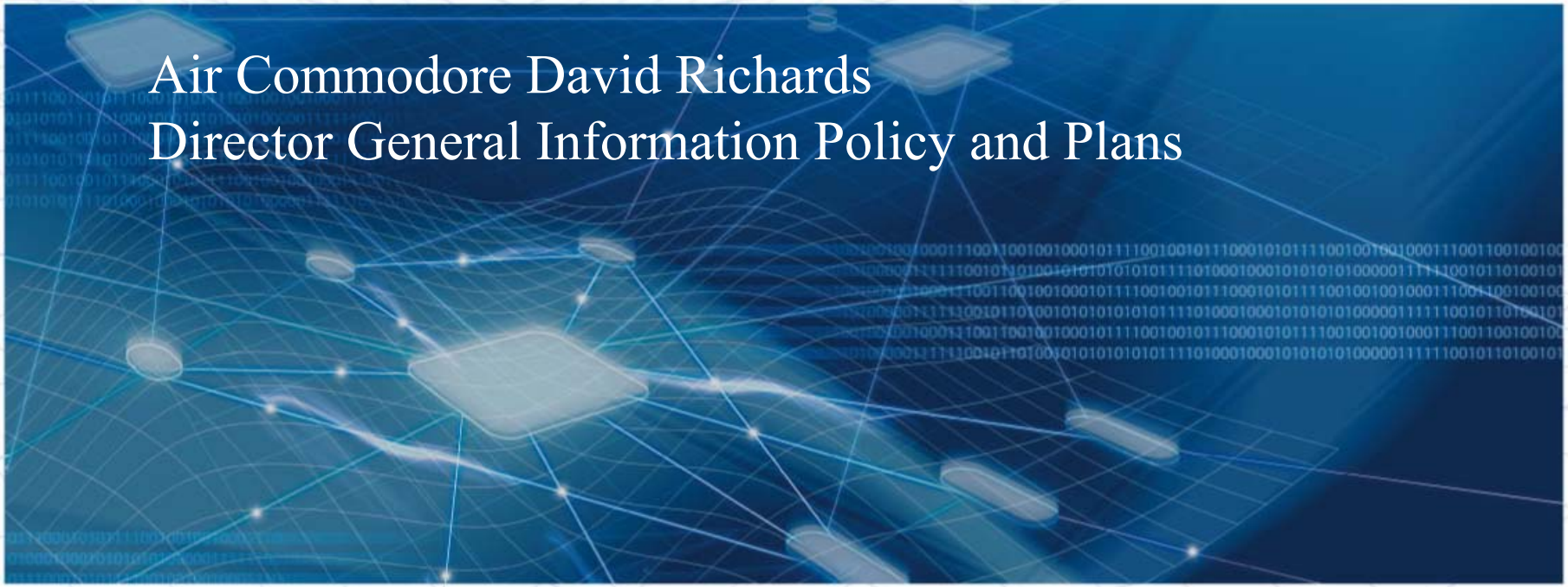
Australian Government
Department of Defence
Chief Information Officer Group

Chief Information Officer Group

Australian Department of Defence's Transition to IPv6



Air Commodore David Richards
Director General Information Policy and Plans

Defence IPv6 Policy

Department of Defence
DEFENCE INFORMATION MANAGEMENT POLICY
INSTRUCTION NO 1/2005
22 February 2005

DEFENCE INFORMATION ENVIRONMENT—TRANSITION TO INTERNET PROTOCOL VERSION 6 (IPv6)
Policy
1. The Defence Information Environment (DIE) will transition from the current Internet Protocol (IP) version 4 (IPv4) to IPv6 and all DIE networks are to have completed transition to IPv6 by the end of 2013. All capability management, development and acquisition staff are to address DIE IPv6 interoperability requirements when developing their architecture in accordance with the Defence Architecture Framework and when implementing associated projects.

Key policy points

- All Defence Information Environment (DIE) networks
  - *Defence Restricted Network (DRN)*
  - *other classified networks*
  - *'Edge' networks*
- 2013 target date
- Tech refresh approach
  - *Hardware*
  - *Software*

Why Transition to IPv6?

- Net-Centric Warfare
  - *Increasing number of entities sharing information*
  - *Increased need for address space*
- Continued Interoperability with key allies
  - *US Department of Defense will transition in 2008*
  - *UK transitioning by 2012-14*
- Emerging technology
  - *The 'killer application'*
- To keep connected
  - *Business & industry*
  - *Internet*
- IPv4 is expected to become difficult to support
  - *Applications*
  - *Operating systems*

Why 2013?

- There is no absolute reason to transition now
- 2013 is a target date derived by balancing the transition risks
  - *Technology/standards evolving*
  - *Industry support*
  - *Our acknowledged immaturity*
  - *Leverage of the experience of our Allies*
- Refresh and replacement cycles

The BIG picture

- Adoption of IPv6 is more than just replacing technology
- Many aspects of the Defence Information Environment will be affected by IPv6:
  - *Leadership*
  - *Transition Management*
  - *Policy and Doctrine*
  - *Logistics*
    Training
    Personnel

IPv6 Challenges

- Transition planning needs to coincide with technical refresh cycles without degrading functionality
  - *Evolving products*
- Maintaining interoperability during and after transition
  - *US DoD, major allies*
  - *Australian Government agencies*
  - *Industry*
- Security
  - *Threats and vulnerabilities*
- Standards
  - *Not all Standards and RFCs are available*

IPv6 Issues

- Transition office
  - *Funding*
  - *Personnel*
- Progress to date
- Compliance by acquisition authorities
- Address block
  - *Size (/20?)*
- Applications
  - *Numbered in the thousands*
  - *BESPOKE*

Industry Engagement

- Engaged with ADIESA during 2006
  - *Confirmed Defence transition to IPv6 is going to happen*
  - *Opportunity for Industry to influence Defence's transition*
  - *Forum to share ideas*
  - *Starting point for an ongoing relationship with Industry*

Transition Office

- Transition Office to be established during 2007
  - *Dedicated team to focus on the task*
- Principle tasks include:
  - *Overhaul the Transition Plan*
  - *Develop an Action plan: who, what, where , when*
  - *Acquire address space*
  - *Develop an address architecture*
  - *Develop a Risk Management Plan*
  - *Audit of existing ICT infrastructure*
  - *Investigate and resolve Security and Information Assurance issues*

Conclusion

- IPv6 will be a key enabler for the ADF's NCW aspirations
- Interoperability with our Allies is a key requirement
- Defence has started on the road to transition and will continue to engage with industry

Australian Government

Department of Defence

Chief Information Officer Group

Branch / Division