Title:	P25 Lost or Compromised Radio	SOP No:	ITS-RADIO-006
Revision:	1.2	Effective Date:	August 28, 2018
Owner:	Manager - Wireless Communications	Department:	IT Solutions

P25 Lost or Compromised Radio

1 Purpose

The objective of P&P 6 is to protect the security of the public safety radio system that provides communications for first responders across much of North Central Texas network from unauthorized and disruptive radio communications due to lost or compromised radios. This policy establishes a process for appropriately reporting, documenting, tracking, disabling and reactivating (if applicable) subscribers that are lost or compromised including those with encryption capabilities.

2 Scope

All subscribers on the Radio System must comply with the procedures dictated in this policy.

3 References

None

4 Conditions for Exemption

Exceptions to the policy must be approved by the Senior Manager over Wireless Communications.

5 Justification

Implement a security policy that protects mission critical communications on the Radio System from unauthorized transmissions, security breaches and downtime due to lost or compromised radios.

Immediately disabling lost or compromised radios ensures that Public Safety communications remain online, active and fully operational and do not encounter downtime due to incorrect or out of synchronization encryption keys.

Title:	P25 Lost or Compromised Radio	SOP No:	ITS-RADIO-006
Revision:	1.2	Effective Date:	August 28, 2018
Owner:	Manager - Wireless Communications	Department:	IT Solutions

6 Lost or Compromised Subscriber Rules

The flowchart in Figure 1 provides an overview of the process described in section 6.0.

6.1 Reporting, Documenting, and Tracking Process

Users must inform Wireless Communications if a subscriber unit is lost or stolen which will result in the creation of an ITSM ticket. A Police Report is required for CFW Stolen Radios and will be appended to the ITSM ticket. External agencies must also follow this process, however, a Police Report is not mandatory.

6.2 Disabling and Reactivation Process

Wireless Communications will inhibit the Subscriber from communications on the radio system via the Provisioning Manager (PM) Client once the radio has been reported lost or stolen per 6.1.

- If the inhibited radio is powered up and attempts to register on the radio system, it will cease to operate and become “bricked”. A radio recovered after it has been completely disabled must be reported to the Helpdesk via written communication which will result in an update of the ITSM ticket. A disabled CFW radio must be brought to Wireless Communications for manual configuration, programming and loading of encryption keys. External Agencies must contact their radio service provider to have their disabled radios reconfigured, programmed and loaded with encryption keys. Wireless Communications will restore radio operations, update and then close the ITSM ticket.
- If an inhibited radio is not powered up but is recovered, it must be reported to Wireless Communications, which will result in an update of the ITSM ticket. If the inhibited radio has battery power, Wireless Communications will remotely uninhibit the subscriber and reenable communications on the radio system via the PM Client. Wireless Communications will then restore radio operations and close the ITSM ticket.
- If a radio is unrecovered after one week, the ITSM ticket must be updated accordingly and closed. Should the radio be recovered after the ITSM ticket is closed, the case can be reopened and the process in 6.2 followed as described above.

Title:	P25 Lost or Compromised Radio	SOP No:	ITS-RADIO-006
Revision:	1.2	Effective Date:	August 28, 2018
Owner:	Manager - Wireless Communications	Department:	IT Solutions

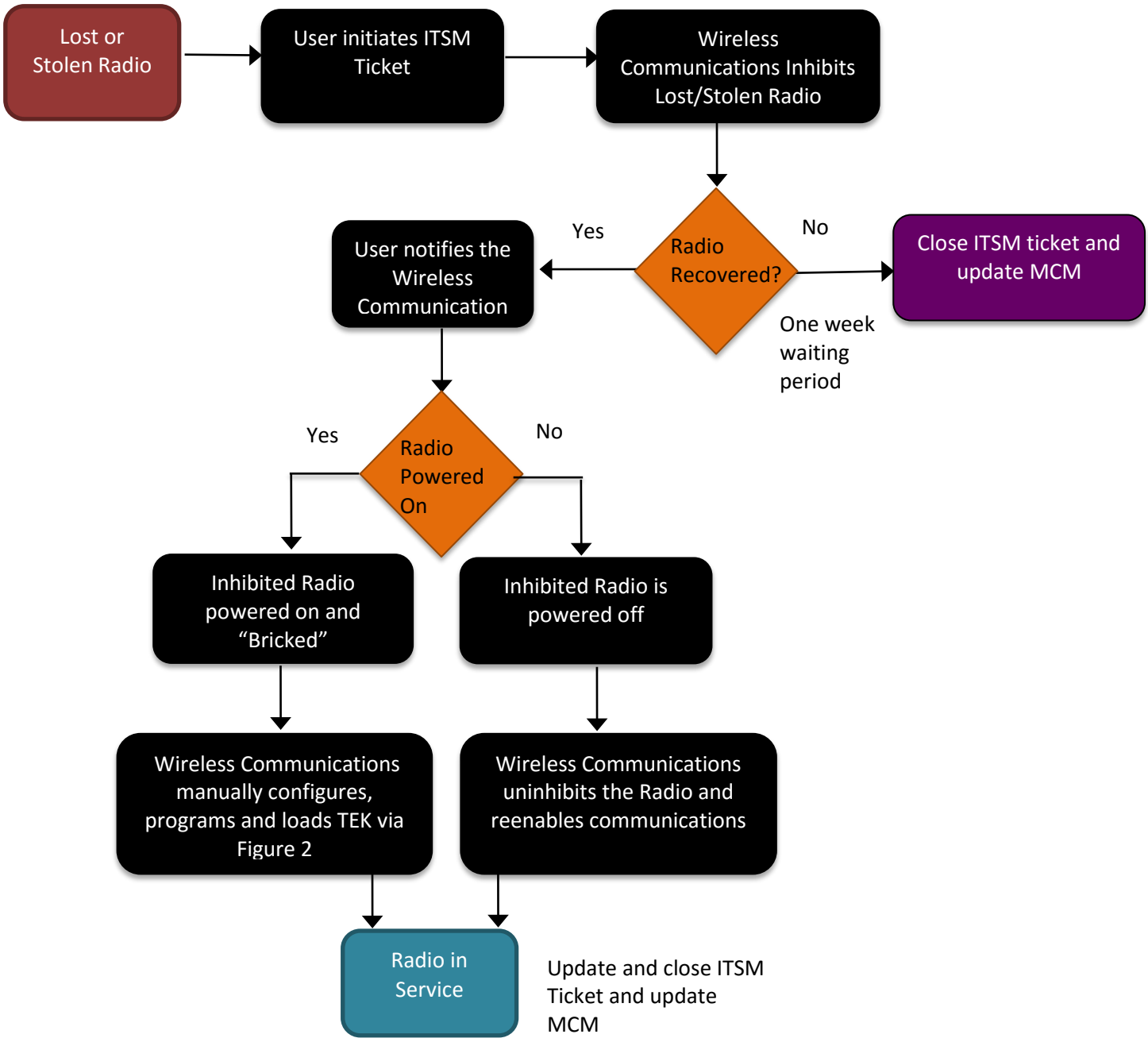

Figure 1: Lost/Stolen Inhibit Process

- After its been determined that an encrypted radio is stolen, the rekey process will begin as soon as practical. But if a radio is lost, the rekey process will initiate within a week. If another radio is lost/stolen less than two weeks after the previous occurrence, successive radio rekey requests will not commence unless deemed necessary. After a rekey request, notification will be sent to affected encrypted radios to press the rekey button on their portables and mobiles and ensure they have the latest key. If the latest key is enabled in their radios, they will receive an indication.

7 Supporting Documentation

None

Title:	P25 Lost or Compromised Radio	SOP No:	ITS-RADIO-006
Revision:	1.2	Effective Date:	August 28, 2018
Owner:	Manager - Wireless Communications	Department:	IT Solutions

Version Control

Version	Date	Description	Author
1.0	8/1/2014	Original version	Abinta Khan
1.1	12/5/2016	Updated CFW P25 Radio System to Fort Worth Regional Radio System, updated Radio Services to Wireless Communications, added encrypted to type of radio stolen to trigger a rekey.	Douglas O'Neal
1.2	8/28/2018	Removed reference to FWRRS, updated HelpDesk notification to Wireless Communications	Larry Crockett