NZ TICSA - Impact on Small (W)ISPs

Presenter: Chris Macneill

TICSA ????

- Who has heard of TICSA?
  - a.k.a. **NZ Telecommunications (Interception Capability and Security) Act 2013**
- Why should I care?
  - Failure to comply could cost you > $2,000 a day!
- What are the chances of getting caught?
  - With few customers less likelihood of being served with a Warrant, but may still be caught if Registrar does an audit.

Legalese / Summaries

- Disclaimer – Opinions stated are my own and Network Operators may need to seek specific legal advice.
- TISCA written in legal speak, hard to translate to Technical specifics, hence ambiguous and contradictory.
- Summaries
  - Any summary is the author's interpretation of the Act, needs actions to proceed before Courts for interpretation and precedents to be made.
  - TCF (NZ Telecommunications Forum)
    - Has guidelines for 2009 TICA, but not updated for 2013 TICSA, so irrelevant.
  - GCSB/NCSC
    - Only covers Part 3, refers to NZ Police for Part 2 guidance. Basically a wordy rewrite of Part 3, doesn't really give any additional insight.
  - NZ Police
    - seems to confuse wholesaler / retailer responsibilities?
    - interpretation seems broader than the Act implies.

The Act

- Part 1
  - General preamble, definitions etc.
- Part 2
  - Lawful Intercept
- Part 3
  - Security risk reporting.
- Part 4
  - Registration, enforcement and misc.

Who is affected (Part 2)?

- ✗ If all services are re-labelled wholesale services e.g. 2Talk, Voyager

- ✗ If you've applied for and received an exemption.

- ✓ If you own or operate a Data or Telecomms Network located in New Zealand and provide those services to another entity or end user and....
  - ✓ Network contains a VoIP, Email or AAA* server.

  *AAA = Authentication, Authorisation, Access Control, i.e. RADIUS and/or DHCP or other server that provides IP addresses and network access.

- ✓ If you provide application services to NZ based end-users, irrespective of the application server location.

Exemptions / Work Arounds (Part2)

- A Network Operator can apply for an exemption
  - Multiple applications for exemptions can be made, but each one must be materially different in order to be considered.
  - If Registrar rejects application for exemption, appeal to Minister.
- Migrate to “white label” services, however Wholesalers are entitled to charge resellers for TICSA compliance.
- Sell your business to someone else and let them worry about TICSA.

Obligations (Part 2)

- Lawful Intercept
  - Two levels defined where customer numbers are below or above an average of 4,000 in a rolling 6 month period.
    - < 4,000 only required to be "Intercept Ready".
    - >= 4,000 required to be "Intercept Accessible".
    - Must record customer numbers on same working day each month.
    - When customer average exceeds 4,000, 10 working day window to report to Registrar.

Lawful Intercept Detail

- “Intercept Ready” (< 4,000 customers)
  - Network operators are required to:-
    - reserve bandwidth.
    - reserve rack space.
    - reserve a connection port.
    - agree on a format for intercepted data to be forwarded.
    - document how Lawful Intercept will performed.
    - maintain the “readiness” capability at all times.
    - co-operate with periodic readiness testing.

Lawful Intercept Detail

- “Intercept Accessible” (>= 4,000 customers)
  - Basically the same as “Intercept Ready”, but intercept capability must be fully implemented, connected and available.
- Forwarding Format
  - Raw data and associated meta-data is required to be packaged and forwarded in near real time in ETSI format or another format as agreed with the Registrar, CALEA format <u>not</u> acceptable.

General Exemptions (Part 2)

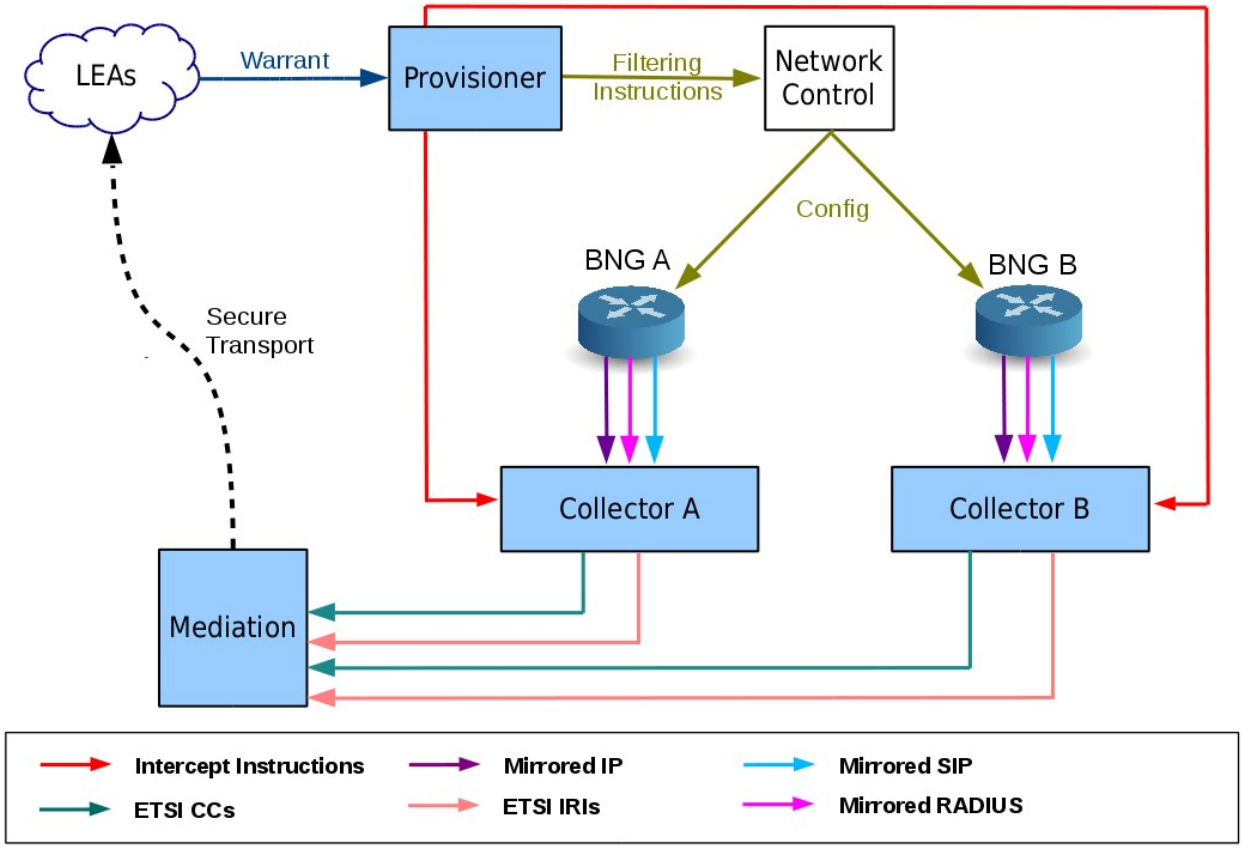
- The Registrar has granted a general exemption relaxing the reporting period of 6 monthly to 12 monthly.
- Network Operators still required to notify when customer numbers breach theshold.

Solutions for Lawful Intercept

- Existing ETSI LI solutions
  - Very expensive, 5/6 figure sums
  - Not fully implemented
  - Not scalable

- Use OpenLI
  - “Free” (but contributions happily accepted)
  - Initially “Wire level” intercept targetting IP and SIP traffic, may need further developemnt at application layer for encrypted Email.
  - Open Source and initial development NZ based by Shane Alcock @ WAND (Waikato University).
  - On target for initial rollout to “foundation contributors” in June 2018.
  - Projected public availability from 2nd half 2018, but may require customisation/integration work for specific network architectures.

OpenLI Architecture



Contradictons (Part 2)

- Monetary Compensation
  - Section 115 allows for actual and reasonable costs to be recovered for assistance under Section 24.
  - Section 116 excludes costs under Section 24.

Who is affected? (Part 3)

- Network Security
  - Network Operators that have 1 or more customers in any of the following categories are required to comply, but there may be exemptions.
    - Central or Local Government
    - Finance, Energy or Food Sectors
    - Communications, Transport, Health or Education Services
  - General exemption
    - for equipment/services installed before 2014
    - generic like for like replacement of equipment
    - day to day maintenance

Obligations (Part 3)

- Network design or hardware changes must be notified and approval received <u>before</u> implementation.
  - Only required where new manufacturer is used or where product from existing manufacturer is substantially different, e.g. different processor or firmware/software family.
- Examples
  - ✓ "AN Other" hardware replaced by MikroTik.
  - ✓ RB2011 replaced by Cloud Core Router (different CPU).
  - ✓ Replace RouterOS with OpenWRT.
  - ✗ RB750 replaced by RB2011 (both mipsbe CPU).

NZNOG 2018 – TICSA Presentations

YouTube – NZNOG 2018 Session 3

- GCSB/NCSC – 00:45:30
- NZ Police – 01:01:30
- OpenLI – 01:25:00

Summary

- If TISCA defines you as a Network Operator, you must:-
  - Register with NZ Police
  - Become LI Accessible/Ready
  - Communicate with GCSB / NCSC
  - Apply for exemptions where appropriate

- Resources
  - CMIT Consulting
    - Assistance with submission of exemption requests
    - Security Assessments
    - Documentation
    - Integration
    - LIaaS ???
    - Be "Security Cleared" interface with NCSC/GCSB ???