Public Safety Network Appendix 4.5 Services Guidelines Transparent Network Management

Commercial In Confidence

Contents

1. Introduction

The Public Safety Network (PSN) programme is an Emergency Services initiative of behalf of Fire and Emergency New Zealand (Fire and Emergency), New Zealand Police (Police), St John New Zealand (St John), and Wellington Free Ambulance (WFA). The PSN programme is tasked with delivering Mission Critical communication services to the Emergency Services sector.

This document should be read in conjunction with the *Appendix 1. Service Requirements* document.

2. Document Purpose

This document is one of a set of Services Guidelines which outlines the network services required for the successful delivery the PSN and should be read as a guide (except where items are specified) for potential suppliers to propose their own solutions for PSN's requirements.

3. Services Scope

Situational awareness is critical for the safety of Emergency Services, operational personnel and for the safety and the welfare of the New Zealand public. When deploying operational personnel, it is important to understand available communications capability both en route and at the response destination. Early awareness of communications capability enables a greater opportunity for success and reduces distraction from unforeseen communications challenges. Emergency Services dispatch and command personnel can guide and direct frontline staff more efficiently when communications capability is known.

Transparent Network Management services will ensure the visibility of communications capability for operational personnel, dispatchers and command personnel both en route and at response destinations. Service providers will enable a web portal dashboard and an Application Programming Interface (API) to provide real-time views of network status, including planned work and any associated service impacts. This will mean any interruptions to the service are understood and operational procedures can be adjusted accordingly.

The tools provided for Transparent Network Management are for operational personnel, including dispatchers and commanders, and so need to be intuitive, user-friendly and usable with dispatch tools on the desktop whilst in a high-pressure situation. Tools can be expected to evolve over time and be integrated with other applications. One example may be for a view of available PSN services to be presented when an address is added into an incident.

The network management functions and processes for the web portal dashboard and Application Programming Interface (API) fall into two major categories:

- Network Status Information; and
- Change Management Processes.

4. Services Outline

4.1 Network Status Information

Emergency Services agencies require a real-time view of network availability primarily focussed on coverage and services status. Services status information is expected to provide agencies with a view of communications capability rather than network element or link status. Services status information at local, regional and national levels should be:

- Proactive, identifying the future state of coverage and services; and
- Reactive, indicating real-time coverage, reduction in redundancy/resiliency and services status as a result of planned or unplanned events.

All network coverage and service status information should be made available via a real-time secure API and a secure web portal. This includes the ability to query historical Network Status Information. The outcome of Network Status Information is that Emergency Services are provided with known minimum communications capability when they are deployed to an incident. They will understand which applications or services are available to them that will better ensure their safety.

4.1.1 Proactive

Coupled with the Change Management Processes, proactive network status will enable identification of the future state of coverage and services status, providing visibility of the forecast impact on communications capability in a service zone. The type of changes that enable a proactive view of network status may include, but are not limited to:

- Site relocations;
- Antenna changes;
- New sites;
- Decommissioning of sites; and
- Other planned network changes likely to impact coverage or services status.

4.1.2 Reactive

Reporting of agency subscriber issues in real-time is an important aspect of services status as it provides visibility of any current impact on communications capability to Emergency Services agencies. Reporting, usually derived from alarm and performance data, will indicate where coverage or service degradation is occurring. As a result, Emergency Services will have a real-time view of communications capability affecting service zones. This will enable operational awareness and BCP processes to be invoked if required.

Examples of service impacts include, but are not limited to:

- Local, regional or national service loss of applications such as Push-to-Talk;
- Local, regional or national service loss of domain name services;
- Local, regional or national loss of cellular, satellite or Land Mobile Radio services;
- Local, regional or national degradation of cellular, satellite or Land Mobile Radio services;
- Local, regional or national loss of priority or consumer voice, data or messaging services;
- Local, regional or national degradation of priority or consumer voice, data or messaging services;

- Local, regional or national loss of service provider to agency interfaces and links; and
- Local, regional or national loss or degradation of network or service status information.

4.2 Change Management Process

Incorporating Emergency Services agencies into the cellular, satellite and Land Mobile Radio service providers' change management processes will enable greater awareness of communications capability availability. It is expected that all information associated with an integrated change management process will be delivered via a secure electronic information and approval process with agreed response levels.

It is expected that vendors will need to coordinate change events to avoid multiple changes in the same time window.

Planned work should include an alternative date in case the initial dates are impacted by weather, staff availability or other events.

Five key categories of change have been identified.

Informational – change that will not affect Emergency Services communications	• Change is low impact and will follow a pre-defined and documented process for implementation. • Typically, these are the day-to-day activities that have no impact on business service performance or availability. • Pre-approved, no lead time required.
Minor – change will have negligible or zero impact on the availability of any Mission Critical or business-critical service	• Change has successfully been made in the past, change is of medium or low risk and executing back-out recovery plan would be straightforward. • Introduces no change to operational processes. • Unless there is a direct conflict with a known Emergency Services response event these changes do not require direct agreement with Emergency Services. • Lead time is usually greater than 24 hours, one working day.
Significant – change will have a direct impact on Emergency Services	• Change will impact the availability of a business-critical service and may impact a large number of end-users. • Change is high-risk and requires significant effort to back out. • Change impacts a single service or organisational division. • Change introduces significant change to business processes. • Lead time is greater than six working days.
Major – change will have a direct impact on Emergency Services	• Change will impact the availability of a Mission Critical service. • Change is high-risk and either it is the first time this change has been attempted or backing out of the change would be very difficult or impossible.

standard operating procedures and therefore will require direct approval by Emergency Services to proceed	• Change is at a cost that requires senior management approval or impacts multiple services or organisational divisions. • Change is extremely difficult to implement or the time required for implementation exceeds the maximum permitted change window for any affected service. • Change introduces major change to business processes. Lives potentially put at risk if there was a problem during the implementation. • From an end-user’s perspective, a major impact on the services provided would occur if there was a problem during the implementation and the number of such users represents a significant percentage of the user community. • Lead time is greater than 12 working days.
Urgent – change required to maintain the integrity of all priority and consumer services	• Change will have a direct impact on Emergency Services standard operating procedures and requires agreement and escalation with Emergency Services. • Change is intended to resolve a problem that is negatively impacting a Mission Critical or business-critical service to such a degree that the timeline required for the normal approval process cannot be followed. • Usually less than 12 hours lead time but should have as much notice as possible.

4.3 Application Programming Interface (API) and Secure Web Portal

Network Status Information will be made available via API and web portal to Service Centres (including ICT & network help desks), Communications Centres and directly to frontline staff either embedded in existing applications or as a stand-alone application.

The solutions should use federated identity and access management to ensure consistent user management across service provider systems. Service providers will need to support agency or government hosted/approved IAM systems.

Standards for data interchange between service providers and Emergency Services agencies are not clearly defined and will need to be agreed. Items for discussion include, but are not limited to:

- Data schemas;
- Data interchange formats;
- HTTP/REST API standards;
- Separate or combined APIs for:
  - Reactive network status;
  - Proactive network status; and
  - Change management.

API and web portal status should be reported in real-time to agency service centres and communications centres 24/7/365.

4.3.1 Security

Individual agency and government security policies and standards must be followed.

Appropriate security measures must be invoked to ensure network management integrity. Information cannot be created, modified or deleted by unauthorised personnel.

Security measures must prevent exposure of restricted information and adhere with the Privacy Act 1993 and planned amendments. Exposure of vulnerabilities to malicious actors must be prevented.

4.4 Network and Service Management Tools

The Transparent Network Management services should be delivered with consideration to other necessary network and service management functions.

Other network and service management functions include, but are not limited to:

- Performance management;
- Performance reporting;
- Service Level Agreement management;
- Usage monitoring;
- Exception reporting;
- Real-time service and device reporting;
- Service management (ITIL);
- User management;
- Carry out simple changes;
- Purchase and provision new devices;
- Manage devices and services;
- Manage device security (encryption, disabling and re-enabling);
- Security monitoring;
- Historical network, service & device status information;
- Report faults and outages; and
- Other operational functions.

5. Risks, Issues, Dependencies and Assumptions

Transparent Network Services are required to support cellular, digital Land Mobile Radio, Personal Alerting and satellite services.

Service providers should have back-up notification systems (such as direct phone calls) in the event of significant outages preventing real-time delivery of notifications to affected Emergency Services agencies.