Information Security

Internet Protocol (IP) Address Management

Standard

Agencies with ownership of publically routable IP addresses must:

- have a registered account with the Asia Pacific National Internet Centre (APNIC);
- enter IP ranges associated with the account;
- include the WoVG APNIC account as a contact;
- annually check and update, if required, contact information for IP ranges;
- provide Department of Premier and Cabinet (DPC) with a list of IP address ranges that agencies wish ACSC to assist with identification of IP address in connection with malicious cyber activity; and
- obtain IPv6 addresses via DPC when required.

Keywords:	IP; IPv6; IPv4; IP Procurement; standard, security, APNIC	
Identifier: SEC STD 10	**Version no.:** 1.1	**Status:** Final
Issue date: 18 February 2016	**Date of effect:** 18 February 2016	**Next review date:** 1 March 2020
Authority: Victorian Government CIO Council	**Issuer:** Department of Premier and Cabinet Victorian Government	

Overview

Publically routable IPv4 addresses within Whole of Victorian Government (WoVG) need to be better managed so that IP ranges are not abandoned and are updated with correct contact information. This will assist with proper attribution of alerts from the Australian Cyber Security Centre (ACSC).

Further, agencies will in the future need to transition from IPv4 addresses to IPv6 addresses. This presents an opportunity to provide a continuous IP range with clear attribution and other management advantages.

Purpose

This document is to provide a clear description as to how Victorian Government owned publically routable IP addresses are to be managed.

Requirements

This standard addresses the risks to information and communications technologies (ICT) underpinning government services. Agencies with ownership of publically routable IP addresses must:

- have a registered account with the Asia Pacific National Internet Centre (APNIC);
- enter IP ranges associated with the account;
- include the WoVG APNIC account as a contact;
- annually check and update, if required, contact information for IP ranges;
- provide Department of Premier and Cabinet (DPC) with a list of IP address ranges that agencies wish ACSC to assist with identification of IP address in connection with malicious cyber activity; and
- obtain IPv6 addresses via DPC when required.

Recommendations

It is recommended that agencies:

- Include the agency's Information Technology Security Advisor (ITSA) as a contact on the APNIC account.

Approach

Government Owned IPv4 Ranges

Publically routable IP addresses that are registered to Victorian Government agencies must be managed through an active account with APNIC.

DPC will act as a secondary contact for all Victorian Government IP ranges.

Departments and agencies must at least annually ensure that the contact details for their associated ranges are correct.

This will ensure that the ACSC can correctly attribute ownership of IP addresses in connection with malicious cyber activity and issue alerts accordingly.

The ACSC uses a variety of sources to aid the discovery of malicious cyber activity of interest to the Australian Government and will pass on such information in a timely manner to any known affected agency. While the ACSC do not monitor Victorian Government networks, adherence to the above approach will greatly assist the ACSC in the identification of legitimate owners of the IP addresses.

Third Party IP Addresses used for Government Services

Departments and agencies who use services utilising third party IP addresses may choose to report these addresses to the ACSC via DPC to also assist with identification of IP addresses in connection with malicious cyber activity.

IPv6 Procurement

DPC on behalf of the Victorian Government is considering procurement of a /32 IPv6 range for use across departments and agencies. Victorian Government organisations seeking IPv6 allocations will then obtain these from DPC.

Derivation

- SEC POL 01 Information Security Management Policy; and
- SEC STD 01 Information Security Management Framework
- Victorian Auditor-General's Report of November 2013: WoVG Information Security Management Framework

Scope

This standard applies to all Victorian government departments and Victoria Police, VicRoads, State Revenue Office, Environment Protection Agency, Public Transport Victoria, Country Fire Authority, State Emergency Services, Ambulance Victoria, Emergency Services Telecommunications Authority, Metropolitan Fire and Emergency Services Board and CenITex.

These agencies are referred to as 'in-scope agencies' in this document.

Note: an expanded scope for information security policies is under consideration, and this standard's scope will be updated if needed.

Compliance

Timing

Agencies must:

- complete transfer of IPv4 ranges into their APNIC account within 6 months of the date of effect on the front of this document; and
- check and update IP range contact information at least annually.

Reporting

Until all in scope agencies are registered on APNIC, annual reports must be completed and sent to DPC by the end of December each calendar year. However, no template will be issued for this, as it is expected all in-scope agencies will be registered and using APNIC by December 2015.

Further information

For further information regarding this standard, please contact the Enterprise Solutions Branch in the Department of Premier and Cabinet at enterprisesolutions@dpc.vic.gov.au.

Glossary

Term	Meaning
APNIC	Asia-Pacific Network Information Centre
DPC	Department of Premier and Cabinet
ACSC	Australian Cyber Security Centre
IP	Publically routable Internet Protocol, either version 4 or 6.
IPv4	Publically routable Internet Protocol version 4.
IPv6	Publically routable Internet Protocol version 6.
ICT	Information and Communications Technologies
ITSA	Information Technology Security Advisor

Version history

Version	Date	TRIM ref	Details
0.1	29 April 2015	DOC/15/122355	Draft for review by Business Systems, Policy and Standards
1.0	03 June 2015	DOC/15/122355	Submission to CIO Council for approval
1.1	17 February 2016	D16/23972	