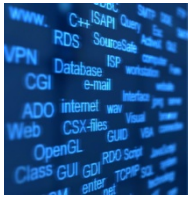
Centre for Critical Infrastructure Protection

Barry Brailey

Operations Lead



23 September 2010

National Lifelines Forum

Overview and Update

New Zealand Government

CCIP

Disclaimer

- We apologise for the profuse usage of the word “Cyber” during this presentation!
  - Core business for years!

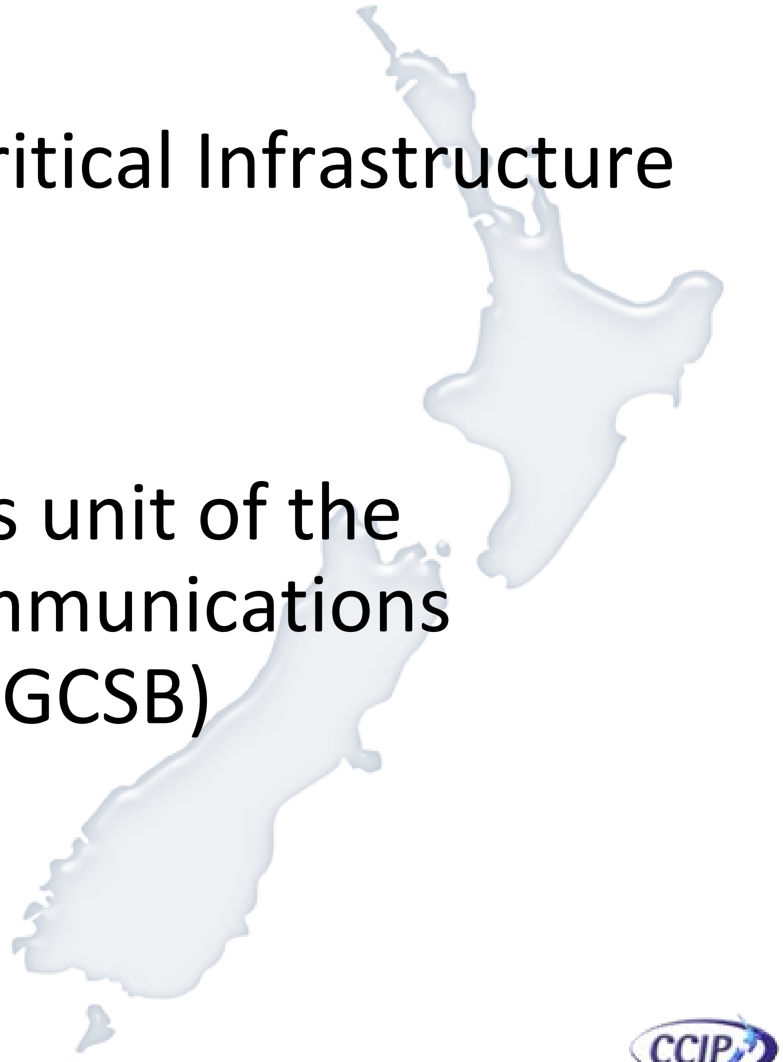
Contents

- Introduction
- National Cyber Security Initiatives
- CCIP Current Work
- Exercise Cyber Storm III
- National Cyber Incident Coordination Plan

Who is the CCIP?

The Centre for Critical Infrastructure Protection (CCIP)

CCIP is a business unit of the Government Communications Security Bureau (GCSB)



CCIP Mission and Vision

- Mission
  - CCIP is dedicated to improving the protection and computer security of New Zealand's Critical National Infrastructure (CNI) from cyber based threats.

- Vision
  - To be recognised nationally and internationally as an authority and a leader on cyber security.

National Cyber Security Initiatives

- Working towards Cyber Security Strategy
- Initial proposal approved by Cabinet
- Strategic Policy Lead and Operational Lead Agencies appointed
- Detailed Business Case for NCSC
- GCSB implementing new structures, SOPs etc

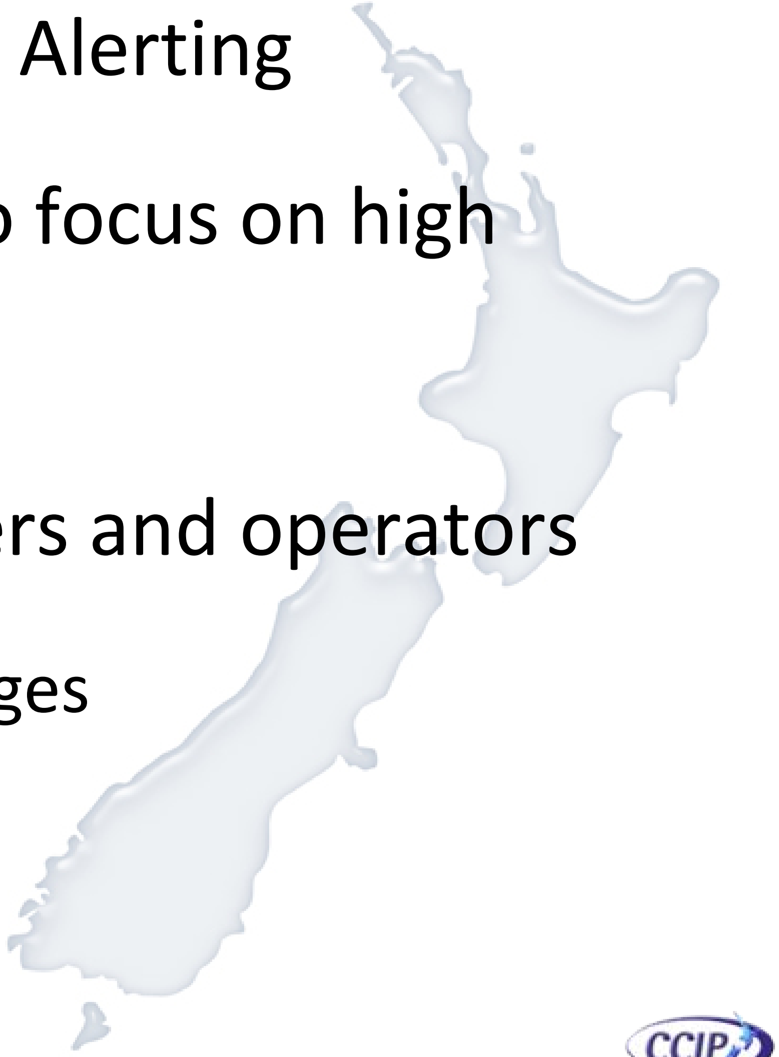
What is CCIP’s involvement?

- Cyber Security is CCIP core business
- CCIP functions and activity feature heavily in current plans
- Transitioning into a Cyber Security focussed Division/ Directorate
- Business case to address resourcing and build upon current work

CCIP’s Current Work

- Domestic Focus and Review
  - Cutting costs can present opportunities!
- Back to Basics
  - Achieving the mission
  - Raising the game
- Looked for Value Adds for NZ and CNI
  - “More with less”
  - Cyber Focus

So what’s changed?

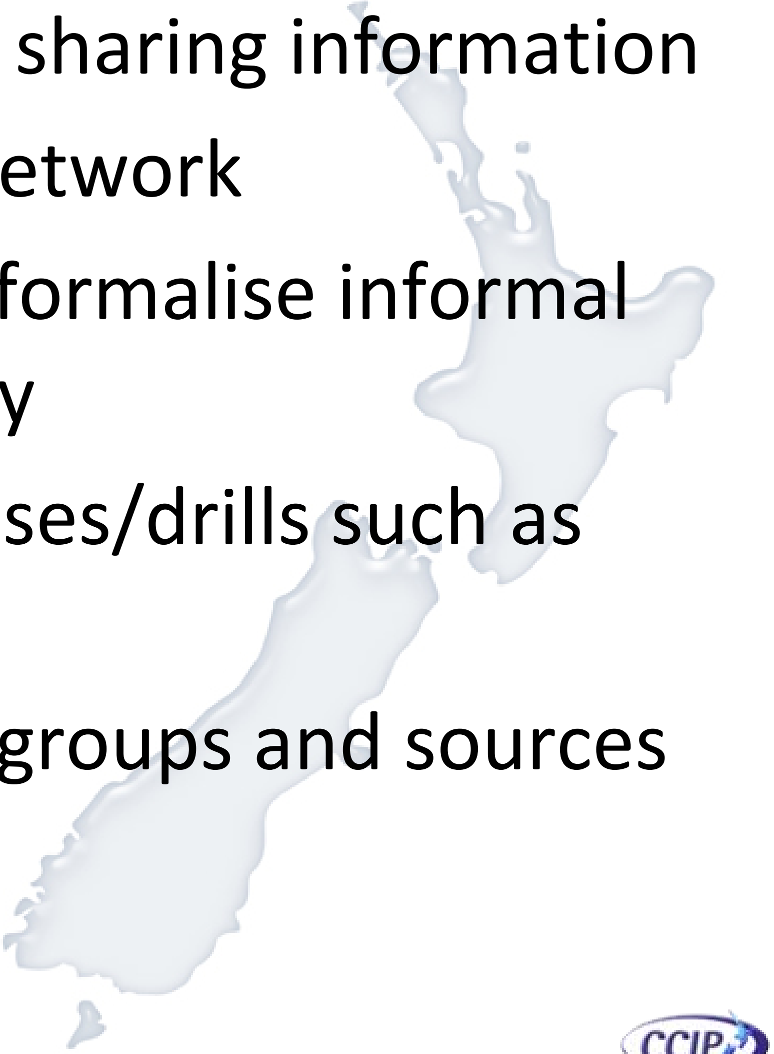


- Transitioned to Exceptional Alerting
- Freed up some resources to focus on high value work
- Re-engaging with CNI owners and operators
  - Security Information Exchanges

Security Information Exchanges

- CCIP’s approach to Information Sharing is establishing Security Information Exchanges (SIE’s) for either sector based groups or common interest groups
- SIE’s are built upon Trust
  - Active Membership
  - Closed forums
  - Membership is a privilege not a right
  - Equal Membership
  - ‘Two-Way Street’

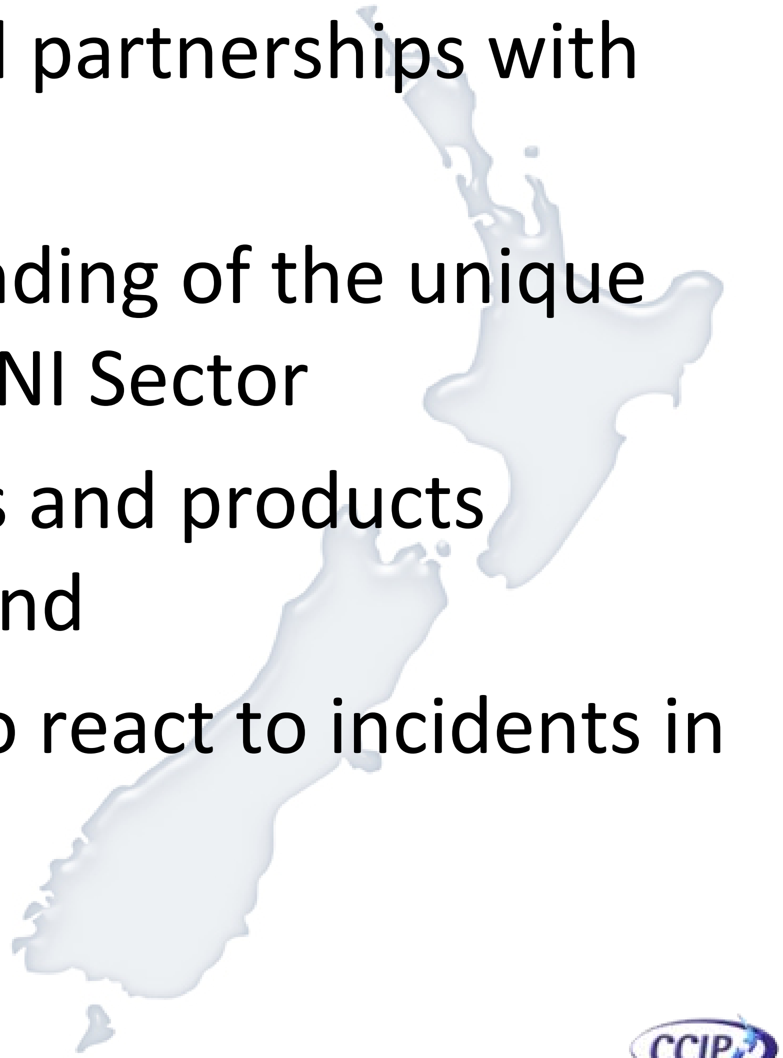
Benefits to Industry



- Provide a trusted forum for sharing information
- Provide a trusted support network
- Provide the opportunity to formalise informal relationships within industry
- Involvement in cyber exercises/drills such as Cyber Storm III
- Access to the International groups and sources of information

Benefits to CCIP

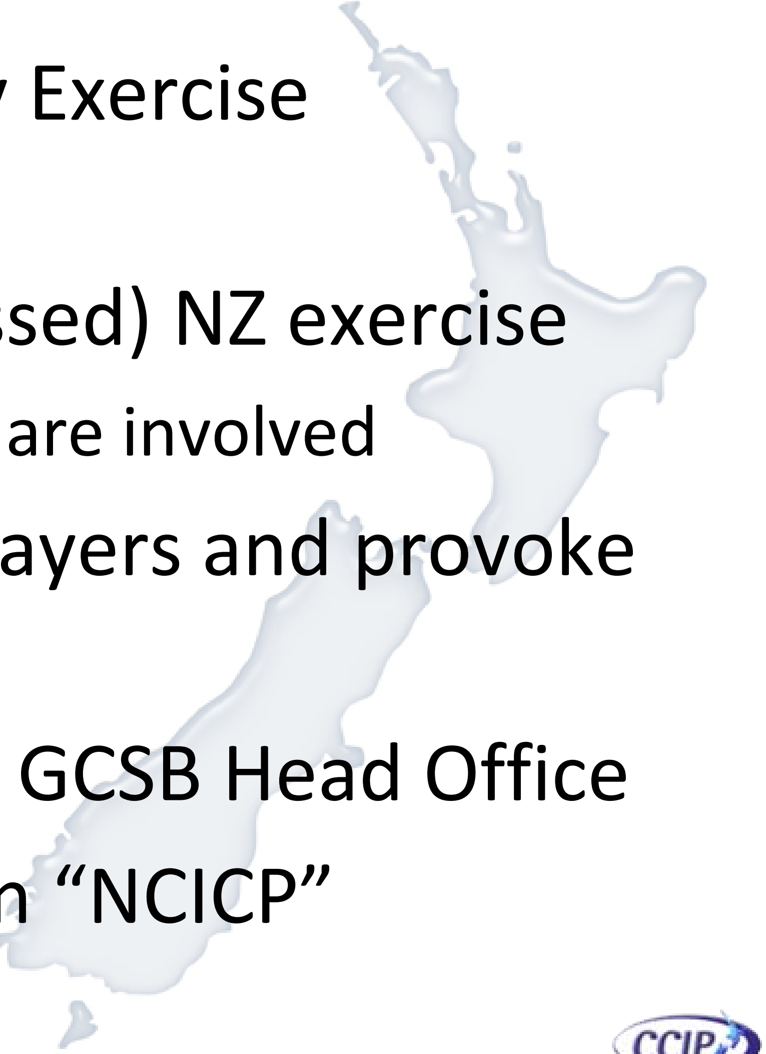
- Formalise relationships and partnerships with industry
- Develop a better understanding of the unique security issues faced by a CNI Sector
- Visibility of the key systems and products deployed across New Zealand
- Trusted points of contact to react to incidents in a timely manner



Security Information Exchanges

- Existing
  - New Zealand Internet Task Force (NZITF)
  - Network Security Information Exchange (NSIE)
  - Control System Security Information Exchange (CSSIE)
  - Internet Fraud Forum
- Upcoming
  - Financial Sector Security Information Exchange (FSIE)
- Future
  - Other Sector SIEs?
  - Regional Cross Sector SIEs (XIEs)?

Exercise Cyber Storm III



- International Cyber Security Exercise starting…. very soon
- CCIP coordinating (SIE focussed) NZ exercise
  - FYI - A lot of your companies are involved
- Realistic scenarios to test players and provoke further initiatives
- Wellington ExCon – ~~NCMC~~ - GCSB Head Office
- Start discussion and work on “NCICP”

National Cyber Incident Coordination/ Handling Plan

- “Update/ formalise current plans”???
- Align with Emergency/ Crisis Management Plans
- RWC 2011 – deadline
- Requires broader planning consultation
  - Hope to engage with MCDEM, TEPF etc

Thanks for your attention

Any Questions?