February 6, 2014

Office of Engineering and Technology
Laboratory Division
Equipment Authorization Branch
7435 Oakland Mills Road
Columbia, MD 210

Att: Tim Harrington

Subject: Response to Correspondence Number 45165 for Certification of Transmitter with FCC ID: AZ489FT3829, EA449420, Jan 28, 2014.

Dear Mr. Harrington,

Motorola Solutions, 8000 West Sunrise Boulevard, Fort Lauderdale, Florida, herein submits its application for a Class 2 Permissive Change to the certified Transmitter with FCC ID: AZ489FT3829. The followings are the consolidation of the operational and technical information that previously provided within the cover letter (12/3/2012), response to the correspondent # 43401 (4/2/2013), correspondent # 43846 (12/16/2013), and correspondent # 45092 (1/27/2014).

I. DESCRIPTION OF THE CHANGES:

1. The present process of using a Dongle coupled with a password given to the authorized service/maintenance personnel meets or exceeds the requirements of Rule Parts 90.203 (g) (1-4). Instead of the Dongle, the proposal is to use a password which will be available only to the authorized service/maintenance personnel and this meets the requirements of Rule Parts 90.203 (g) (1-4). (Referenced response to correspondent # 43401, Q6)
2. Consistent with Section 90.203 (g) of the FCC Rules, the devices with the above FCC ID are configured via software means only to allow the authorized service/maintenance personnel to program transmit frequencies using the keypad and a password. Additionally a standard programming cable when attached to the device will enable the same operation.
3. The prime hardware difference lies in the elimination of the hardware dongle accessory that is attached to the side connector of the device. Further, there is the addition of a Advance System Key that must be attached to the side connector of the computer on which the authorized service/maintenance personnel is enabling the FPP feature via the CPS. (Referenced response to correspondent # 43401, Q2)
4. The firmware difference is that the device will no longer look for a hardware dongle to be attached to the side connector of the device when entering FPP mode. Rather, the device will query the authorized service/maintenance personnel for a

password since the hardware USB dongle was already utilized in enabling the FPP feature via the CPS. (Referenced response to correspondent # 43401, Q2)

5. This change will be accomplished by configuring the device with a codeplug that permits FPP operation with the use of a password (refer to the Section III – Additional supporting Information for more detail on setting a FPP password). The frequencies that can be programmed from the keypad will only be those frequencies that are certified by the FCC for this transmitter.

   A codeplug is a solid-state chip inside a device where the device's personality data is stored. Personality data is created using the Motorola CPS. CPS defined data can be transferred to the device's chip or to a codeplug file. Codeplug files can be archived on the computer's hard drive for later use. (Referenced response to correspondent # 43401, Q4)

   CPS will only enable the frequencies that the device is certified for and FPP will access those identical sets of frequencies. It's important to note that these devices are for licensed services and the licensee (i.e. authorized service/maintenance personnel) shall program only authorized frequencies, this meets the requirements of Rule Part 90.427 (b). (Referenced response to correspondent # 43401, Q5)

   Codeplug changes to any Motorola device requires the use of the Motorola CPS along with a specific programming cable that attaches to the side connector of the device. The CPS is distributed to the authorized service/maintenance personnel. (Referenced response to correspondent # 43401, Q9)

6. The capability is in the current shipping products; however a firmware change would be required in order to enable the FPP feature to work without a dongle attached to the device. (Referenced response to correspondent # 43401, Q10)
7. There will be no change to the FPP option; however the software version cannot be determined until the FCC grants Motorola Solutions the right to develop and implement such feature. It is estimated that this feature will require version R10.00.00 or later. (Referenced response to correspondent # 43401, Q1)
8. Instructions for operating in the FPP mode will be made available through the detailed user manual for the device. This manual is provided to authorized service/maintenance personnel through CD's that ship with the device as well as online at Motorola's website that requires authentication via username and password. At this site the password will be created by the authorized service/maintenance personnel. (Referenced response to correspondent # 43401, Q8)
9. The current User Manual for the device does not provide detailed information on the FPP including password. There will be a separate set of user instructions for Front Panel Programming which will only be made available the authorized service/maintenance personnel

II. PERFORMANCE DIFFERENCES:

1. There are no Spurious Emissions or RF Exposure performances resulting from this software change. Additionally, all other data on file at the FCC continues to be compliant including 90.203(j) provisions. (Referenced response to correspondent # 43401, Q3; and response to correspondent # 45165, Q4)
2. FPP option does not change any of the feature set of the device and is compliant to all of the rules parts 2, 80 and 90 as described in the current certification of the device with FCC ID listed above. (Referenced response to correspondent # 43401, Q11; and response to correspondent # 45165, Q4)

III. Additional supporting information (Referenced response to correspondent # 43846; correspondent # 45092; and response to correspondent #45165, Q1 - Q3 and Q5):

Motorola Solutions contacted Scot Stone of the FCC's WTB (Wireless Telecommunication Bureau) and Michael Wilhelm of the PSHSB (Public Safety and Homeland Security Bureau) on August, 2013. The FCC's official position is that utilizing only a password to enable FPP does meet the spirit of the FCC's rules, provided it is a "legitimate" password protection. In our discussion, he explained that they don't expect the password to be a simple default for all devices, which never has to be changed, so that 2 minutes on Google could allow anyone to enable FPP.

The FCC did not proscribe how it needed to be done, but gave examples such as forcing a default password to be changed when the device is initially programmed, or somehow making the passwords unique on a customer by customer, or even device by device, basis, although the last may be impractical. These are just examples with lots of flexibility to define a process that fits with both our product teams' and our customers' needs.

Scot also indicated that this has been discussed between the Wireless and Public Safety bureaus, as well as OET, so they are all on the same page.

Based on the above opinion and guidance from the WTB and the PSHSB, Motorola Solutions will be implementing FPP by eliminating the need for a dongle for FCC users as follows:

1. Devices purchased by non-federal agencies customer from Motorola Solutions would order a device with an FPP option. This option would include the following:
   a. Advanced System Key is an external hard key (control normally inaccessible to the end user) which would be used for enabling FPP feature on the device through the use of a computer
   b. Motorola would restrict the enablement of the FPP feature through the programming software to the authorized service/maintenance personnel by use of the Advanced System Key
   c. Customer Programming Software (CPS)

2. The authorized service/maintenance personnel would receive the devices and connect the devices to a computer
3. The CPS (control normally inaccessible to the end user) would read the device configuration
4. The authorized service/maintenance personnel would connect Advanced System Key to the computer to allow the CPS to enable the FPP feature
5. The FPP feature would then become available through the CPS with the presence of the Advanced System Key
6. The authorized service/maintenance personnel would be the only personnel with access to enable the FPP feature
7. The CPS would then require the authorized service/maintenance personnel to enter a password (FPP password) that authorized service/maintenance personnel would use on the device when that person is to operate the FPP feature. Steps 2 thru 7 above will need to be repeated in order to change the FPP password of the device.
8. A menu item or button selection would be added to the device's programming by the authorized service/maintenance personnel that would be used to access the FPP feature on the device
9. The device would be written and programmed with FPP password
10. In order to use FPP, the authorized service/maintenance personnel would need to access the menu item or button on the device, enter the password for FPP that was set by the authorized service/maintenance personnel, and at that point the authorized service/maintenance personnel would be able to use the FPP feature.
11. For Rule Part 80, FPP is a feature that is being offered in accordance with the requirements for 80.203(b) for operations in the 156-162 MHz. When the device is being operated on frequencies licensed under Part 80 of the FCC rules, pursuant to 47 CFR 80.169(a), 80.203(b)(1) and 80.203(b)(3) the programming of authorized channels must only be performed by a person holding one or more of the following qualifications:

    a. First Class Radiotelegraph Operator's Certificate,
    b. Second Class Radiotelegraph Operator's Certificate,
    c. Radiotelegraph Operator License, or
    d. General Radiotelephone Operator License.

IV. Definitions:

CPS: Customer Programming Software

FPP: Front Panel Programming

If you require any additional information, please contact me at (954) 723-5422 (Phone).

Sincerely,

Kim Uong
Regulatory Compliance
Email: Kim.Uong@motorolasolutions.com