Australian Government

Department of Finance and Deregulation

Australian Government Information Management Office

A Strategy for the Implementation of IPv6 in Australian Government Agencies

July 2009

Version 2

For General Distribution

AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE (AGIMO)

A Strategy for the Implementation of IPv6 in Australian Government Agencies

July 2009

Version 2

For General Distribution

AUSTRALIAN GOVERNMENT INFORMATION MANAGEMENT OFFICE (AGIMO)

ISBN 978-1-921600-05-0

Department of Finance and Deregulation
Australian Government Information Management Office

This publication is intended for use by Commonwealth agencies to form the basis of a common language between agencies.

Acknowledgements
Photographs taken by Steve Keough, Steve Keough Photography
Copyright: Department of Finance and Deregulation

Contents

Foreword

While there are no critical business drivers forcing the Australian Government towards IPv6 in the short term, the enablement of IP telephony and digital wireless networks by ubiquitous IP-based networks, the shift to IP-based communications, and the adoption of e-business strategies across numerous other technologies, are all putting pressure on the available IPv4 address space.

Throughout 2008, attention surrounding the depletion of the IPv4 address space, currently predicted to occur at end of 2010-11, increased. The depletion of IPv4 address space has implications for all levels of government and industry.

The Australian Government has already initiated a whole-of-government action plan to ensure that citizens' access to online government services is sustained during agencies' transition from IPv4 to IPv6-based platforms.

IPv6 capability is available in all contemporary communications and network infrastructure. Industry has indicated that it expects to supply dual capable IPv4 / IPv6 equipment for the foreseeable future. In the next three to five years, industry expects that equipment and services based on the IPv6 set of standards will become dominant.

Although IPv6 network traffic will dominate, it is anticipated that Australian Government agencies will be required to sustain IPv4 network traffic for at least the next ten years.

The purpose of this strategy is to assist agencies and interested parties by providing guidance on the steps that the Australian Government is taking to plan and manage the transition from IPv4 to IPv6. Co-ordinated planning of the transition allows agencies to take advantage of the features of dual capable IPv4 / IPv6 platforms as they become available, while providing time to undertake the necessary training of staff and testing of systems.

The Department of Finance and Deregulation, through the Australian Government Information Management Office (AGIMO) monitors agency progress through regular surveys and report to government on the progress of agencies' preparedness for IPv6-based service delivery.

Ann Steward

Australian Government Chief Information Officer
Australian Government Information Management Office
Department of Finance and Administration

July 2009

one Introduction

one

1 Introduction

A Strategy for the Implementation of IPv6 in Australian Government Agencies was first prepared for the Australian Government Chief Information Officer Committee (CIOC) in 2007. The Strategy was distributed to all Australian Government agencies, and made publicly available in January 2008. The Strategy proposed that all Government agencies should have IPv6 capable hardware and software platforms by 2012 and be able to operate dual stack IPv4 / IPv6 environments by 2015.

A revised IPv6 transition strategy was endorsed by CIOC in January 2009. The revised strategy sees agencies having their IPv6 ready hardware and software in place by end 2011 and having all systems IPv6-enabled by end of 2012.

Issues relating to the implementation of IPv6 in an Australian Government context include:

- Government services remaining accessible to all citizens, regardless of whether they are using IPv4 or IPv6;
- Agencies being able to access web based services, regardless of whether they are provided over IPv4 or IPv6;
- The risk that unplanned and uncontrolled implementation of IPv6 equipment into government networks could compromise service delivery capability;
- The risk that the skills shortage in the ICT arena and in particular, the IPv6 field, may increase to the point that the government will not be able to engage suitably qualified IPv6 skilled technical and administrative staff;
- The opportunities for enhanced service delivery, particularly in the health, environment and transport industries, that IPv6 will allow with its ability to have multiple sensor / tracking devices in a variety of fields; and
- The risk that the cost of moving to IPv6 when industry and suppliers are driving the market will be significantly greater than if the whole-of-government transition is undertaken in a planned way.

The IPv6 transition strategy will be reviewed annually to take into account advances in IPv6 technologies, industry developments, lessons learned from similar implementations and the progress of agencies in implementing the strategy.

two Stage 1: Preparation

two

2 Stage 1: Preparation

The preparation stage of the Strategy will see agencies plan, conduct, and manage the following activities in preparation for transition to IPv6:

- **Review Procurement Policy**

Agencies should ensure that IPv6 capability is reflected in agency procurement process guidance.

- **Stock take of Equipment**

Agencies should undertake a comprehensive hardware stock take. International experience shows that such a stock take is vital to an agency understanding its current state of IPv6 readiness and to the preparation of an agency-specific transition timeline.

- **Stock take of Applications**

Agencies should determine the priority of upgrading specific applications. They should consider issues such as how critical the application is to the agency's ability to deliver services.

- **Progressive installation of IPv6 Capable Equipment**

Agencies may commence the replacement of their IPv4-only capable equipment as part of their regular ICT refresh cycle during this stage.

- **Training and Training Needs Analysis**[1]

Agencies should liaise with their suppliers of hardware and software to ascertain what training is relevant, required and available for their staff.

AGIMO will liaise with agencies to determine a whole-of-government IPv6 training curriculum for agency managerial and technical staff.

- **Threat and Risk Assessments (TRAs)**[2]

Agencies should ensure that that IPv6 related security threats and risks are considered as part of the regular Threat and Risk Assessments of their networks.

Elements of many of these tasks are ongoing, but their planning and commencement should be undertaken by end-December 2009.

1 Training and the Training Needs Analysis are 'Business as Usual' tasks in that they will be ongoing for the life of this project and beyond.

2 The Threat and Risk Assessment is to a 'Business as Usual' task in that it will be ongoing for the life of this project and beyond.

three Stage 2: Transition

three

3 Stage 2: Transition

The transition stage of the Strategy sees agencies planning, conducting and managing the following tasks as they move to a state of IPv6 readiness:

- **Upgrade of ICT Hardware to be IPv6 ready**

Agencies should ensure that all hardware is IPv6 ready unless it is designated as legacy equipment that will run IPv4-only systems. The Network Infrastructure Backbone should be the first hardware segment of the network to be made IPv6 ready. Other segments of the network can be staged as required.

- **Upgrade of Operating Systems to be IPv6 ready**

Agencies' operating systems should be upgraded to ensure IPv6 capability and compatibility.

- **Upgrade of Applications to be IPv6 ready**

Applications should be upgraded to ensure IPv6 capability and compatibility. Agencies should determine the priority of this work based on the level of criticality of the application to the agency's ability to obtain or deliver services.

- **Upgrade of ICT Gateways to be IPv6 ready**

Agencies should upgrade their gateways or liaise with their gateway service provider as to when these devices will become IPv6 ready.

- **IPv6 Certification**

Agencies should ensure that all IPv6 capability has been certified to the appropriate level of security.

At the completion of this stage, agencies will be ready to securely send and receive IPv6 packets of information.

Agencies will progressively undertake the enhancement of IPv4-only capable equipment to be IPv6 capable[3]. Hardware and software upgrades should occur as part of agencies' regular ICT refresh cycles.

Agency network designers and engineers will develop the most suitable strategy for their agency to complete this stage of the transition in a secure and seamless manner.

Elements of some of these tasks are ongoing. Agencies may plan and commence tasks in parallel with the previous stage. The certification of IPv6 capability should be completed by end-December 2011.

TESTING

Agencies are responsible for testing all IPv6 ready hardware and software installed in their ICT environments. Testing of hardware and software will predominantly take place in Stage 2. It will require agencies to enable IPv6 capability to check the readiness of components being tested. The IPv6 capability should be disabled when testing is completed.

[3] IPv6 capability may be provided by equipment operating in a 'dual stack' mode.

four Stage 3: Implementation

four

4 Stage 3: Implementation

The implementation stage of the Strategy sees agencies confirm their IPv6 readiness and commence operations through the following tasks:

- **Agencies to be IPv6 ready**

Agencies will undertake final testing of IPv6 ready hardware and software.

Agencies will ensure that all systems (including applications) are operating as expected and that the desired level of connectivity is achieved.

- **Agency Enablement of IPv6**

Agencies may enable IPv6 capability, subject to the satisfactory conduct of all Threat and Risk Assessments and certification of IPv6 platforms.

AGIMO will consult with agencies on the timing and process of enabling IPv6 across government.

CIOC will endorse the timing and coordinate the approach for agencies to enable IPv6.

- **AGIMO to report completion of Strategy**

AGIMO will report to government on the successful completion of the Strategy, and that the Australian Government is IPv6 ready.

Agency ICT management and technical staff will plan and undertake Stage 3 tasks based on the Australian Government endorsed approach. The implementation of IPv6 across Australian government agencies should be completed end-December 2012.

Agencies may retain some IPv4 hardware and applications as legacy equipment.

five Governance and the Marketplace

five

5 Governance and the Marketplace

The CIOC provides oversight for the whole-of-government implementation of the Strategy. The CIOC has established an IPv6 Community of Expertise (CoE) to:

- Advise on issues that need to be addressed in the Strategy; and
- Share information between agencies regarding the Strategy, transition issues and IPv6 technical issues.

To assist the CIOC, AGIMO will:

- Coordinate whole-of-government reporting;
- Coordinate management of whole-of-government issues;
- Liaise with industry, state and territory governments, and internationally, to ensure that lessons learned are shared with agencies;
- Promote the availability of IPv6 test-bed facilities to all agencies to enable them to undertake specific tests if required; and
- Co-ordinate information sessions and discussions involving government and industry.

Agencies are responsible for the governance and implementation of the Strategy within their portfolios.

THE MARKETPLACE

AGIMO will continue to liaise with industry and service providers as they release IPv6 offerings to the market to ensure that Government has up-to-date information on market trends and timings.

Agencies should work with their suppliers of ICT equipment to ensure that they are aware of the timeframes of the strategy. It is anticipated that suppliers may be able to assist agencies with training, hardware and software stocktaking and the installation of upgraded equipment. For example, IPv6 technical training courses are becoming more readily available and could be provided ‘off-the-shelf’ or configured to agencies’ requirements.