


<p>REGIONAL WIRELESS COOPERATIVE POLICIES AND PROCEDURES</p>	
	<p>No. O-14.13</p>
<p>Subject: Long Term Talkgroup Reservation Policy</p>	<p>Revised: 01/2024</p> <p>Prior Rev: 01/2022 02/2020 01/2017 09/2014</p>

1.0 Purpose

1.1. The purpose of this procedure is to support the long-term use of interoperability talkgroups.

2.0 Owner

2.1. RWC Operations Working Group (OWG)

3.0 Applies To

3.1. All Members, Associates, Conditional, and Interoperability Participants that need long term use of RWC interoperability talkgroups.

4.0 Background

4.1. The RWC has identified Interoperability talkgroups that may be requested for long term operations.

5.0 Policy Statement

5.1. These talkgroups can be used to facilitate communications among agencies that typically communicate with each other on a regular basis.

5.2. Utilization of Interoperability resources for more than 29 days constitutes “long term” use.

6.0 Supporting Rules

- 6.1. Agency requests for long term talkgroup usage must be submitted to the OWG. All requests must include:
 - 6.1.1. Interoperating agencies.
 - 6.1.2. Number of users.
 - 6.1.3. Beginning and ending dates.
 - 6.1.4. Coverage requirements.
 - 6.1.5. Purpose for request.
 - 6.1.6. Explanation of encryption needs if secure communications are requested.
 - 6.1.6.1. All encrypted interoperability talkgroups have permanently assigned keys.
 - 6.1.6.2. If encryption needs to be managed for secure access, a subscriber workbook will be required.
 - 6.1.7. Contact person, including phone number and email address.
- 6.2. Long term interoperability talkgroups will be assigned by the OWG.
 - 6.2.1. Denied requests may be appealed to the RWC Executive Director.
- 6.3. When resources are requested, assignments are based on the following criteria.
 - 6.3.1. Network usage and system impact.
 - 6.3.2. RWC membership.
 - 6.3.3. Number of agencies and total number of users involved.
 - 6.3.4. Requestor requirements.
 - 6.3.5. Resource availability.
- 6.4. Long term interoperability usage will be evaluated quarterly.
 - 6.4.1. If extensions are not requested, users may be subject to disconnection.
- 6.5. Terminations
 - 6.5.1. The RWC reserves the right to rescind agreements.
 - 6.5.2. Upon termination, the encryption key must be removed from the radio.
 - 6.5.2.1. If the radio is Over-The-Air Rekeying (OTAR) capable the key will be removed by the Encryption Manager via the Key Management Facility (KMF).
 - 6.5.2.2. If manually loaded, radios must be presented for encryption key removal upon request.
- 6.6. There is no support for emergency buttons on G, H, L, O and P interoperability talkgroups.

- 6.7. The RWC does not provide dispatch monitoring or recording for G, H, L, O and P interoperability talkgroups. Agencies must make their own arrangements for dispatch monitoring and/or recording.
- 6.8. If an encrypted talkgroup is patched to an unencrypted talkgroup both talkgroups should be treated as non-secure/unencrypted.

7.0 Responsibilities

- 7.1. A representative of the requesting agency(s) will be available in person or via teleconference for discussion at the time the OWG considers the request.
- 7.2. Requesting agency needs to ensure that all agencies have access to the assigned resources.
- 7.3. When the operation ends, notification must be made to the RWC Executive Director that the assigned resource is no longer needed.

8.0 Conditions for Exemption or Waiver

- 8.1. As provided in the Waiver or Exception Policy.

9.0 Applicable Procedures:

- 9.1. As listed at www.rwcaz.org