Government Radio Network Radio Programming Policy

May 2016

DOCUMENT ADMINISTRATION

Document Location

This Policy has been developed to underpin the operations of the Telco Authority Spectrum Management Office (SMO).

The master copy of the document is held with the SMO currently at the following location:

Level 18, McKell Building
2 – 24 Rawson Place
Sydney NSW 2000

Contents

1. Purpose 4
2. Objectives 4
3. Scope and Audience 4
4. Use of specific terms 4
5. Context 5
6. Expectations of stakeholders 6
7. Radio programming 6
Appendix A 13
Appendix B 14

1. Purpose

1.1 The NSW Telco Authority is responsible for the overall coordination of radio telecommunication services for the NSW Government, including the NSW Government Radio Network (GRN).

1.2 The purpose of the Government Radio Network Radio Programming Policy is to inform NSW GRN users (GRN Client) and vendors/suppliers of the security requirements that apply to applications or hardware used to configure or program GRN terminals (radios). This policy is a component of the NSW Telco Authority information security management system.

2. Objectives

The objectives of this policy are to:

2.1 Minimise the risk of exposing GRN users to un-authorised access due to poor controls of Programming Devices and/or System Keys

2.2 Provide clear and concise instructions when un-authorised access to Programming Devices is identified

2.3 Provide clear and concise instructions on compliance with this policy.

3. Scope and Audience

3.1 The scope of this policy is the management of information, application and hardware used to program Terminals that connect to the NSW GRN.

3.2 Excluded from the scope of this policy is the programming of any device that is not an approved device for connection to the NSW GRN. Only devices that are procured specifically to connect to the NSW GRN by a user agency are covered by this policy. Unauthorised devices are not permitted to connect to the GRN.

3.3 This document should be read and understood by GRN Client administrators, NSW Telco Authority (TA) engineering staff, the GRN Network Manager and radio vendors/suppliers.

3.4 Compliance to this policy is a requirement on registered or prequalified vendors providing services under the whole of government Panel Contract ITS2573 and who provide hardware or software to programme Terminals for use on the GRN.

4. Use of specific terms

4.1 "Terminal" is a portable or mobile radio device that contains configuration enabling authentication and access to the Government Radio Network (GRN)

4.2 "Codeplug" means a radio configuration file

4.3 "Programming Device" refers to either, and/or both hardware and software/s used to store and/or change a codeplug. It is used by either the Administrator or a radio programmer to configure radios. In the instance multiple software components and IT hardware is used to manage and deploy a codeplug to a radio, these are all captured under the term "Programming Device"

4.4 "Administrator System Key" refers to either hardware or software that is required to unlock the "Programming Device" to a level of authorisation that enables full control of terminal configuration. It is used by an Administrator to create the Slave System Keys issued to Radio Programmers and can be a hardware dongle or software application.

4.5 "Slave System Key" refers to either hardware or software that is required to unlock the "Programming Device" to a level of authorisation limited to configuration changes of a codeplug A "Slave System Key" can be a hardware dongle or software application.

4.6 "System keys" refers to both administrator and slave system keys

4.7 "Administrator" refers to an authorised agency representative who has access to the Administrator System Key and radio programming device

4.8 "Radio programmers" refers to an authorised agency representative who has access to the slave system key and radio programming device

4.9 "Third Party" refers to any other party that is not another government agency

4.10 "NOCC" refers to the GRN Network Manager who operates the Network Operating Control Centre

4.11 "Vendor" refers to a Telco Authority approved supplier of hardware or software for radio programming

4.12 "Compromised" refers to a radio that has had its codeplug intentionally changed to connect to GRN Talkgroup(s) without approval

4.13 "Dongle" is a hardware Programming Device

4.14 "Mobile" is a radio mounted in a vehicle

4.15 "Portable" is a handheld radio.

5. Context

5.1 A Programming Device is required to make changes to a radio codeplug

5.2 A Programming Device is required to make changes to a radio programmers access and control permissions

5.3 A Programming Device requires either an Administrator System Key or slave system key

5.4 A Programming Device can store one or multiple radio code-plugs

5.5 A Programming Device is managed by an Administrator

5.6 A Programming Device is used by an Administrator and a Radio programmer

5.7 A master system key is used by a Vendor to create the Administrator System Key issued to Administrators

5.8 Administrator System Keys is used by an Administrator to create the Slave System Keys issued to radio programmers

5.9 A Vendor may provide a single key that functions as both the Administrator and Slave System Key

5.10 It is understood that a radio may have both a conventional and trunked profile. Unless otherwise specified, this document relates to a trunked profile.

6. Expectations of stakeholders

When implementing this policy, it is expected that:

TA and its Network Manager will:

6.1 ensure use of Vendor neutral terminology

6.2 demonstrate a coordinated and proactive approach to managing GRN related security requirements

6.3 be supportive of Administrators in the use and compliance to this policy

6.4 be supportive of Vendors in identifying compliance to this policy.

Administrators will:

6.5 comply with the policy

6.6 ensure policy requirements are met by radio programmers.

Vendors will:

6.7 comply with the policy

6.8 clearly articulate full or partial non-compliance for Terminals to the TA upon request.

7. Radio programming

7.1 Administrator System Key

7.1.1 The Administrator has full accountability for maintaining the security of the Administrator System Key

7.1.2 The Vendor will not provide Administrator System Keys to any individual or party without written approval from the NOCC

7.1.3 The NOCC must keep a current list of approved Administrators

7.1.4 Administrators must not accept or receive Administrator System Keys from anyone other than a prequalified vendor.

7.1.5 Administrators must cease the use of an Administrator System Key if requested by the NOCC

7.1.6 Administrators must notify the NOCC and vendor of any lost or known compromised Administrator System Keys at the earliest opportunity, and not more than 4 hours from the time the device was known to be lost or compromised. The unique ID related to the hardware/software must be provided

7.1.7 Vendors must deactivate Administrator System Keys when notified by the approved Administrator (as authorised within form in Appendix A) or by the NOCC

7.1.8 Administrators must not share Administrator System Keys with any other Administrator, vendor or third party

7.1.9 Administrators must request Administrator System Key renewals from the NOCC via the same process for requesting an Administrator System Key (form in Appendix A)

7.1.10 The NOCC will update the register of lost or known compromised Administrator System Keys by a unique ID related to the hardware/software.

7.2 Slave System Key

7.2.1 The expiry date for a slave system key must be programmable by the Administrator and cannot be changed by a radio programmer

7.2.2 A slave system key expiry date must be less than or equal to12 months, after which the key becomes inactive and unusable

7.2.3 A programming device with a slave system key must be capable of limiting the amount of failed radio programming coding attempts

7.2.4 Slave system key programming devices must only be able to configure approved Unit IDs and Talk Group IDs

7.2.5 Administrators are accountable for managing and keeping a record of all slave system keys, associated programming devices, and users

7.2.6 Administrators are accountable for ensuring radio programmers comply with this policy

7.2.7 Administrators must notify the NOCC of any lost or known compromised slave system keys and associated programming devices at the earliest opportunity, and not more than 4 hours from the time the device was known to be lost or compromised

7.2.8 The NOCC will update the register of lost or known compromised slave system keys and associated programming devices.

7.3 Programming Device

7.3.1 Programming Devices should be purchased and sourced by the Administrator

7.3.2 The security of Programming Devices must be managed by the Administrator

7.3.3 TA should review Vendor Programming Device compliance periodically as agreed with vendors

7.3.4 The NOCC should maintain a list of Vendor Programming Devices that are compliant to this policy and update this list each time new information is provided

7.3.5 Administrators must only use Programming Devices that are on the prequalification list. This list should be published on the Telco Authority website www.telco.nsw.gov.au and can also be obtained from the NOCC

7.3.6 All Programming Devices must comply with the system key guidelines in this policy

7.3.7 Administrators should maintain a register of all Programming Devices that is reviewed and updated no less than every 6 months and must provide this to the NOCC whenever this list is updated or upon request

7.3.8 Administrators must request, via the NOCC, qualification of any Programming Device not on the approved list

7.3.9 The NOCC should seek approval from the TA prior to the addition of new Programming Devices on the approved device list and issuean updated prequalification list with any changes

7.3.10 Programming Devices that have known security vulnerabilities must not be issued by a vendor.

7.4 Passwords

7.4.1 Programming Devices must be password protected and the password must contain a minimum of eight alphanumeric characters

7.4.2 Programming Devices should lock out any user that fails to authenticate five consecutive times

7.4.3 Programming Devices should have a time out period in which a user must wait prior to attempting to authenticate again after a lock out

7.4.4 Programming Devices should contain a log that enables identification of authentication activity including user name, date, time, action and cause

7.4.5 Administrators must not share or reveal passwords.

7.5 Radio configurations

7.5.1 Restrictions on the radio configuration done by radio programmers is the responsibility of the administrator

7.5.2 Programming Devices must be restricted to radio and talkgroup identification (ID) ranges permitted to that agency by the NOCC.

7.6 Physical security

7.6.1 Administrators must ensure they take all precautions and make every effort to implement controls to secure physical access to Programming Devices

7.6.2 Administrators should maintain physical separation of Administrator System Key hardware and the Programming Device software. i.e. dongles are not kept in the same case as a laptop

7.6.3 Programming Devices must be stored in a location that requires key, security swipe card or punch code access

7.6.4 Administrators must not share or transfer Programming Devices that have Administrator System Keys with any other agency, vendor or third party

7.7 Administrators must manage the physical security of a Programming Device during repair, upgrade or replacement

7.8 Control documentation

7.8.1 Administrators must maintain a record of the Programming Device location

7.8.2 Administrators must maintain a record of who has physical access to a Programming Device

7.8.3 Administrators must notify the NOCC of incidents that could or have compromised the physical or logical security of a Programming Device, and implement controls to mitigate the likelihood of reoccurrence

7.8.4 Administrator must maintain a complete record of Programming Devices (Appendix B)

7.8.5 Administrators should audit and review their controls on radio Programming Devices annually

7.8.6 The NOCC must maintain a register of Administrators

7.8.7 The NOCC must maintain records of approvals granted to vendors for providing Administrator System Keys

7.8.8 The NOCC must maintain records of reported stolen, lost, damaged or compromised system keys and associated Programming Devices.

7.9 Administrator System Key access process

7.9.1 All Administrator System Key requests must go to the NOCC

7.9.2 All details in Appendix A must be provided in an Administrator System Key request unless marked as optional

7.9.3 A Services Agreement must be in affect between the Administrator's agency and the TA prior to an Administrator System Key being provided by the Vendor to the Administrator. This will be managed by the NOCC who must not approve a request for an Administrator System Key if the Services Agreement is not in affect

7.9.4 Vendors must only provide Administrator System Keys to Administrators when evidence of approval from the NOCC is provided

7.10 Administrator System Key lost or stolen process

7.10.1 Administrators must notify the NOCC and the Programming Device Vendor of a lost or stolen Programming Device that has an active Administrator System Key at the time the incident occurs. Administrators should provide this notification immediately and no more than 4 hours from the time the device was known to be lost or stolen

7.10.2 The NOCC must update the register of lost or known compromised Administrator System Keys

7.10.3 Vendors must immediately deactivate Administrator System Keys when notified by the approved Administrator or by the NOCC

7.10.4 Vendors must notify the NOCC when an Administrator System Key has been deactivated (using Appendix B as the Register)

7.10.5 A request to replace an Administrator System Key that is lost or stolen is the same process as requesting an Advanced System Key(Appendix A)

7.10.6 The NOCC contact details are:

Email: helpdesk@radnet.nsw.gov.au

Telephone: 1800 679 476

7.11 Pricing

7.11.1 Charges for the Programming Device are set by each vendor

7.11.2 The Administrator must purchase and pay for the Programming Device directly with a vendor from the Programming Device prequalification list

7.11.3 Charges for the Administrator System Key are set by each vendor

7.11.4 The Administrator must purchase and pay for an Administrator System Key directly with a vendor from the Programming Device prequalification list. This list can be obtained from the NOCC.

List of Abbreviations

Abbreviation	Description
GRN	Government Radio Network
NSW	New South Wales
NOCC	Network Operation Control Centre
RFID	Radio Frequency Identification
LTE	Long-Term Evolution
RF	Radio frequency

Appendix A

Part A Terms and Conditions Acceptance

I hereby accept the terms and conditions as set out in the document "Government Radio Network Radio Programming Policy".

Signed _____

Name (Print) _____

Role Communications Manager / Operations Manager / Engineering Manager

Agency _____

Date _____

Part B Agency Approval for requesting advanced system key

The following details are required for an agency to receive an advanced system key.
(To be completed once Part A is signed)

Request type: *New/Renew or replace*

Programming device vendor name: _____

Programming device vendor product name: _____

RADIO ID range: _____

Talkgroup ID range: _____

Vendor related quote/ID: *(optional)* _____

Additional requirements of ASK: _____

_____

NSWTA NOCC Operator Approver name: _____

NSWTA NOCC Case Number _____

Approval date: _____

Date request sent to Vendor: _____

Appendix B

Register of Programming Devices

The attached Register of Administrator System Key(s) must be maintained by ALL Administrators for their Agency

The Register needs to be maintained by all Vendors for all Administrator System Keys issued. This Register must be submitted to the GRN NOCC in its entirety every time an Administrator System Key is issued or changes made.

Email to helpdesk@radnet.nsw.gov.au

Administrator System Key Tracker.xlsx

This page left intentionally blank