# NT III Discussion Paper

December 2013

## Purpose

Currently the Tasmanian Government procures its wide area data network (WAN) services via what are known as the Networking Tasmania (NT) II agreements. These agreements end in May 2015.

This discussion paper is intended to generate discussion amongst NT II stakeholders, including customers and potential suppliers, on the future requirements that will be delivered under the next generation of purchasing agreements – to be known as NT III. These discussions will be used by the government's contract management organisation, TMD, to help formulate the government's range of business requirements beyond the current arrangements.

To assist in generating the discussion, this paper outlines at a high level:

- Highlights the principles that underpin the current and future NT service frameworks.
- Summarises the current network model and principles.
- Proposes a high-level summary of a future network service model and principles.
- Outlines a roadmap to the next generation arrangements - to be known as NT III.
- Sets out the next steps.

## Background

The Tasmanian Government ICT Strategy articulates, in KPI 3c, a core role of government data network services-

> *"…by 2015 all government staff will have access to all the information and services that they require in order to perform their role, regardless of their physical location and organisational context within government".*

The experience by agencies to date supports the continued use of the whole of government approach that underpins delivery of its current NT II services. The continuation of this approach is also consistent with Objective 5 of the Tasmanian Government ICT Strategy which is to have a common approach to the provision of commodity ICT resources.

Large organisations purchase and manage enterprise data networking services to securely support current and emerging business requirements by:

- Providing secure connectivity between corporate sites and ICT services and thus enable modern business operations
- Managing and protecting against the range of external and internal ICT risks and threats to the organisation's information assets
- Achieving value for money from the endorsed purchasing arrangements.

The Tasmanian Government's wide area network (WAN) and related services are delivered under the current NT II arrangements which are due to end in May 2015.

Since entering into the NT II arrangements in 2007, there have been a number of internal and external influences that have impacted on government's requirements and the expectations of agencies and of staff. These influences include:

- Increasing reliance of data network services to underpin all government business operations – such as the migration of government telephony services onto the WAN.
- The impact of the National Broadband Network (NBN).
- Increase in the use of third party or cloud based ICT services.
- Increasing requirement and expectation by staff for collaboration across the Tasmanian public sector utilising ICT services, combined with greater mobility for users in accessing government ICT resources.
- Increasing expectation of Government that agencies can seamlessly join-up to deliver its public services.
- Gradual exhaustion of IPv4 internet addresses combined with the global adoption of IPv6 internet addresses, highlighting the need to have a planned migration strategy.

All of these drivers are triggers for determining options for the structure of future NT III service arrangements. The end of the current NT II agreements, which include a 12 month transition-out period, is an appropriate and timely trigger to commence the implementation of changes.

The key governance and responsibility arrangements for the development of NT III are:

- The Agency ICT Reference Group is the corporate business owner of the NT arrangements.
- TMD is the responsible government contract management organisation, including procurement.
- The broader context includes the Tasmanian Government ICT Strategy.
- The Office of eGovernment is responsible for coordinating strategic and policy direction.

# National Broadband Network (NBN)

The NBN will impact on the appropriate timeframes and services to be procured under NT III by government in the future. The key NBN questions that need to be considered now are:

1. What speed of NBN services will be available to government customers and where? i.e. which government locations will be connected via the different underlying technologies (either fibre to the premises, fibre to the node, wireless or satellite)
2. What is the NBN rollout timeframe for Tasmania?
3. When will NBN deliver business and enterprise grade services, and exactly what underlying service level agreements will be offered?
4. Where are the final locations of the NBN points of interconnect (POI)?
5. What will be the range and quality of the retail service providers who may wish to deliver services under NT III agreements?

It is anticipated that the NBN will impact on the timing and range of connection services included in NT III. It is unlikely that the NBN will impact on the broader principles and network model of NT III.

# Principles and business model

The following table summarises security and access principles that underpin the current NT II arrangements and that are proposed for NT III.

| Underpinning the NT II model | For proposed NT III model |
|---|---|
| - The network provides a high level of security (availability, integrity and confidentially) of services | - The network provides a high level of security (availability, integrity and confidentially) of services |
| - Where you are and which agency manages the site determines the services you may access.<br>- Physical security in buildings is a fundamental plank of network security.<br>- Agencies apply security protections to separate themselves from other agencies. | - Who you are, not your agency or location, will determine which services you may access.<br>- Physical security will support, not be the foundation of, network security.<br>- Agencies will collaboratively build security frameworks that exhibit trust in each other. |
| - Collaboration is managed by exception to the default security rules<br>- The majority of staff can only access their own agency's services | - Collaboration and mobility is the norm and it is expected and supported<br>- Staff can routinely access whole of government or other agency services, where authorised |

The following examples are currently complex or exceptions under NT II, but will be normal under the principles proposed for NT III:

1. A government employee will be able to have identical access to ICT resources when using end-user computing devices from any government site.
2. Agencies will be able to easily provision and manage access to ICT services by government employees from any agency, when the ICT services utilises the proposed government identity management service
3. All sites, by default, will allow multi-agency collaborative teams to access a range of ICT services, with some ICT services being shared by the team and other ICT services not being shared by the team.

## Current NT II network zones & customer groups

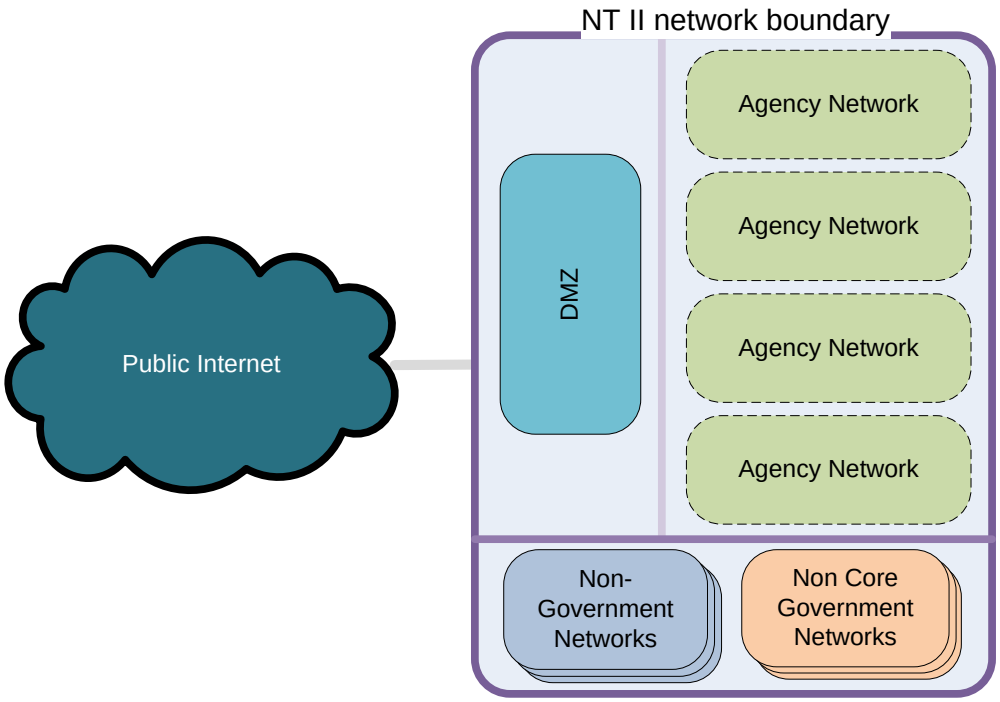


**Figure 1 – The current NT II model - organised by customer groups and networks. Each agency has its own network. To enable collaboration across government, numerous "holes" have been opened in each agency's network.**

## Desired NT III service zones & customer groups

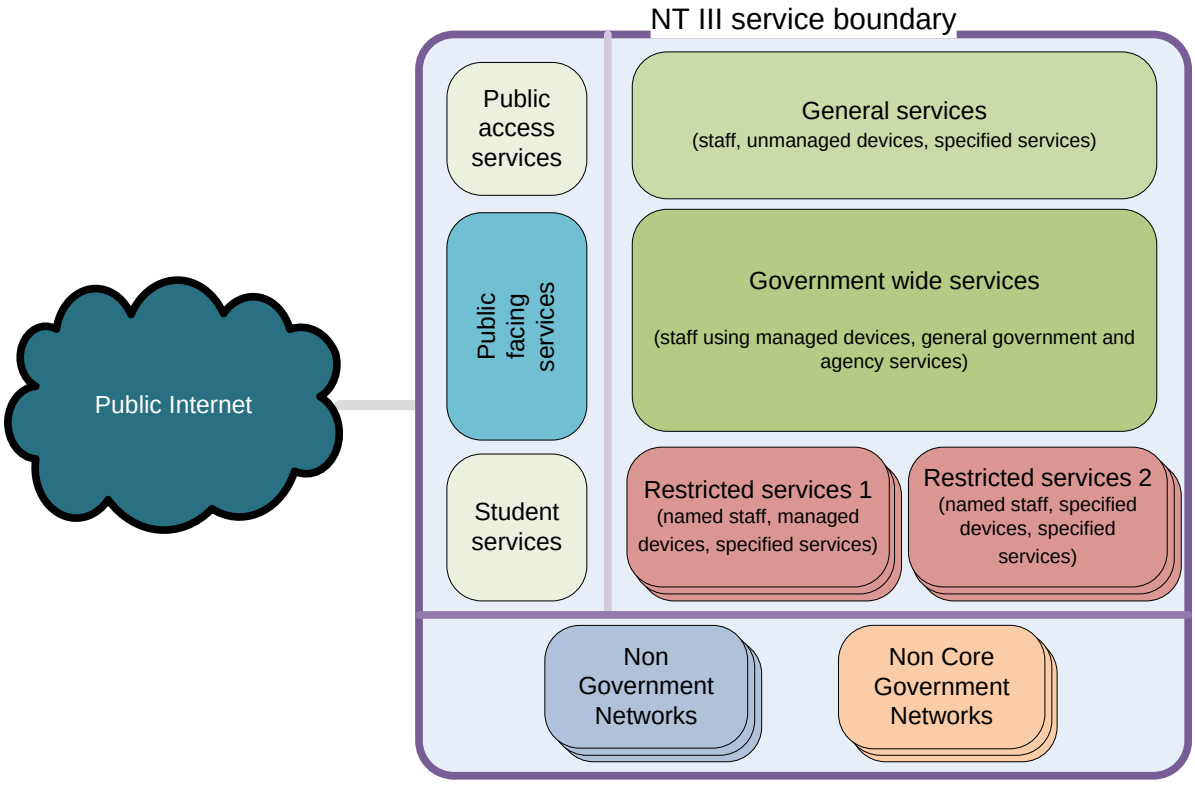


**Figure 2 – The proposed NT III model. Based on most services being appropriately protected by application access controls. However, for higher risk services, restricted service zones will be created.**

# NT III Roadmap

| Activity | Now | Procurement (mid-2014) | Contract Commencement (May 2015) | Completion of transition (May 2016) |
|---|---|---|---|---|
| **Coordination** | | | | |
| **Governance** | Establish | | | |
| **Communications** | Develop communications plan; continue stakeholder engagement | Stakeholder engagement | Stakeholder engagement | Stakeholder engagement and review |
| **Transition plan** | Agreed high-level overview | Defined overview and expectations | Defined, elements progressing | Progressing, elements completed |
| **NT III** | | | | |
| **Service zones** | High level agreement (endorsed by Agency ICT Reference Group) | Defined and linked to identity management and security policy | Established and commence transition | Implemented |
| **Contract structure & service levels** | Draft/agreed overview | Defined. Use in procurement processes / RFT documents | Completed | |
| **Transition plan** | Agreed high-level overview | Defined overview and expectations | Defined | Completed |
| **Scope** | Overview of customer groups<br><br>Overview of services and service boundary | Defined. Inform customers of implications<br><br>Define services and respective boundaries | Commence transition of customers and services | Completed transition of customers and services |
| **Procurement** | Plan approach to procurement | Commence procurement processes | Completed | |

| Activity | Now | Procurement (mid-2014) | Contract Commencement (May 2015) | Completion of transition (May 2016) |
|---|---|---|---|---|
| **Dependent activities** | | | | |
| **Identity management (IM)** | Agreed high-level roadmap that builds on the identity management service developed for government email service. | Defined data quality standards and technical model for the authentication and authorisation service.<br><br>Agreed roadmap and business processes to support data quality. | Implemented technical service to provide network authentication and authorisation service.<br><br>Progression on implementation of roadmap. | Continued progression on implementation of roadmap. |
| **Security policy** | Understand that current NT Security Policy is not fit for NT III purpose. | Agreed scope of policy and standards.<br><br>Defined key essential and desirable standards, including network boundary/endpoint standards, and minimum end user computing / device security standards | Implemented key essential standards, including network boundary standards and minimum end user computing / device standards. | Progressive revision and implementation of desirable standards, including network boundary/endpoint standards, and minimum end user computing / device security standards. |
| **IP Version 6** | Develop the case that timing is right to prepare for IPV6 transition as part of NTIII, IM and related security policy activities | Specify requirement at appropriate point of the procurement cycle and develop rollout plan | Introducing capability and commence rollout | Rollout of IPv6 capability underway as set out in the IPv6 rollout plan |

# Steps

## Planning for procurement

| | What | Who | When |
|---|---|---|---|
| 1. | Confirm Governance framework | OeG | Oct 2013 |
| 2. | Engage consultant to provide expert advice on:<br>- Achievability of service zone model<br>- Implications on NT III scope<br>- Identity management requirements to support of the service zone model and NT service quality<br>- Security policy implications, scope and requirements<br>- NT service boundaries<br>- Implications on contract structure and service levels<br>- Procurement implications<br>- High level transition framework and stakeholder issues | OeG & TMD | Q4 2013/ Q1-2014 |
| 3. | Develop and execute communications plan / stakeholder engagement | OeG & TMD | Q4 2013/ Q1-2014 |
| 4. | Determine contract structure and service level requirements | TMD | Q1 2014 |
| 5. | Develop overview and expectations for transition plan | TMD | Q1 2014 |
| 6. | Define security policies, which TMD and agencies will be responsible for implementing, including essential and desirable standards including network boundary/endpoint standards and minimum end user computing equipment security standards. | OeG | Q1 2014 |
| 7. | Defined business requirements and technical model for the authentication and authorisation service. | OeG & TMD | Q1 2014 |
| 8. | Plan and prepare procurement processes and documentation and initiate procurement processes. | TMD | Q2/Q3 2014 |

## Concurrent with evaluation and negotiations

| | What | Who | When |
|---|---|---|---|
| 1. | Continue procurement process, including negotiations | TMD | TBD |
| 2. | Develop the transition plan in negotiation with preferred suppliers | TMD | TBD |
| 3. | Implement technical service to provide network authentication and authorisation service | TMD | TBD |
| 4. | Defined data quality standards for the authentication and authorisation service. | OeG & TMD | TBD |
| 5. | Implement key essential standards, including network boundary / endpoint standards, and minimum end user computing equipment security standards | TMD & agencies | TBD |
| 6. | Commence transition from NT II to NT III | Suppliers & customers | May 2015 |

# Definitions

| | |
|---|---|
| Collaboration | As described in *Collaboration - a Tasmanian Government approach* (http://www.dpac.tas.gov.au/divisions/policy/collaboration) 'agencies working across portfolio boundaries to achieve a shared goal and an integrated government response to particular issues'. In today's environment, this form of collaboration invariably utilises use of shared ICT resources. |
| Completion of transition | The end of the migration from the NT II arrangements to NT III. |
| Connect (brand) | TMD services to government. |
| Contract structure & service levels | The structure of the agreements, including service level requirements, which services are included in which agreements and where there will be multiple suppliers. |
| Core agencies | Tasmanian Government agencies mandated to use NT services.<br>Those inner-budget Tasmanian Government agencies as defined in the Financial Management and Audit Act, Schedule 1 - Agencies to which this Act applies; and Schedule 2 - Special appropriations to which this Act applies. |
| Customer Groups | Grouping of customers by common status - either (1) Core agencies, (2) Non-core government or (3) Non-government |
| General services | The service zone that provides the secure gateway to access Government services for all staff while using 'un-managed' devices. |
| Government wide services | The service zone that provides the secure gateway to access Government services for all staff while using 'managed' devices. |
| Identity management | Identity management is the control of information about staff, devices, applications and services which are authorised to use a computer network. |
| Managed devices | Devices that a responsible agency manages, ensuring compliance with the Government security policy requirements. |
| Non-core government | Tasmanian Government organisations that are not mandated to use NT services but elect to do so. Includes GBEs, SOCs etc. |
| Non-government | Organisations eligible to use government arrangements to purchase services under NT II. Includes non-government schools, community organisations etc. |
| NT (brand) | Range of agreements, managed by TMD, providing outsourced WAN and related services to government. |
| NT III Core contract commencement | The point the vendor for the NT III Core contract commences |
| NT II | Existing WAN and related services agreements |
| NT III | Future WAN and related services agreements |

| | |
|---|---|
| NT III Scope | Scope of the agreements including-<br><br>• Definition of core customers, non-core government customers, non-government customers<br>• Services included in the range of agreements.<br>• Mandatory services for core customers.<br>• Service boundary. |
| Procurement | Process of acquiring specified services in accordance with Government guidelines. There may be more than 1 procurement process. |
| Public access services | Service zone for services made available to members of the public, such as public Wi-Fi and public access terminals in LINC centres (libraries), and public access terminals in Service Tasmania shops. |
| Public facing services | Public websites, the List, the Law and other services made available to the general public. |
| Restricted services | Service zones, based on the level of risk, where access needs to be restricted to specified staff, ICT services and devices. Examples include zones for sensitive applications such as the Budget Management System and zones to restrict access to databases and other data sets to approved applications. |
| Security policy | The information security policies and standards associated with the delivery of the Tasmanian Government's WAN and Internet services. |
| Service boundaries | The physical point of delineation on a network between a supplier service and the customer infrastructure. The service boundary will be used to delineate the respective responsibilities of the parties from a security, ownership and maintenance perspective. |
| Service zone | A discrete security zone within the NT III network model. Each zone provides secure, private network-like separation from other service zones. A tailored security policy will apply to each zone. A threat and risk assessment will assist to determine what government applications and services might reside in a particular zone. |
| Student services | Service zone(s) for use by students in schools and colleges. |
| Unmanaged devices | Devices that are not managed by responsible agency, either through technical or ownership restrictions. These can include BYO devices |