REGIONAL WIRELESS COOPERATIVE POLICIES AND PROCEDURES	Regional Wireless Cooperative
	No. **S-02.10**
Subject: **Encryption Management Guidelines Policy**	**Effective Date: 7/28/10** **Revised: 2/8/18**

1.0 Purpose

1.1. The Encryption Management guidelines set forth in this policy are intended to ensure the security, management, generation, distribution, use, storage, and destruction of Regional Wireless Cooperative (RWC) encryption key materials.

2.0 Owner

2.1. RWC Operations Working Group (OWG)

3.0 Applies To

3.1. RWC members, interoperability participants and any entities otherwise using the secure operational capabilities of the RWC.

4.0 Background

4.1. RWC communications often contain sensitive and vital information relative to law enforcement and other public safety related activities. Disclosure or modification of this information could adversely impact public safety operations and pose a threat to the safety of public safety officials and citizens. The RWC has recognized the need for protected radio transmissions and has equipped the RWC with encryption capabilities that provide the required level of protection.

4.2. The generation of RWC encryption keys and distribution of those keys to subscribers in a synchronized fashion is a complex process that is critical to the encryption of radio transmissions. There are inherent risks and vulnerabilities to public safety personnel if proper key management processes are not followed. The RWC can significantly mitigate these risks and vulnerabilities by establishing standard key management processes.

4.3. Each RWC encryption key is associated with a system-wide key reference, referred to as a Common Key Reference (CKR). The same encryption key is referenced by the same CKR in every secure component, and allows key management in a device-independent manner. CKRs are assigned to talkgroups and multi-groups.

5.0 Policy Statement

5.1. The Network Managing Members of the RWC designate the Encryption Manager under the authorization from the RWC Board of Directors, to be responsible for the generation, distribution, storage, destruction, and maintenance of RWC encryption materials, and to implement established guidelines to support RWC encryption operations.

6.0 Supporting Rules

6.1. The Encryption Manager will centrally administer the RWC encryption management program for all RWC members.

6.2. All RWC members using encryption will designate a departmental Encryption Key Owner for the control and authorization of the encryption keys associated with departmental owned talkgroups.

6.2.1. Each CKR will have a single designated Key Owner that is assigned by talkgroup owner.

6.2.2. All authorizations for use and distribution of the encryption keys will be made in writing by the approved Key Owner using the RWC workbook.

6.2.3. The Key Owner is the authority to modify any assignment of the CKR.

6.3. The Encryption Manager will maintain an encryption key map showing current assignments and authorizations, and a list of CKR Owners. This information will be distributed periodically to the Encryption Key Owner for validation. Subsequent changes to the current encryption key map and list of owners will be by notification of exception.

6.4. Key Generation

6.4.1. RWC encryption keys will be generated by the Encryption Manager using the automatic key generation capabilities of the Key Management Facility (KMF).

6.4.2. RWC encryption keys will be generated using 256 bit Advanced Encryption Standard (AES).

6.4.3. The active key material will be changed on a periodic basis, not to exceed 24 months.

6.4.4. Ranges for the CKRs are maintained by the Encryption Manager.

6.5. Key Distribution

6.5.1. Member agencies are required to own or have access to a Member owned RWC provisioned Key Variable Loader (KVL).

6.5.2. KVLs owned by other entities and provisioned by the RWC must be formally authorized by the OWG.

6.5.3. Authorized KVLs may contain a Universal Key Encryption Key (UKEK) and other keys approved by the Key Owner(s).

6.5.4. Contractor owned KVLs authorized by the RWC shall only contain a contractor specific UKEK.

6.5.4.1. Contractors shall coordinate with the Encryption Office for all encryption services.

6.5.5. The RWC recommends that all encryption keys for subscribers be sent or updated via the KMF only. However, agency specific encryption keys may be manually loaded upon approval of the Key Owner.

6.5.5.1. Encryption keys loaded manually with a KVL will not show on the Encryption Summary Report unless the subscriber information is provided and entered into a KMF record. It is recommended that the information of subscribers with manually loaded keys be sent to the Encryption Manager so a record can be maintained.

6.5.5.2. Subscribers containing manually loaded encryption material will lose their encryption access when a key material change is performed on any CKRs that they have access and will need to be manually reloaded.

6.5.5.3. Subscribers containing manually loaded encryption material cannot have keys removed or access deleted via Over the Air Rekeying (OTAR) - keys must be manually erased.

6.5.6. Manual loading of CKR 1 via a KVL in to any subscriber is not authorized without the approval of the OWG.

6.5.7. Console Key Loading

6.5.7.1. Agencies requesting Over the Ethernet Keying (OTEK) for their consoles will be responsible for loading of a UKEK using an authorized KVL.

6.5.7.2. Consoles that do not support OTEK must have keys manually loaded via KVL by a responsible Member agency.

6.5.8. Destruction of active key material contained in a subscriber will be accomplished by zeroizing the key set in the subscriber via the KMF, KVL, or manual operation if available.

6.6. Key Material Distribution

6.6.1. Requests for distribution of Member owned key material to be used in non-member KVL and KMFs must be made in writing (letter or email) by the Key Owner, and sent to the Encryption Manager.

6.6.2. It will be the responsibility of the Encryption Manager to present a written request for distribution of any encryption material to be used in a non-member KVL or KMF to the OWG for approval.

6.6.2.1. The agency making the request must include the following: Purpose for the request, number of subscribers needing access, key material requested (i.e., CKR 1) and the name and contact information for the non-member agency.

6.6.2.2. Distribution of encryption keys will be by physical exchange of the key material directly from the KMF to the KVL device(s).

6.6.3. RWC keys shall not be transferred by direct KVL to KVL connection.

6.6.4. Agencies must provide a report of all subscribers containing any OWG owned key material within three (3) business days upon request by the RWC.

6.6.5. It will be the responsibility of the non-member agency to obtain new key material in the event of an encryption key set change.

6.7. Encryption Materials

6.7.1. The RWC encryption database will be backed up and stored onsite in the Encryption Services Office, as well as offsite as designated by the Encryption Manager.

6.7.2. The RWC encryption database will be stored in encrypted format.

6.7.3. If the integrity of the RWC encryption database is compromised, all RWC key material will be immediately changed.

7.0 Responsibilities

7.1. The Encryption Manager will provide encryption services during normal business hours, Monday through Friday, 8:00 am to 4:00 pm, excluding defined holidays. All encryption related requests should be sent to RWC.Encryption.ppd@phoenix.gov. Any requests received after hours will be processed according to the timelines outlined in this policy. Any after hour support requests will be evaluated on a case by case basis and will only be considered in exigent circumstances.

7.1.1. A minimum of three (3) business days lead time is required for all encryption requests, unless special circumstances exist. Larger projects may require a longer lead time.

7.2. Encryption Manager

7.2.1. Performs key management functions on a day-to-day basis.

7.2.2. Protects keying materials and limits access to individuals with a valid need-to-know.

7.2.3. Configures security features of key management system components in accordance with RWC policies.

7.2.4. Maintains required RWC encryption key workbooks and related documentation for a period of 24 months.

7.2.5. Performs periodic backup of KMF databases.

7.2.6. Reports any known or suspected incident involving keying material to the OWG.

7.2.7. Creates and loads keys into KVLs.

7.2.8. Coordinates with RWC members relative to the daily operational aspects of RWC encryption.

7.2.9. Responsible for receiving and investigating any encryption-related incidents, including oversight of corrective actions related to compromised subscribers containing encryption keys.

7.2.10. Zeroizes subscribers that have become compromised.

7.2.11. Authorizes the establishment and closure of system accounts for the key management facility.

7.2.12. Provides administrative guidance on the implementation of RWC key management activities.

7.2.13. Assigns all CKR numbers as part of the talkgroup approval process.

7.2.14. Ensures that encryption reports are generated monthly and distributed.

7.2.15. Ensures that currency reports are generated quarterly and distributed.

7.2.16. Ensures completion of annual KVL audit.

7.3. RWC Executive Director is responsible for facilitating requests from outside agencies for KVL access to RWC key material and presenting the requests to the OWG for approval.

7.4. Authorized KVL Owner Responsibilities

7.4.1. Ensuring KVL devices will be physically secured at all times when not in use.

7.4.2. Responsible for loading of the initial UKEK or authorized encryption keys into all RWC subscribers requiring secure capabilities.

7.4.3. Verifies that the Radio Set Identifier (OTAR ID) matches the subscriber ID before loading encryption keys.

7.4.4. Immediately reports any known or suspected incident involving compromised key material to the Encryption Manager who in turn notifies the OWG.

7.5. RWC Participating Agencies

7.5.1. Maintain inventory control of secure subscribers.

7.5.2. Designate individual(s) in the agency to act as the Key Owner.

7.5.2.1. Each secure key will have a single owner.

7.5.2.2. The Agency may delegate a temporary alternate Key Owner to act in the absence of the primary Key Owner.

7.5.3. Responsible for implementing a training program for agency personnel relative to proper use of subscribers containing encryption keys.

7.5.4. Load and maintain agency owned KVLs.

7.5.5. Any agency utilizing encryption capable consoles must have access to their own KVL or arrangements need to be made with another Member to provide this service.

7.5.6. Responsible for reporting lost or compromised radios to the RWC using the established distribution list (see RWC Lost Compromised Radio Procedure).

7.6. Key Owners

7.6.1. Responsible for authorizing subscriber encryption through the Encryption Manager.

8.0 Encryption Management Process

8.1. Requests for Creation of CKRs

8.1.1. CKR creation requests must be made in writing (letter or email) and sent to the Encryption Manager. This request must include CKR number, CKR name, and Key Owner information.

8.2. Addition or Changes to Subscribers in the KMF

8.3. All requests for the addition of new subscriber IDs or any encryption changes requested to existing IDs or names must be made using the approved RWC workbook. Requests for encryption permissions will be the responsibility of the requesting agency to secure from each Key Owner affected. Additions or change requests need to be sent to the Encryption Manager for processing.

9.0 Conditions for Exemption or Waiver

9.1. As provided in the Waiver or Exception Policy.

10.0 Applicable Policies and/or Procedures

10.1. As listed at www.rwcaz.org.