MARYLAND FiRST
First responders Interoperable Radio System Team

Wes Moore
Governor

Aruna Miller
Lieutenant Governor

Katie Savage
Chairman of the Board

Addendum A – Checklist for Subscriber Decommissioning
SOP 0.13

***This checklist was developed for and contains references to Motorola-specific programming features, alternate manufacturers may use different terminology, but the underlying procedures remain the same.*

□ **Radio Codeplug:** Restore to factory default “BLANK” codeplug

Where possible, radios should be programmed with the original blank codeplugs they came with out of the box.

If the original codeplug is not available, a new blank codeplug should be created for programming, with particular attention paid to the following (where applicable):

- ***Secure Configuration (Secure Wide, ASTRO OTAR Profiles, CA Certificates)***
- ***Data Profiles***
- ***Conventional Systems and Conventional Personalities***
- ***Call Lists***
- ***Trunking Systems and Trunking Personalities***
- ***Zone Channel Assignments***
- ***Scan Lists***

Contact MD FiRST personnel for assistance if required.

□ **Encryption Keys:** Remove all encryption keys from the radio

Subscriber radio should be wiped of all key material and verified by connecting to a Key Variable Loader (KVL). This can be accomplished in one of 3 ways (may vary by manufacturer):

- ***Delete Keys via KVL: Configure Device -> Remove Keys -> Remove All (Zeroize)***
- ***“Zeroize” command via KMF Server***
- ***Special button combination on select radios***

□ **Radio System Provisioning:** Remove Radio from Provisioning Manager (or equivalent) from home **and partner systems**

Unless a Radio ID is to be immediately re-used (in a replacement radio, for instance), it should be removed from the MD FiRST Provisioning Manager. In addition, the Radio Managers for other Radio Systems that this radio had access to, should also be notified so that it can be removed from those systems as well.

□ **“Smart Feature” Provisioning:** Remove Radios from various portals

Today’s newer radios can take advantage of “smart” features (e.g. SmartConnect) to access LMR systems using cellular or WIFI networks. Typically, to access these features, radios are set up in a “portal” by the Radio System Manager for each authorized system. When decommissioning radios that had access to smart features, be sure to notify applicable System Managers so they can remove the decommissioned radios from any associated portals.

□ **Read/Write Password Removal:** Remove agency-specific read/write passwords from radios/codeplugs

It is suggested to remove any agency-specific read/write passwords from radios / codeplugs before transferring/decommissioning radios so that these passwords are not compromised. It has come to MD FiRST’s attention that with the correct software and know-how, some individuals are able to “retrieve” read/write passwords from the radio itself during the handshake process with Customer Programming Software (CPS).

□ **Write Protection Removal:** Remove the write protection so new owners can program the radio

Unless the radio in-question is to be transferred to another MD FiRST Agency, the MD FiRST Write Protection should be removed from the subscriber radio. If this write protection is left in place, the recipient will not be able to program the radio unless they have a MD FiRST Advanced System Key (ASK). MD FiRST **will not** be distributing ASKs to entities who are not authorized users of the system.

□ **Damaged Subscriber Equipment:** Radios that cannot be “sanitized” by normal means, should be destroyed rather than sold/transferred

In instances where radio equipment is damaged and no longer useable, care must still be taken to ensure sensitive information cannot be retrieved by unauthorized parties. If any applicable steps in this checklist cannot be performed due to damage to the radio, the subscriber equipment should be destroyed rather than sold/transferred. Additional guidance can be found in NIST SP 800-88 Rev. 1 (Guidelines for Media Sanitization), which is available at https://csrc.nist.gov/pubs/sp/800/88/r1/final