security incident service requests" from?
- Do we really have access to all CIRA Registrar/Registrant CSIRTs?
- WHOIS does not necessarily provide the right contacts

## We're missing a CSIRT registry….

# CSIRT Registry Concept

- A tool for Coordination Center to reach CSIRTs
- An authoritative registry of CSIRT contact information
- Each ccTLD hosts a CSIRT registry
- Global and national CSIRT Coordination Center use the CSIRT registries to disseminate information
- Internal CSIRT can locate CSIRT Coordination Centers
- Secure CSIRT-WHOIS type interface
- Secure CSIRT portal with role-based access
- A secure EPP type interface for WHOIS queries and building email lists
- Secure mailing lists generation for Coordination Centers

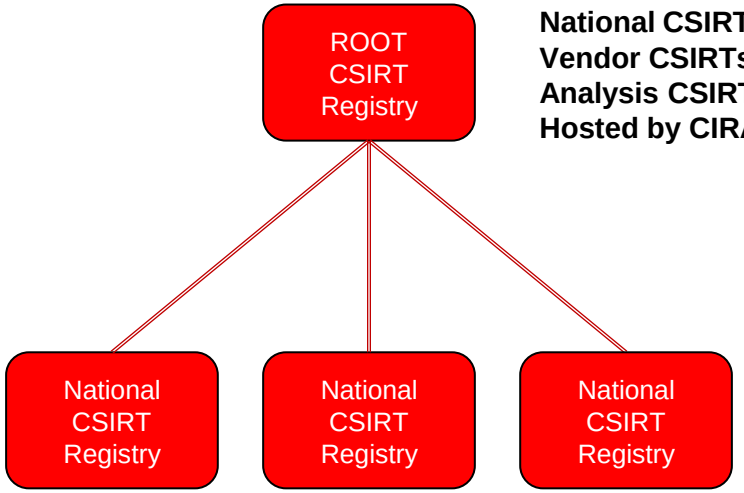
**Focus**

**YES : CSIRT Contact Management**

**NO: Security & Content & Trust Model**

# CSIRT Registry Framework
# CSIRT Hierarchy

- Just like DNS, there would be a need for a ROOT CSIRT registry
- ccTLD operator could operate the National CSIRT registry




**National CSIRT Registries**
**Vendor CSIRTs**
**Analysis CSIRTs**
**Hosted by CIRA in Canada?**

**Internal CSIRT Registry**
**Internal CSIRT/CC Registry**
**Hosted by each country**

**Global Framework**

# CSIRT Registry Concept

- A certified CSIRT/CC has access to all CSIRT information
- A CSIRT has access to all CSIRT/CC information
- High level of confidence in information accuracy
- A method for annual manual registration verification
- Businesses register their CSIRT with their National CSIRT registration authority
- There is a cost to Operate
  - i.e. '$50'/year for registration maintenance
- A root CSIRT registry (hosted by CIRA to start)

**The CSIRT Registry is a non-public infrastructure**

# CSIRT Registry Concept

- Type/Example of CSIRT WHOIS queries;
  - Global CSIRT/CC (give me all the National CSIRTs)
  - ISPs for a country
  - National CSIRT/CC for a country
  - Vendor CSIRT for a country
  - Analysis Center CSIRT for a country
  - All Banking CSIRTs for a country
  - Provincial Government CSIRTs
  - Municipal CSIRTs
  - CSIRT for a specific domain name (via DNS)
  - CSIRT for a specific IP address network (via RIR/LIR)

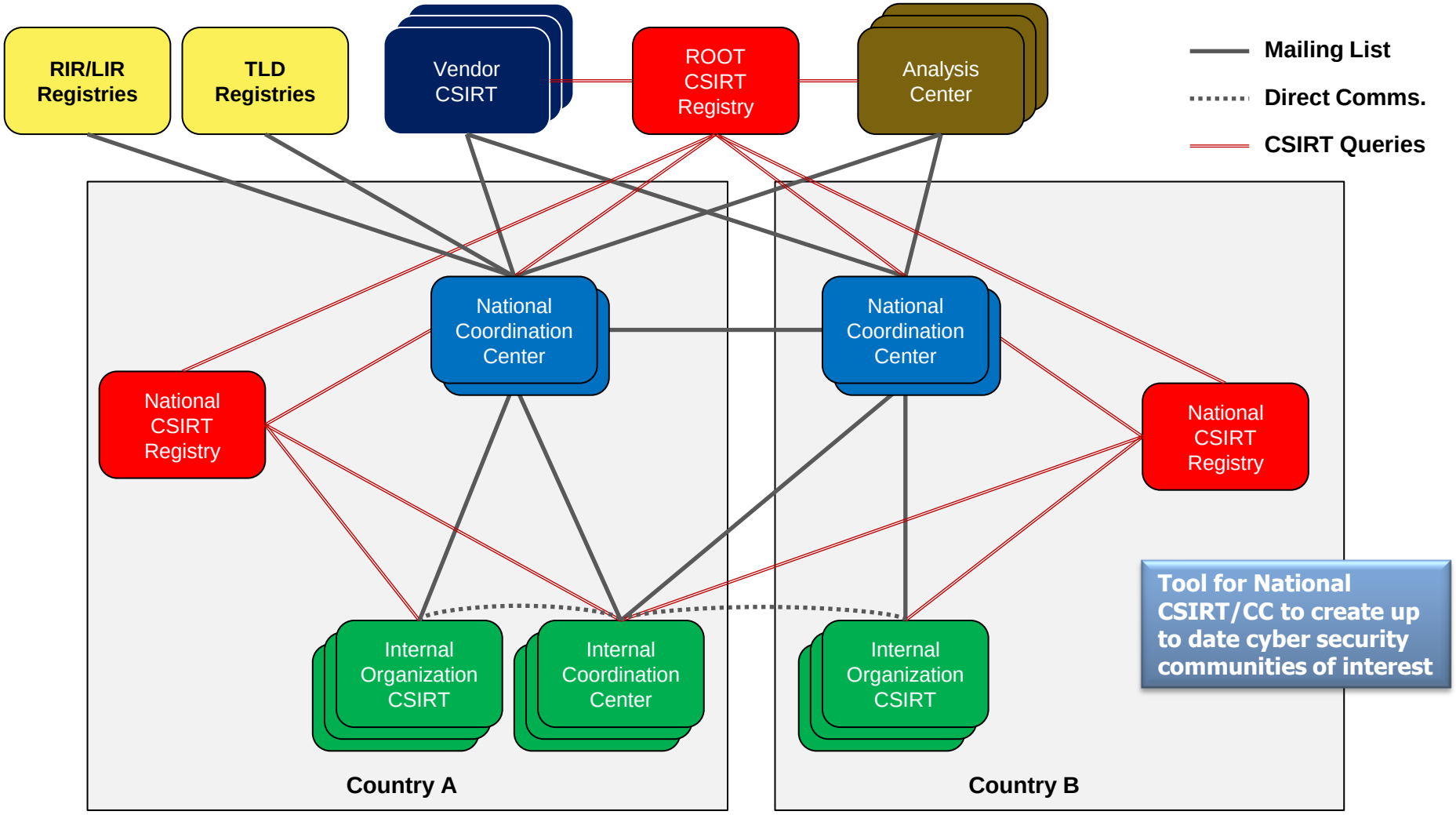
**A tool for CSIRT Coordination Centers**

# CSIRT Registry Concept

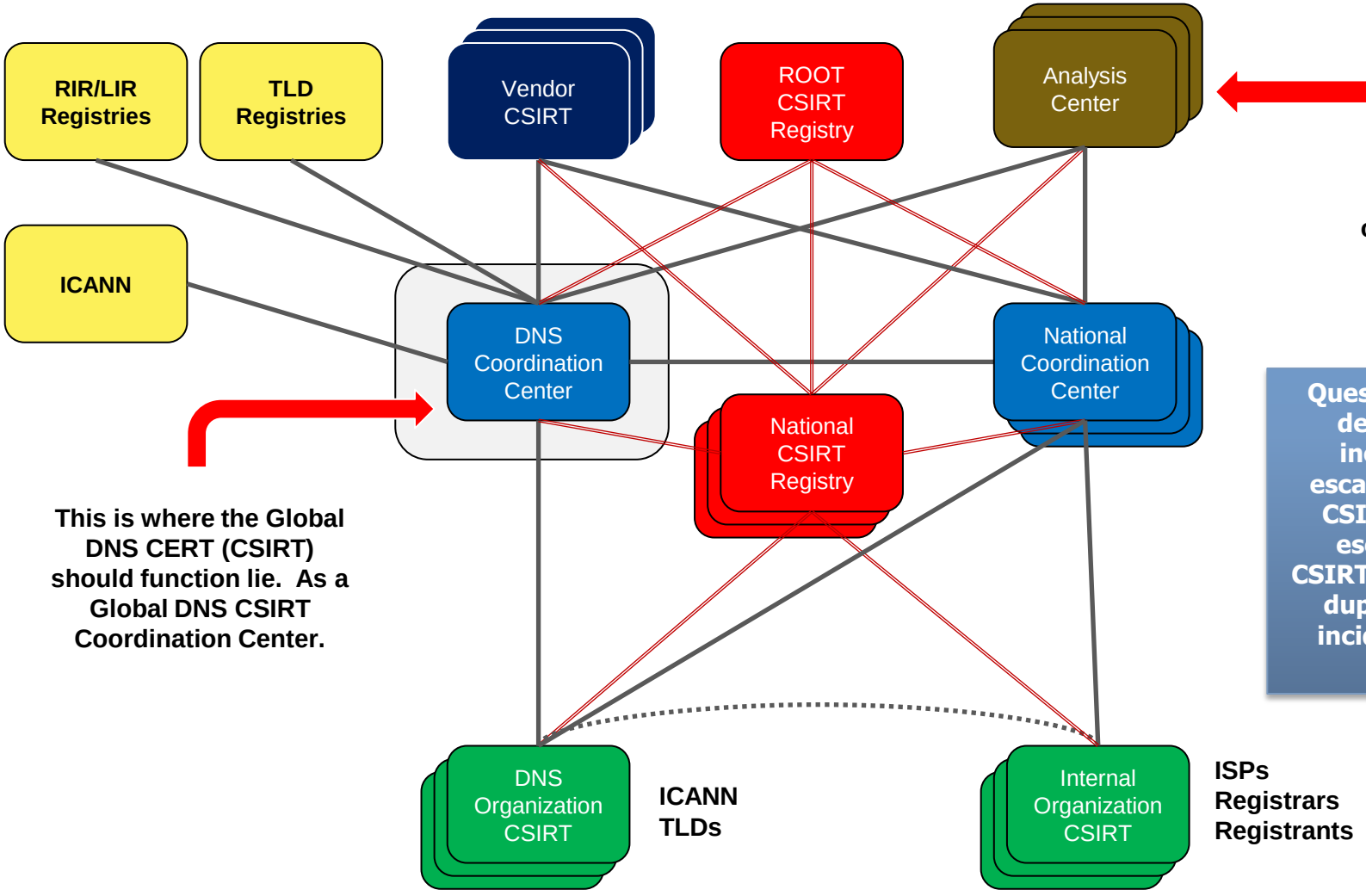
Example of the type of information held in the registry

- Company/Organization
- Type of Business
  - Banks
  - Law Enforcement
  - Government
  - Hydro
  - ISP, Telco
  - Etc..
- Role:
  - CSIRT/CC (Coordination Center)
  - CSIRT/Internal (Incident Response)
  - CSIRT/Vendor
  - CSIRT/Analysis Center
- Secure email addresses
- Contact Information
  - Admin, Technical
- Operating Countries
- Domain(s) under control
  - xyz.ca
- Security profile (?)
  - This defines the subject matter expertise by vendor/technology
    - Red Hat, Cisco, IBM
    - Phishing, Spam
    - DNS

# CSIRT Registry Framework



# CSIRT Registry Framework
# DNS Related



# Next Steps

- Socialize the idea and concept with subject matter experts
  - √ Canadian CCIRC
  - √ DNS CSIRTs (.UK, .NL, etc…)
  - √ Analysis Center (DNS-OARC, Defence Intelligence, InternetIdentity)
  - √ ISC (Paul Vixie)
  - √ CERT/CC
  - – Enforcement agencies (Sûreté du Québec, RCMP, FBI)
  - – ICANN, FIRST
  - – ISPs CSIRTs (Bell, Rogers, Videotron, Telus)
  - – Business CSIRTs (BMO, RBC, Bombardier, Government)
  - – Security subject matter experts
- Update the concept with new ideas & feedback
- Assess prototype development for Canada's CSIRT (CCIRC, Public Safety)

# Contact Information

Jacques Latour
Director, Information Technology
Canadian Internet Registration Authority
350 Sparks Street, Suite 306
Ottawa, ON K1R 7S8
Office: 613 237-5335 x294
Mobile: 613 291-1619
Email: jacques.latour@cira.ca

**MERCI / THANK YOU**