CONSOLIDATED COMMUNICATIONS NETWORK OF COLORADO

POLICY & PROCEDURE MANUAL

Revised/Updated July 2024

TABLE OF CONTENTS

15.1.4.3.4 MAC 12 SE
15.1.4.4 MAC 13 SW THRU MAC 16 SW (SOUTHWEST)
15.1.4.4.1 MAC 13 SW
15.1.4.4.2 MAC 14 SW
15.1.4.4.3 MAC 15 SW
15.1.4.4.4 MAC 16 SW
15.1.4.5 MAC 17 THRU MAC 20 NW (NORTHWEST)
15.1.4.5.1 MAR 17 NW
15.1.4.5.2 MAC 18 NW
15.1.4.5.3 MAC 19 NW
15.1.4.5.4 MAC 20 NW
15.1.5 CO MAC 21 (STATEWIDE)
15.1.6 REGIONAL EMERGENCY MEDICAL AND TRAUMA ADVISORY COUNCIL (RETAC) REGIONAL MUTUAL AID
15.1.6.1 EMS MH
15.1.6.2 EMS NE
15.1.6.3 EMS PP
15.1.6.4 EMS SE
15.1.6.5 EMS S
15.1.6.6 EMS FH
15.1.6.7 EMS CM
15.1.6.8 EMS NW
15.1.6.9 EMS SLV
15.1.6.10 EMS SW
15.1.6.11 EMS W
15.1.6.12 EMS MAC
15.1.6.13 ER MAC
15.1.7 COUNTY HEALTH DEPARTMENTS
15.1.7.1 CHD NE
15.1.7.2 CHD NC
15.1.7.3 CHD SC
15.1.7.4 CHD S
15.1.7.5 CHD SE
15.1.7.6 CHD NW
15.1.7.7 CHD W
15.1.7.8 CHD SW
15.1.7.9 CHD SL
15.1.8 SCHOOL BUS TALKGROUPS

CHAPTER 1 PURPOSE

The Consolidated Communications Network of Colorado, CCNC, is a non-profit corporation organized exclusively for the purpose of managing, promoting, and propagating the Colorado Statewide Digital Trunked Radio (DTR) System, under and by virtue of the laws of the State of Colorado. CCNC membership is made up of the agencies that participate on the Statewide DTR System under and by virtue of the laws of the State of Colorado. The primary objectives of the project are:

- To achieve interoperability with all participating agencies.
- Improve statewide radio coverage.
- Improve radio spectrum efficiencies.
- Develop and use partnerships to build a systems of systems radio network, sharing costs and resources while providing added value for all users.

The levels of participation will vary by agency from partners that own and operate a portion of the system down to a single radio user. Each user agency will determine their individual mobile, portable and console equipment needs. Any local, regional, tribal, state or federal agency that chooses to participate will have the capability to communicate not only within their organization but also with all other participants.

Please see the CCNC ***Articles of Incorporation***.

CHAPTER 2 OVERVIEW/SCOPE AND AUTHORITY

The Statewide DTR System infrastructure is comprised of a consortium of sites, wireless links, wireline links, network equipment, and servers which provide the uniform statewide radio coverage for public safety and public service users from local governments, county, state, tribal, federal agencies, special districts, and EMS providers.

This manual was developed in order to provide policies and procedures for use of the system, subscriber equipment, and delineating various technical and operational matters.

The CCNC as a group operates under a set of by-laws developed by the users. Each agency and its users will subscribe to this guide as the defined methods in order to achieve operational efficiency of the system. The By-laws are reviewed and amended as necessary.

The systems goal is to provide radio coverage throughout the State of Colorado, to public safety users so that they can provide essential government services and have wide area radio interoperability.

This manual will be an evolving document in order to address needs that arise from an ever- developing technology. The technical staff members that work under the Technical & Operations Committee will vigilantly monitor the systems performance and make recommendations to the CCNC Board of Directors addressing necessary adjustments to the system to maintain optimum performance. The committee's scope and authority are defined in the By-laws.

Please see ***CCNC Bylaws.***

CHAPTER 3 CONFLICT OF INTEREST POLICY

Directors of the Consolidated Communications Network of Colorado, Inc., in accordance with applicable state statutes, shall not be, or become, involved in any activity which is a conflict of interest. A Director shall not engage in activities where they may receive a gift, compensation, or payment in return for an official act, or for the performance of any service, in their role as a Director.

Should a conflict arise after a member has been elected to a director position, it is the responsibility of the Director to notify the other Board members in an open meeting before any discussion or action is taken. The affected Director(s) shall not actively participate in the discussion of any matters in which they have an identified conflict of interest or cast a vote relative thereto.

CHAPTER 4 RECORDS RETENTION POLICY

This General Records Retention Schedule lists records commonly originated and maintained by the Consolidated Communications Network of Colorado, Inc. Electronic mail messages sent or received on a system not maintained by CCNC are not considered records of CCNC and are not subject to this Records Retention Policy.

Record Title	Retention Period
General Correspondence and Subject Files	
A. Documentation on the establishment or implementation of policy, procedure, programs, organizational structure, or history of the organization.	Permanent
B. Documentation on the routine administration and transactions of the - organization.	1 year or until no Longer needed for reference.
Agenda, Meeting Minutes and Election Results	
A. Agenda of items to be discussed or acted upon, and the Minutes of proceedings of general membership meetings, executive board meetings, technical & operations committee meetings, operations committee meetings, and other sub-committee meetings.	Permanent
B. Ballots for the election of Regional Directors, Executive Directors and Officers of the Board of Executive Directors.	1 Year
Applications	
A. System Participation Agreement, Statewide DTRS Participant Application, Update Agreement, System Key Application and Agreement, Statewide DTRS Participant Agreement for Tribal Agencies.	Permanent
Accounting Payment and Reports Documentation	
A. Purchase requisitions or orders, invoices, packing slips, payment vouchers, claim vouchers, any other documentation for or relating to expenditures.	6 years
B. Files or documentation relating to payment on contracts or leases.	Until related lease or contract is no longer retained.
C. Monthly Treasurer's Report	6 years
Bank Account Records	
A. Account statements, cancelled checks, check stubs, deposit receipts, account reconciliations for bank checking and savings accounts.	6 years
Contracts And Leases	

A.	Original copies of contracts and agreements.	6 years after expiration or fulfillment of all terms of the agreement or contract, whichever is later, provided the agreement or contract no longer has any binding effect. Prior to destruction, evaluate for continuing legal, administrative or historical value.
B.	Original copies of leases.	6 years after termination

CHAPTER 5 WHISTLE BLOWER POLICY

If any director, officer, member, or employee reasonably believes that some policy, practice, or activity of the Consolidated Communications Network of Colorado, Inc., is in violation of law, a written complaint may be filed by that director, officer, member or employee with the President of the Board. If the complaint involves the President of the Executive Board, the director, officer, member, or employee may file the written complaint with any officer of the Executive Board.

It is the intent of the Consolidated Communications Network of Colorado, Inc., to adhere to all laws and regulations that apply to the organization, and the underlying purpose of this policy is to support the organization's goal of legal compliance. The support of all directors, officers, members, and employees is necessary to achieving compliance with various laws and regulations.

A director, officer, member or employee is protected from retaliation only if the director, officer, member or employee brings the alleged unlawful activity, policy or practice to the attention of the Consolidated Communications Network of Colorado, Inc., and provides the Consolidated Communications Network of Colorado, Inc., with a reasonable opportunity to investigate and correct the alleged unlawful activity. The protection described below is only available to directors, officers, members, or employees that comply with this requirement.

The Consolidated Communications Network of Colorado, Inc., will not retaliate against a director, officer, member, or employee who, in good faith, has made a protest or raised a complaint against some practice of the Consolidated Communications Network of Colorado, Inc., or of another individual or entity with whom the Consolidated Communications Network of Colorado, Inc., had a business relationship, on the basis of a reasonable belief that the practice is in violation of law or a clear mandate of public policy.

The Consolidated Communications Network of Colorado, Inc., will not retaliate against a director, officer, member, or employee who discloses or threatens to disclose to a director, officer, or a public body any activity, policy, or practice of the Consolidated Communications Network of Colorado, Inc., that the director, officer, member, or employee reasonably believes is in violation of a law, a rule, or a regulation mandated pursuant to law or is in violation of a clear mandate or public policy concerning health, safety, welfare, or protection of the environment.

CHAPTER 6 TRAVEL POLICY

Eligible CCNC members for Per Diem & Mileage Reimbursement:

CCNC Officers and Administration shall be eligible for Per Diem, Mileage reimbursement for any corporate responsibility which requires a travel distance greater than 100 miles from point of departure to destination one way. CCNC Executive Board members may request reimbursement for annual CCNC Executive Board Work Session. Other members wishing reimbursement requires Executive Board approval.

Eligible CCNC members for Lodging Reimbursement:

CCNC Officers and Administration shall be eligible for Lodging reimbursement for any corporate responsibility which requires a travel distance greater than 100 miles from point of departure to destination one way and will be attending a CCNC function that warrants an overnight stay for preparation or safe return to home based on not being able to return by a normal close of business. CCNC Executive Board members may request reimbursement for annual CCNC Executive Board Work Session. Other members wishing reimbursement requires Executive Board approval.

Per Diem (Meals), Lodging, & Mileage Reimbursement Rates:

Per Diem, lodging, and mileage reimbursement rates will be the rates published on the government site GSA.GOV at ***http://www.gsa.gov/portal/content/104877*** . Exceptions to this must be approved by the Executive Board on a case-by-case basis. The attached CCNC mileage form will be provided with any request for reimbursement. There is an alternative Excel spreadsheet that can be requested through the CCNC Secretary.

Per Diem (Meals), Lodging, & Mileage Reimbursement:

Requests for reimbursement will processed through the CCNC Secretary or Designee and paid by the CCNC Treasure. Any requests for exceptions to this policy will be brought to the attention of the Executive Board by the CCNC Secretary.

CHAPTER 7 PURCHASE CARD/BUSINESS DEBIT POLICY

CCNC business debit cards will be used for official CCNC business only. The CCNC Treasurer is the designated Business Debit Card Manager (BDCM). The eligible business debit card holders are the CCNC Officers, Administrative Assistant, and others as designated by the Executive Board.

If a purchase is over $1,000.00 the purchase must be approved by the CCNC Executive Board. If there are time constraints or other special conditions purchases over $1,000.00, but less than $5,000.00, may be approved by two Officers.

If there is accidental use of the CCNC business debit card, the card holder must notify the BDCM in writing, and arrange for a reimbursement to CCNC as soon as possible, but not to exceed thirty (30 days). Any accidental use will be reported by the BDCM to the Executive Board at the next meeting.

The monthly spending limit is $1,000.00. The BDCM's card will be unlimited. Purchases over $1,000.00, with approval, will be coordinated through the BDCM. The allowable charges are items covered by the CCNC budget.

Prohibited transactions include, but are not limited to: Cash Advance/Travelers checks, entertainment, spirits, personal use and personal services. Any unauthorized or prohibited use by the card holder shall be the financial responsibility of the card holder, and shall be reimbursed to CCNC within thirty (30) days of purchase.

The Business Debit Card Holder Responsibilities:

a) The person issued the card is the only one authorized to use the card. Cards are issued to one individual and cards should NEVER be given or shared with anyone.
b) The card holder shall provide the Business Debit Card Information, I.E: card number, name on the card, the expiration date, and security code on the back of the card to the BDCM.
c) If the card is declined – Notify the BDCM.
d) If the card is stolen or lost – Notify the BDCM and the bank immediately.
e) The card holder is to notify the BDCM of any suspected privacy breach of their assigned card.
f) The card holder will keep contact information up to date with the BDCM.
g) The Business Debit Card will remain the property of CCNC. Upon leaving their position with CCNC, the card holder must return the card to the BDCM within ten (10) business days.
h) Card holder will provide purchase documentation to the DBCM within ten (10) days of purchase.
i) The card holder will provide a statement in writing to the BDCM to document any lost or unavailable purchase documentation.

The Business Debit Card Manager Responsibilities:

a) Reconciliation of the bank statement.
b) Activation and deactivation of Business Debit Cards.
c) Monitor Business Debit Card accounts for fraud.
d) Ensure that unauthorized use is noted in the monthly Treasurer's report.
e) BDCM shall ensure the Business Debit Card information belonging to the card holders, I.E.: card number, name on the card, the expiration date, and security code on the back of card, is kept on file.

An increase of monthly purchase amount limit, or any other changes to this policy must be approved by the Executive Board.

CHAPTER 8 FUNDING

CCNC, as a non-profit organization, may implement a membership fee after notifying its member of such action. This fee may be used to offset the corporations operating fund, provide member training, provide member events and for corporate travel no covered by an agency. The fee may also be used to promote the corporation statewide, assist with advocacy where necessary, and provide corporate involvement in communication activities. At this time, the feels will not assist in funding any infrastructure, maintenance or purchase of radio equipment.

The Corporation is organized exclusively for the purpose of managing, promoting, and propagating the statewide radio network under and by virtue of the laws of the State of Colorado concerning nonprofit corporation and shall have and exercise all the rights, powers and privileges granted to such corporations by those laws, as amended from time to time, subject to the restrictions and limitations contained in these articles.

The purpose of the Corporation shall be to promote and support social welfare and public safety and lessen the burden to government through the support of the following activities and purpose.

From the Articles of Incorporation:

- The corporation may solicit and receive gifts, donations, grants, contributions, devices, bequests, and other property, real or personal, tangible and intangible, and will hold, manage, control, sell, transfer, invest and reinvest the same.
- The corporation may generate revenue as determined appropriate by the Board of Directors.

No part of the net earnings of the Corporation, nor any assets of the Corporation, shall inure[1] to the benefit of any member, director, or officer of the Corporation, or any private individual, except that the Corporation shall be authorized and empowered to pay reasonable compensation for the service rendered, to reimburse actual expenses.

CHAPTER 9 SYSTEM SECURITY

All personnel who have access to the DTR system, including sites, site equipment, the system networks, system console equipment and those who have direct responsibility to configure and program subscriber units must pass a state and national fingerprint-based criminal history record check and be granted authorization from the CCNC Executive Committee and the State of Colorado Office of Public Safety Communications, hereinafter referred to as the OPSC. If a fee is charged for this background check the cost will be the responsibility of the employer of the subject of the background check.
The State of Colorado (SOC) uses an advanced radio system to provide mission critical two-way voice communications to thousands of public safety responders and governmental organizations across the state. In keeping with technology Best Practices, network security, and system performance, it is critical that all Digitally Trunked Radio System (DTRS) users comply with Consolidated Communications Network of Colorado (CCNC) and SOC Office of Public Safety Communications (OPSC) policies and procedures. This is particularly critical for system key holders programming radios to place on the system.

An 'Advanced System Key' (ASK) is a specialized hardware device used in programming subscriber equipment (radios.) The ASK has predefined security and permissions to prevent unauthorized use of software, programming information, and radio types that access the SOC DTRS. The holder of an ASK is held to the highest standards to ensure the integrity of the system, the radio equipment, and the first responders that rely on a radio in performance of their duty. Thus, it is of great importance that proper training, authorization, and oversite be held to the highest standards.

CCNC Board Members, working with the SOC OPSC DTRS Program Manager has come up with an Advanced System Key Training and Testing Program. This program may change based upon technological advances, governance needs, and policy changes by CCNC and the SOC. Contact the DTRS Program Manager, the CCNC Executive Board, or CCNC Regional Representative for the latest policy.

To be granted an ASK, you must complete specialized-training, demonstrate competence in radio programming, and have a comprehensive understanding of the DTRS system and knowledge of the SOC and CCNC policies.

All system key holders in good standing are required to complete the Knowledge City training and testing on a two-year basis for the key renewal process.

To obtain an Advanced System Key you must complete the following steps:

1. Go to the website ccncinc.org and to the Advanced System Key Link
    a. System Keys - Consolidated Communications Network of Colorado Inc. (ccncinc.org)
    b. Read and understand the documentation
2. Click on the link for the ASK application and agreement
    a. APPENDIX C (ccncinc.org)
3. Read over the ASK application for pertinent information
4. Contact your local ARWG by checking the CCNC website for questions or guidance with filling out the System Key Application

5. Attach evidence of a nationwide fingerprint based background check or agency background check, proof of CPS training and proficiency with CCNC Policy, and testing certificate, as stated in the ASK agreement
6. Submit ASK application and supporting documents mentioned in #5 above, to the DTRS Program Manager
    a. The State of Colorado approves or denies all System Key Applications
7. Once a System Key Application is approved, the applicant will be notified
8. Applicant is responsible for getting the proper training and testing before an Advanced System Key may be issued
9. Arrange for training from an approved trainer by contacting the DTR Program Manager
    a. Training must be done for each manufacturer ASK
        - For example, there will be a different key for Motorola, EFJ, Kenwood, BK RELM, ICOM, Tait, and Harris, etc
    b. Online training and testing for manufacturers are currently limited to Motorola
    c. All applicants will be required to take the Policy and Procedures online test, regardless of the radio manufacturer
        - Other radio manufacturer tests will be added as they are completed and made available
10. Training could be time and space limited depending on the manufacturer key for which the applicant needs training
    a. For example, if you are getting the training from Douglas County, they do training once a quarter for up to 4 trainees
    b. It is recommended to schedule training as early as possible
11. Applicants are responsible for their own scheduling, travel, and other requirements to get to and from training
    a. CCNC and SOC are not responsible for getting an applicant to a training or testing location, or ensuring the applicant has the required items for the testing or training with them, such as a laptop capable of accessing the internet.
12. When training is complete, the trainer will notify the DTRS Program Manager
13. The DTRS Program Manager, will notify the approved administrators to add the applicant to the Knowledge City testing site and the applicant will be emailed a notification from Knowledge City
14. Applicant must take the Knowledge City test at one of the 13 State of Colorado office locations listed on the CCNC website
    a. Testing can be scheduled once per quarter same as the training
        a. Schedule can be located on the CCNC website
        b. It is recommended to schedule testing as early as possible
    b. Applicant is required to bring a photo ID and agency affiliation, a laptop with internet capability, and provide for their own travel to the State office being used as the testing center
    c. Must provide identification to State personnel, as requested
15. Applicant must take the Knowledge City test at a sanctioned state testing center and pass the test w/ 90% or above
    a. Test is open book
    b. State proctor will not respond to any questions from the applicant during the test.
    c. 75 questions in 75 minutes
    d. Test includes both Manufacturer and Policy and Procedure questions
    e. There is a 30-day waiting period before the test can be rescheduled to be retaken if applicant fails to achieve a score of 90% or greater

16. DTRS Program Manager will be notified that the testing is complete, the applicant will print out the certificate to send in with application
17. Applicant will request test documents from DTR Monitoring to build the required three test code plugs.
18. Complete the following using test code plug documents and criteria provided by DTR Monitoring to the applicant
    a. Three blank fresh code plugs per manufacturer key requested to be submitted to DTR monitoring for review/approval/denial
    b. Once the three fresh code plugs have been vetted and are found to be error free, applicant will be eligible to receive a 30-day provisional system key in order to take the practical JPR test with the assigned Proctor
        - Must pass JPR testing with 100%
    c. Once JPR test is complete, the Proctor will notify the DTRS Program Manager
19. DTRS Program Manager will vet all application requirements and send it for final approval to the CCNC Executive Board
20. Once the ASK application and agreement are completed and approved, the applicant will be issued an applied key by the SOC

Annual Renewal

1. Applicant will mail or meet in person the State representative to get the ASK renewed before the end of March each year
2. Have the ASK Renewal Agreement completed
3. Verify and submit unexpired ASK Knowledge City Certificate
4. Verify and Submit Background check

Every 2 years

1. Per the System Agreement, a new State and National fingerprint based criminal history record is required to be renewed/obtained
2. The ASK Knowledge City test needs to be retaken and a new certificate received
    a. Contact the DTR Program Manager to receive a new Knowledge City test logon

    b. Renewal tests for Knowledge City can be taken locally and applicant does not need to travel to a State Test Center

All ASK holders are responsible for understanding and following all SOC and CCNC policies and procedures in regard to the use and ability to have an Advanced System Key.

9.1 PERSONNEL BACKGROUND SCREENING FOR DTR SYSTEMS ACCESS /SYSTEM KEY ACCESS

To verify identification, state of residency and national fingerprint-based criminal history checks shall be conducted within 30 days prior to initial employment or assignment for all personnel who have authorized access to the DTR system and those who have direct responsibility to configure and program subscriber units and/or DTR network equipment operating on the DTR system. Agencies with wireline console connectivity will be responsible for conducting background checks for all their employees that have access to dispatch consoles or user terminals to ensure the security of the console network. All other requests for DTR system access or DTR System Key access shall be made as specified to the CCNC EXECUTIVE COMMITTEE AND THE OPSC. The CCNC EXECUTIVE COMMITTEE AND THE OPSC, or their official designee, is authorized to approve DTR system access. All official designees to the CCNC

EXECUTIVE COMMITTEE AND THE OPSC shall be from a CCNC User agency or the OPSC.

If a felony conviction of any kind exists, the requesting person shall be denied DTR system access and access to the DTR System Key. However, the requesting person or the employing Agency for the requesting person may ask for a review by the CCNC EXECUTIVE COMMITTEE AND THE OPSC in extenuating circumstances where the severity of the offense and the time that has passed would support a possible variance.

If a record of any other kind exists, systems access shall not be granted until the CCNC EXECUTIVE COMMITTEE AND THE OPSC or their official designee reviews the matter to determine if systems access is appropriate.

If the person is determined to be a fugitive appropriate action will be taken immediately.
If the person appears to have an arrest history without conviction for a felony or serious misdemeanor, the CCNC EXECUTIVE COMMITTEE AND THE OPSC or his/her official designee shall review the matter to determine if systems access is appropriate.

If an applicant has already undergone a nationwide fingerprint based criminal background check as a prerequisite or a condition for hire with their current employer, a letter on department head and signed by the highest level of authority within the agency may be substituted for the additional nationwide background check. The letter must contain language stating the nationwide background check is a condition for hire, and that the employer understands the requirement for notice to the OPSC in the event the employ is notified of their employee being charged with criminal activity.

If the person already has passed a recently conducted criminal history check for access to another public safety agencies systems, the CCNC EXECUTIVE COMMITTEE AND THE OPSC or their designee may grant systems access without requiring a new security check. A Criminal Justice Information System (CJIS) Security Level Training Certificate may be substituted for the FBI Background check.

If the CCNC EXECUTIVE COMMITTEE AND THE OPSC or their official designee determines that DTR systems access by the person would not be in the best interest of the CCNC Membership, access shall be denied and the person's appointing authority shall be notified in writing of the access denial.

Support personnel, contractors, and custodial workers who access DTR system areas shall be subject to a state of residency and national fingerprint-based record check, unless these individuals are escorted by authorized personnel at all times. Support personnel and contractors who access DTR system areas may submit evidence of their participation in the State of Colorado – Criminal Justice Information Systems (CJIS) Vendor Management Program as a substitute for and FBI background check.

9.2 SYSTEM KEY AND FLEETMAP SECURITY STATEMENT

Participating agencies in the Colorado Statewide Digital Trunked Radio (DTR) System and CCNC have operational needs that require the use of various talkgroups to meet their communication needs. Agencies need to be able to manage the use of their agency talkgroups to meet their agency communications requirements and expectations. Agencies may also have need for communications with other CCNC users or with radio users from other systems outside of the DTR. Agencies must be able to satisfy these communications requirements in ways that are both effective and efficient while maintaining the integrity of the System Fleetmap. Fleetmap information is system sensitive information

that should not be divulged without proper security procedures and a valid need to know. The user agency needs must be balanced with the system security and capacity requirements so as not to have an adverse effect upon system performance.

The Office of Public Safety Communications (the State) will be responsible for managing the Fleetmap information for all agencies on the system. The DTR Monitoring Center (DTRMC) shall be notified of all new talkgroups to be added to the system and all approved name changes. New talkgroups must be approved by the CCNC Technical Committee prior to activation; see CHAPTER 10 and/or CHAPTER 11 Notification shall be by email to webdtr@state.co.us.

9.3 SYSTEM KEYS

As the owner of the DTR System Identification Number, the State will house and keep secure the Master System Key for all manufacturers of equipment authorized to operate on the system. Agencies requesting a system key will complete the ***COLORADO DIGITAL TRUNKED RADIO (DTR) SYSTEM, SYSTEM KEY APPLICATION AND AGREEMENT***, and submit the completed application to the OPSC for review for accuracy and completeness.

The State OPSC will be responsible for programming keys for eligible programming agencies. Manufacturer Software Keys or files are not permitted for programming use on the DTR system. The use of any DTR System Key and associated equipment is subject to all rules, regulations and policies established by the State of Colorado, CCNC, the FCC and applicable vendor. Any violation will result in the **COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM, SYSTEM KEY APPLICATION AND AGREEMENT** being terminated and the DTR System Key revoked.

9.3.1 ELECTRONIC SYSTEM KEY POLICIES

Agencies requesting a system key will complete the ***COLORADO DIGITAL TRUNKED RADIO (DTR) SYSTEM, SYSTEM KEY APPLICATION AND AGREEMENT***.

System Keys will only be issued to authorized CCNC infrastructure owners that are self-maintained and use the System for their primary dispatch functionality, to Manufacturer Authorized Service Shops that are maintaining equipment for CCNC Agencies, and to member agency users with a verifiable and justifiable need for a programming key to support a significant radio fleet size, and only after completion of approved training. Approved training is defined as completion of designated training course provided by the CCNC training committee designee. Vendor provided courses are encouraged but are not a substitute for the CCNC training.

No CCNC Party will directly or indirectly permit any third party to: view, read, print, extract, copy, archive, edit, create, clone, transfer, tamper with, or otherwise compromise the security of any radio code plug programming file, system key file, encryption key file, or template information for any radio on the system. The System Key will not be distributed or any DTR radio ID's or talkgroup(s) information disclosed to a third party for any reason. However, DTR Advanced System Key holders may create code plugs and provide the code plugs to qualified agencies or service providers for programming into subscribers' units.

In the event that a CCNC agency, individual member or member associate learns that any party has improperly or fraudulently obtained radio code plug file information, system key file information, encryption key file information, or template data, they will immediately notify the CCNC Executive

Committee and the OPSC of the security breach.

Any Agency or Service Provider found to be responsible for a security breach as listed above will be responsible for the cost of all reprogramming to include but not limited to system infrastructure and subscriber programming necessary to overcome said breach.

System Keys that are capable of expiring will be set to expire annually and will be reissued annually after reverification of agency needs.

Only ID(s) and talkgroups that have received prior authorization from CCNC may be programmed, including talkgroups programmed for receive-only operation.

Self-maintained agencies may only program radio ID(s) and talkgroup(s) of the DTR radio system for their own agency or agencies they provide DTR subscriber maintenance. Agencies shall provide copies of all talkgroup authorization letters to the DTRMC at webdtr@state.co.us. Private Service providers may only program radio ID(s) and talkgroup(s) of the DTR radio system for which they provide DTR subscriber maintenance. All requests for ID's and programming codes from a private service must be accompanied by an appropriate copy of a written authorization from the agency granting the requesting shop permission to program their radios. Providers shall provide copies of all talkgroup authorization letters to the DTRMC at webdtr@state.co.us.

All radios will be programmed for write protect file access if the equipment supports the write protect function.

All radios will be programmed to allow Radio Inhibit from the System Management Terminal. Any radio sent to the vendor for repair may be sent with the programming intact. Whenever possible, the sending agency should archive the file from the radio prior to shipping. When radios are returned from Vendor repair, they should be verified for correct codeplug information and that they are write protected if capable.

All System Key holders shall maintain current and accurate records of all programming performed. Records shall be made available upon request to the State of Colorado OPSC or CCNC. Any programming agency with a System Key will provide electronic update to the DTR Monitoring Team for any radios that have been added, removed or modified in the UCM. This update should be sent via email within five (5) days of the change. The recommended format is a spreadsheet with 19 columns labeled:

- Radio Type (APX6000, XTS2500, VP6430);
- Radio ID (8-Characters);
- Serial Number;
- Radio Alias (16-Characters);
- Radio User;
- Organization;
- Owner;
- Model;
- Flash Code;
- HOST Version; Optional

- DSP Version; Optional
- County;

9.4 SYSTEM PROGRAMMING EQUIPMENT

Each programming agency will be responsible for acquiring the proper programming software and equipment necessary to program the radios they support. Approved system key holders are fully responsible for purchasing the necessary hardware (USB device, iButton, etc.)

The System ID programmed on the Ibutton or other manufacturer hardware remains the property of the State of Colorado. Programming software and the required cables purchased by an agency or service provider remain the property of the agency or service provider.

Any Computer connected to the system or used for any radio programming will have up to date antivirus software installed and maintained. See Section 10.7

CHAPTER 10 MEMBER RIGHTS AND RESPONSIBILITIES

CCNC Members' rights and responsibilities are determined by their status as Primary Members, Subsidiary Members, or Associate Members and by the infrastructure assets they commit to the DTRS.

10.1 CCNC PRIMARY MEMBERS

Primary Members are government entities that collect taxes and make use of the DTRS as their primary means of communications. Primary Members examples: state government, counties, cities, towns, and special districts. They may have their own talkgroups on the DTRS. Primary Members may vote and participate in the governance of CCNC. Any taxing entity must be a Primary Member in order operate on the DTRS . Primary Members may be required to pay membership fees to CCNC as established by CCNC policy.

CCNC Primary Members have the right to interoperable communications statewide through the use of a travel channel, mutual aid talkgroups, regional interoperability talkgroups and/or conventional interoperability channels. Primary Members have the right to communicate their dispatch traffic or their daily business traffic on those sites that they have implemented into the DTRS, on those sites that they have been granted communication access to through negotiations with the site equipment owner, or to those sites where they have been granted communication access as compensation for having implemented site resources to compensate for their traffic loading at sites owned and maintained by other agencies.

Primary Members do not have the right to unlimited dispatch communications or their daily business communications on all DTRS sites. Primary Members have the responsibility of limiting their dispatch communications and/or their other daily business communications to only those DTRS sites that provide coverage in their response area.

The owners of DTRS site equipment and/or connectivity equipment between DTRS sites are responsible for the maintenance of such equipment as identified in Maintenance- System Infrastructure, 16.4.

CCNC Primary Members who have invested in the Statewide DTR System infrastructure by developing communications sites retain all their rights as owners of the equipment. This includes the right to coordinate with other eligible users to provide or restrict communication access to their sites for usage beyond mutual aid communications. Coordinated agreements may include but are not limited to provisions for usage fees, ongoing maintenance provisions, infrastructure improvements, and/or reciprocal uses of infrastructure.

Site access may be restricted using one or both of the following methods:

- *Site Preferences based on a list programmed into each subscriber unit that selects sites by evaluating the Received Signal Strength (RSS) and Bit Error Rate (BER) readings in the subscriber or denial by site access profiles in the User Configuration Manager (UCM).*

- *Site Preferences can help to steer radio site access in cases where sites have little coverage*

overlap and the preferred site/s provide the strongest RSS/BER readings in your normal coverage area.

- *Site Access Profiles in the UCM allow subscribers to register with sites based on their Unit IDs and selected Talkgroups. If either the radio's unit ID or its selected talkgroup is disallowed at a site, the radio will not be allowed to remain registered with the site; rather it will roam to* an *adjacent site on which both the unit ID and the talkgroup are authorized to operate.*

Coordinated agreements with the site equipment owners should specify the agreed-upon site access/restriction method.

The CCNC Technical Committee will create and maintain a master list of site access profiles. Updates to any site access profiles (the name of the site access profile which needs to be updated along with the changes that need to be made) may be sent to DTR System Engineering for entering into the system, but must also be sent to the CCNC Technical Committee Chair for maintenance and updating of the master list.

10.2 CCNC SUBSIDIARY MEMBER

Subsidiary Members are departments within the Primary Members' entity. Examples of Subsidiary Members are public works, OEM, EMS, public health, fire department, search and rescue. They do not have their own talkgroups but may use talkgroups owned by Primary Members. They may not vote or participate in CCNC governance. Subsidiary Members must be sponsored by a Primary Member and a sponsorship letter from that Primary Member must be included with this application.

10.3 CCNC ASSOCIATE MEMBER

Associate Members are entities that only use the DTRS for coordination and mutual aid, not as their primary means of communication. An example of an Associate Member is a private ambulance service that coordinates with a Primary or Subsidiary Member. They may only use existing talkgroups designated for mutual aid or interagency coordination. They may not participate or vote in CCNC governance. Associate Members must be sponsored by a Primary Member and a sponsorship letter from that Primary Member must be included with this application.

10.4 CCNC VENDOR MEMBER

A CCNC Vendor Member is a manufacturer, corporate communications equipment distributor, RF Consultant, or Radio Frequency Engineers. A CCNC Vendor Member is established for the purpose of identifying a source that agencies may go to for studying radio coverage, creating appropriate engineering data, selecting the appropriate radio and programming them. Vendors will not have voting privileges but may participate in discussions vital to clarification for the understanding of the topic being discussed. A Vendor Member can help prospective members determine if the DTRS is the appropriate system for them.

Since most agencies do not have the technical expertise, their contracted vendor may speak about technical issues for them during the application process. This includes explaining coverage and site loading studies. If the applicant is not a current member of CCNC, they may make a written request to CCNC or the State Monitoring team to use State assigned talkgroups for this testing. Current members needing vendor assistance should provide the vendor with one of its own radios and designate which talkgroup(s) the vendor is to use for testing. Vendors will not be assigned talkgroup(s).

10.5 PIKES PEAK REGIONAL COMMUNICATIONS NETWORK (PPRCN) MEMBERS

PPRCN members and their radio users that in the future execute, or have in the past executed PPRCN Participation Agreements, will be accepted into CCNC without the necessity of separate application to the CCNC. PPRCN members operating on the DTRS outside the coverage range of PPRCN sites shall be subject to CCNC policies and procedures and shall have the same rights and responsibilities as CCNC User Members . PPRCN members operating within the PPRCN coverage area on PPRCN sites are subject to PPRCN policies and procedures per their PPRCN Participation Agreement.

Should a member within the operational area of PPRCN apply to CCNC, CCNC will not process the application and will recommend the applicant become a participant of PPRCN.
For further information refer to the "***PPRCN CCNC-Joint Position Statement***."

10.6 STATE OF COLORADO MEMBERSHIP FEES

In 2022 the CCNC General Board approved a resolution that absolved all State of Colorado users from paying Membership fees based on the in-kind services provided by the PSCN and other State agencies towards the day to day operations and maintenance of the Statewide DTRS

10.7 MONTHLY WINDOWS RESTART OF ATTACHED WORKSTATIONS AND ASSOCIATED HARDWARE

10.7.1 DEFINITIONS:

Connected devices are defined as:

Console equipment: Workstations commonly referred to as consoles which include a windows central processing unit (CPU), monitor, voice processing module (VPM) and may include speakers, footswitch, microphone, headset, and other accessories.

Logging recorder devices: Are computer devices provided through local purchase from various vendors for the purpose of digital recording of radio traffic, such recordings often stored and used as evidence or historical reference.

AIS: Archiving Interface Server workstations, commonly referred to as an AIS, are used to interconnect logging recorders, Computer aided dispatch (CAD) or other applications to the radio network.

CAM Server: Console Alias Manager (CAM) is a Windows workstation that allows for local management of Unit IDs and Aliases.

Console Proxy Server: An Application that converts audio packets inside the radio network to be sent outside the radio network to an MCC 7500E Dispatch console.

NM Clients: Network Management Clients (NM Clients) consist of a windows workstation with Motorola software that allows the user to perform functions and request information based upon selected permissions associated with that users login credentials.

First half of the month: Is the 1st day of every month through the 15th day of every month.

Second half of the month: Is the 16th day of every month through the last day of every month.

DTRS: Digital Trunked Radio System. For the purpose of this document we are referring to all the zones and sites interconnected to make up the Statewide Colorado public safety radio system owned by the State of Colorado and local governmental infrastructure owners.

PSCN: Public Safety Communication Network. The designated state division responsible for oversight operations and the installation, operation, and maintenance of the DTRS equipment.

10.7.2 Description:

Due to the potential risk and related severity of a breach of security of the Public Safety Radio infrastructure, it is mandatory that the most current "MOTO Patches" be pushed out through the network by the DTR System Engineers on a monthly basis, between the first day of every month and through the fifteenth day of every month. In order for all of the above defined hardware attached to the DTR System, such as workstations, logging recorder devices, console equipment, AIS and other windows operating subsystems be in a ready state to accept, install and implement the monthly patches, all defined devices shall be restarted monthly between the 16th day of every month and the last day of every month. The restart of the Windows operating system, not just the Motorola applications, shall be accomplished by closing applications and then choosing the 'Restart' option from the power options on the menu.

If a breach of network security caused by a malicious virus, mal-ware, trojan, bot, or any other network security breach is traced to a device not in compliance with this Section 10.7, the device will be immediately disabled from the system and all costs related to any interruption in delivery of public safety communications to any CCNC member agency, all damages, and full costs of recovery of the public safety communications network will be borne by the violating agency.

The following steps and procedures are instituted for agency users who fail or repeatedly fail to restart the appropriate hardware between the 16th day of every month and the last day of every month, posing a threat and risk to the public safety communications system. Posting any known vulnerability on a public facing website is prohibited.

10.7.3 First Offense:

Defined as failure to restart each and every connected device between the 16th day and the last day of every month. Any device listed as not ready to accept and install the monthly patch to the DTR System Engineer pushing out the Motorola patches will be force restarted without prior notification to the agency. There is no assurance that the device will restart normally following the forced restart, and there is no liability should the device fail to restart. There will be an effort to avoid disabling an entire dispatch center. The DTR System Engineer providing the Monthly System Report during the CCNC Technical/Operations meeting will provide a list of the violating agencies not restarting during the previous 30-day period. The CCNC Regional Executive Board member for each region will receive a list of violating agencies within their region from the Administrative Assistant. The CCNC Regional Directors will make contact with each agency or department failing to comply with this policy. The Regional Directors will discuss this policy and agency responsibilities to comply with the restarting policy. Once the agency informs the Regional Director of their changed method of meeting compliance by restarting the associated devices, the Regional Director will notify the DTR System Engineer that the violating agency has been notified and offered evidence of internal policy to achieve and maintain compliance.

10.7.4 Second Offense:

Defined as failure to restart each and every connected device between the 16th day and the last day of every month, regardless if a consecutive or recurring monthly violation, further defined as a second violation within a 12-month period. The second offense will be handled in the same manner as the first offense for forced restarting, reported to the CCNC by the DTR System Engineer providing the Monthly System Report at the CCNC Technical/Operations meeting. The violating agency head (Sheriff, Police Chief, Fire Chief, Mayor, 9-1-1 Authority, Comm Board, etc.) will receive a letter from the CCNC President requiring a two-week written response detailing the process and steps the agency will institute to ensure their hardware does not become a three-time violator. The letter will recommend they discuss any questions they have with any of the CCNC Regional Directors or the DTR System Engineer. The agency head will be required to notify the appropriate Executive Board Regional Director when the corrective actions have been implemented. The DTR System Engineer will be notified by the Regional Director when the agency has provided the appropriate notice of corrective action. The letter will include a reminder of the consequences for a third violation.

10.7.5 Third Offense: Defined as failure to restart each and every connected device between the 16th day and the last day of every month, regardless if a consecutive or recurring monthly violation, further defined as a third offense within a 12-month period. In order to protect the integrity of the public safety communications network, the device or devices will be force restarted by the DTR System Engineer. The third violation will be reported to the CCNC Officers by the DTR System Engineer. It shall be the responsibility of the CCNC Officers and/or Regional Directors to make reasonable attempts via all methods of contact available to contact the violating agency department head or command level staff. The agency director, department head or command level staff will be required to attend, either in person or virtually, a meeting with the CCNC Executive Board and the DTR System Engineer, arranged by the CCNC. The meeting shall address the nature of risk and threat to the public safety communications network and the severity of the agency lack of response to the network security policies. The meeting may include discussion surrounding the agency's desire, or lack thereof, to remain fully committed as an integrated agency with connectivity to the network core. The agency will be granted a period of five business days to provide documentation defining local policy and procedures for restarting all devices connected to the DTR System. Upon receipt of the agency policy and procedures, the CCNC Executive Board and the DTRS Engineer shall review for document approval and acceptance. A follow up meeting

may be requested with the agency director, department head or command level staff to assess the successful implementation of the local policy and compliance with this CCNC policy.

Agency failure to acknowledge and comply with the conditions of this Section 10.7.5 may result in extreme sanctions. Those sanctions may include assessed fees related to cost recovery. Cost recovery fees will be calculated on an escalating scale and will be applied to each device not in compliance and per violation. Repetitive violations may result in disabling the network port, thereby disconnecting the device from the network.

10.7.6 Reoccurrences of Offenses:

The offenses of failing to restart attached workstations is intended to be in a 12-month period, not a calendar year. The timeframe for any agency begins with the first offense. Example: If your agency fails to restart your NM Client in January 2022, your 12-month period concludes at the end of December 2022.

10.7.7 Disconnected Equipment:

If any windows workstation is temporarily disconnected from the DTR System by the device owner for any length of time, causing it to miss one or more monthly MOTO patch software update(s), the DTR System Engineer must be notified of the intent to reconnect the equipment. The DTR System Engineer will coordinate with that agency to ensure that the equipment is downloaded with all current software updates and MOTO Patches prior to reconnection in order to protect the network from security breaches.

CHAPTER 11 ELIGIBLE USERS

The Statewide DTR System offers membership to public safety and public service users from State, Tribal, County, and Local governments; federal agencies; special districts; and EMS providers. Users must be eligible under Title 47 of the Code of Federal Regulations (CFR) Part 90 Private Land Mobile Radio Services §90.20 Public Safety Pool.

11.1 PRIVATE AMBULANCE SERVICES

Private ambulance companies that request access to the Statewide DTR System may be granted talkgroup privileges as an Associate Member as determined by their contractual agreements to governmental agencies. LICENSED PRIVATE AMBULANCE SERVICES are those licensed by a county to operate an ambulance service. LICENSED PRIVATE AMBULANCE SERVICES UNDER CONTRACT are those licensed by a county to operate an ambulance service and under contract to a governmental agency to provide ambulance services for that agency. Private ambulance talkgroup privileges are identified as follows:

11.2 LICENSED PRIVATE AMBULANCE SERVICES

Private ambulance companies granted access to the Statewide DTR System shall not be assigned talkgroups dedicated to the ambulance company, and furthermore shall not conduct private business communications on any DTR system talkgroup. They must have the Channels and Talkgroups programmed into their subscribers as listed in Chapters 12.1.1 and 12.1.2.

11.3 LICENSED PRIVATE AMBULANCE SERVICES UNDER CONTRACT

Private ambulance companies under contract, granted access to the Statewide DTR System shall have the Channels and Talkgroups programmed into their subscribers as listed in Chapters 12.1.1 and 12.1.3.

11.4 PRIVATELY OWNED RADIOS

Private owners of radios wishing to operate on the Colorado Statewide Digital Trunked Radio System must be:

- *An active staff member of a CCNC User Agency,*
- *Must agree to either the "**COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM PARTICIPANT AGREEMENT**", or the "**COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM PARTICIPANT AGREEMENT FOR TRIBAL AGENCIES**" whichever applies, must have a signed letter from their CCNC User Agency stating that the CCNC User Agency assumes the responsibility for the individual's operation of the radio,*
- *Must agree to and sign the "**COLORADO STATEWIDE DIGITAL TRUNKED RADIO SYSTEM PRIVATE RADIO USER AGREEMENT**".*
- *Must agree to allow the radio to be programmed with a secure System Key and to be "Write Protected."*
- The use of a secure System Key could cause the radio to always require a secure

System Key for further programming.

If CCNC approves the request, the CCNC User Agency letter shall be presented to the authorized programming agency and to the DTRMC. The user shall only operate the radio in accordance with Title 47 of the Code of Federal Regulations (CFR Title 47), particularly Part 90 Private Land Mobile Radio Services, CCNC P&Ps and the User Agency's SOPs as well as the applicable "***COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM PARTICIPANT AGREEMENT***" , or "***COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM PARTICIPANT AGREEMENT FOR TRIBAL AGENCIES***" .

CCNC requires the use of a secure System Key; this could cause the radio to always require a secure System Key for further programming. CCNC will not be responsible for any cost associated with removing a requirement for use of a secure System Key or write protection. The User will be responsible for any upgrades required to keep up to date with the operating firmware/software version of the Colorado Statewide Digital Trunked Radio System.

CCNC has the right to inhibit the radio should it be in the best interest of CCNC, the Colorado Statewide Digital Trunked Radio System, or its members. Should the radio be inhibited by CCNC, CCNC will be responsible for deprogramming, uninhibiting, and removing the radio from the System Database when the radio is presented to CCNC by the user.

11.5 MEDIA ACCESS

The modern media and the citizens they serve are accustomed to timely, sometimes immediate access to information regarding police or fire emergencies. In the past, news agencies have been able to gather information by scanning police and fire frequencies, and dispatching reporters to incidents that they feel are of concern to the public. This policy is applicable to Media agencies using system subscriber units for monitoring. This does not apply to commercial scanner equipment. Participating user agencies wishing to provide media monitoring access to any of their talkgroups should provide a letter of permission to CCNC.

The media outlet would purchase the equipment, and would also be responsible for all costs relating to the necessary modifications and programming. Only those technicians designated by the CCNC Technical Committee would do such modifications and programming. Maintenance of any equipment will be the media outlet's responsibility. The media outlet would contract for such work through their representative.

Any media outlet wishing to monitor radio traffic of an agency, which is a member of the 700/800 MHz Statewide DTR system, would have to submit their request to the CCNC Executive board. All requests for permission shall be in writing signed by a senior level official from the agency requesting permission.

Requests should be sent to:
CCNC Executive Board
40 West Littleton Blvd.
Suite 210-129
Littleton, CO 80120

The request should contain the information:

- Name, address, E-mail and telephone number
- Specific agencies to be monitored
- Quantity and type of subscribers requested (Base, Mobile, Airborne or Portable) Purpose for monitoring
- Users of the equipment

If an agency has no media access permission on file, the Executive board will contact the agency whose talkgroups are being requested to approve the request. Once the agency has approved or denied the request, the requesting media outlet will be contacted with the status of their request. If the request is approved, CCNC will provide an agreement form to be completed by the requesting agency. Once the form is completed and returned, CCNC will provide information on how and where to get the equipment programmed. The maximum number of subscriber units authorized to a single media outlet will be non-affiliated and restricted to a quantity of two. All radios, upon request by the State Telecommunications Director, CCNC Executive Board or designee, are subject to inspection immediately upon demand. Decisions of the CCNC Executive board are final. Radios modified or used not in compliance of this policy can result in confiscation and civil and/or criminal actions.

CHAPTER 12 APPLICATIONS FOR MEMBERSHIP

MEMBERS OF PPCRN MUST FIRST COORDINATE APPLICATIONS WITH PPCRN DIRECTOR PRIOR TO APPLYING TO CCNC.

Users wishing to participate in the Consolidated Communications Network of Colorado, Inc. (CCNC)/ Colorado Statewide Digital Trunked Radio System should complete the "***COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM INITIAL PARTICIPATION APPLICATION***" and either the "***COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM PARTICIPANT AGREEMENT***" or the "***COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM PARTICIPANT AGREEMENT FOR TRIBAL AGENCIES***". Each agency must apply individually and not on another's behalf. Example: The County dispatch center applies on its behalf and the agencies they dispatch for. Each agency must complete the Initial Participation Application and apply individually.

12.1 SUBMITTAL PROCESS

Applications and Participation Agreements need to be submitted together. If each is not received together, the application cannot be processed or acted upon until all documentation is received and complete. Applications and Participation Agreements may be obtained from the ***CCNC Website.***

Mail: Consolidated Communications Network of Colorado, Inc.
40 West Littleton Blvd, Suite 210-129
Littleton, CO. 80120

Once the application packet is received by CCNC, the Administrative Assistant will enter it into a spreadsheet before being forwarded to the Regional Executive Director who passes the application to his/her region's designee for processing. Hand delivered applications at the Technical Operations meeting will not be acted on until the application is processed by the Administrative Assistant.

An Application Review Working Group (ARWG), which is comprised of ten (10) members, will consist of the eight Regional Executive Director's appointees within CCNC with foundational understanding of the DTRS. There is a minimum of two State of Colorado PSCN representatives. One should be a DTRS System Engineer familiar with daily system operations and associated with statistical data that can be drawn from the system's database. The other PSCN representative should be associated with the State Monitoring Center to verify the naming and make the necessary alterations.

The CCNC Technical Chair will present the application at the Technical Operations meeting where it will be voted on. The Technical Committee will make a recommendation to the CCNC Executive Committee for final approval. The applicant is required to attend, or have a member of the applying agency attend, the technical committee meeting(s), as well as the monthly Board Meetings.

If there are errors and/or questions concerning the documentation during the evaluation by the ARWG, the application will be placed in a pending status at the Technical Committee level until a resolution to the issues has been determined.

If the Technical Committee recommends approval of the application, the application shall be forwarded to the Executive Board of Directors who may approve the application. If the CCNC Executive Board of

Directors does not approve the application, the application shall be placed into a pending status where it will be reopened for review upon availability of frequencies, or resolution of the reason for denial.

If an unfavorable recommendation is made, the Technical Committee will notify the applicant as to the reason(s). Any pending applications will be reviewed quarterly for changes that would modify the applicant's status.

Once approved, the applicant will coordinate with the State of Colorado and an authorized programming agency or vendor to coordinate a template build. The applicant is encouraged to begin attending monthly CCNC meetings and may participate in committee meetings they are interested in.

12.2 ACCEPTANCE OF NEW USERS

New Users will be classified as User Agencies if their primary source of communications will be the Statewide DTR System or as an Associate Member if your system usage is for Interoperability with User Agencies or Mutual Aid Communications only.

To ensure compliance with CCNC rules and by-laws and to properly coordinate Subscriber ID and talkgroup assignments on the Statewide DTR System, the CCNC Technical Committee will coordinate these assignments for the initial integration of the agency. This will include agency specific talkgroups as well as standard Mutual Aid talkgroups that are available. Any additional outside agency's talkgroup requests must have written authorization from that agency.

Upon receiving the talkgroup assignments, subscriber profiles and authorizations, contact an agency authorized to program subscribers for the CCNC. The agency will need to discuss the talkgroup/channel layout for their subscribers and the available features and functions to be included in their programming template. The type and model of the subscribers will also need to be provided.

A schedule to program and activate the agencies subscribers can then be established. Programming Agencies shall contact the State of Colorado Governor's Office of Information Technology to have the subscriber IDs activated in the proper Zone Controller. Subscriber ID's will only be activated if CCNC has received and approved the agency's User Application and the Participation Agreement.

CHAPTER 13 CURRENT USER MODIFICATIONS

Current User Agencies desiring to modify their agency talkgroup allocations and/or subscriber counts beyond their original approved counts must submit an additional ***"COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM UPDATE PARTICIPATION APPLICATION"*** describing the desired additions. The Application will be reviewed with the same process as a new application described in chapters 10.1and 10.2.

Modifications to agency talkgroup names or the transfer of ownership of talkgroups will be presented to the CCNC Technical Committee as an informational item to keep all records and databases up to date. Any agency that changes the names of their allocated talkgroups is required to notify all agencies that it has shared those talkgroups with of the modified names and the effective date of the change.

CHAPTER 14 TALKGROUP/CHANNEL USAGE

Talkgroups are assigned to member agencies on an as needed basis. All Agencies requesting talkgroups complete a Participation Application showing the justification for the desired talkgroups and Mail/Deliver the original to CCNC. The CCNC Technical Committee will review the request using the Application Process as described in CHAPTER 10.

Every effort should be made to label talkgroups/channels with the same name as used by the talkgroup owner. In the case of Mutual Aid Channels, CCNC has adopted the use of ***the APCO- NPSTC-ANSI-104-1 standard*** for naming conventions. Where CCNC has created Mutual Aid Talkgroups/Channels that are not part of the NPSTC naming convention, the names as listed in these P&Ps shall be used.

14.1 REQUIRED CHANNELS AND TALKGROUPS

CCNC requires specific talkgroup/channels to be programmed into all subscribers. CCNC also strongly recommends the inclusion of additional talkgroup/channels as determined by the type of user agency and the constraints of the subscriber equipment.

14.1.1 ALL SUBSCRIBERS

All voice subscriber units excluding Public Safety Communications Dispatch Center Base Stations, granted transmission access to the Statewide DTR System are required to include the following channels and talkgroups in their subscriber templates:

The National Interoperability Channels (7CALL and 8CALL, and 7TAC and 8TAC) may be available for repeater operation, as well as simplex communications using the DIRECT mode of operation (example 800CALL90D) where transmit and receive are the same frequency (RX). The Statewide Interoperability Channel (STAC). This channel is available for temporary mobile repeater operation (STAC) as well as for simplex communications (STACD). The Regional Mutual Aid Channels for the CCNC region they operate in i.e. MAC 1 MET – MAC 4 MET, MAC 5 NE – MAC 8 NE, MAC9 SE _ MAC 12 SE, MAC 13 SW – MAC 16SW, or MAC 17 NW – MAC 20 NW. The Statewide Mutual Aid Channel CO MAC 21. 700 MHz National Interoperability Channels as required by the F.C.C Region 7 – Colorado 700 MHz Regional Plan if your radio is programmed to operate on 700 MHz frequencies. The required 700 MHz interoperability channels are also listed in chapter 13.7.

Recommended Channels:

The following talkgroups are strongly recommended for all subscribers if space is available. The Mutual Aid Calling Channels for the other CCNC Mutual Aid Regions (the first MAC for each region).

Regional Interoperability Channel (RIC) talkgroups for the All Hazards Regions that the subscriber operates in i.e., North Central All Hazards Region may include the North Central All Hazards Region RICs (Network First Talkgroups). Southwest All Hazards Region may include SW RIC A through SW RIC D talkgroups. South Central All Hazards Region may include SCR, CMD, SCR LAW, SCR FIRE and SCR EMS talkgroups.

14.1.2 LICENSED PRIVATE AMBULANCE SERVICES REQUIREMENTS

Private ambulance companies granted access to the Statewide DTR System shall not be assigned talkgroups dedicated to the ambulance company, and furthermore shall not conduct private ambulance company business communications on any DTRS talkgroup. They must have the following Channels and Talkgroups programmed into their subscribers for interoperable communications with public safety responders: (Refer to the Section CHAPTER 13 for appropriate MAC channel use). The Channels and Talkgroups required for all subscribers of the Statewide DTR System as listed in Section 12.1.

- The Statewide EMS Mutual Aid Channel (EMSMAC)
- The Statewide Hospital Emergency Room Mutual Aid Channel (ERMAC)
- The Mutual Aid Calling Channels for the other CCNC Mutual Aid Regions (the first MAC for each region) are not required but are strongly recommended to be programmed into all subscribers for interoperable communications
- The Hospital Talkgroups may be included with approval from the State of Colorado, Electronic Engineer/EMS Telecommunications Liaison, (303) 692-2536.
- The Regional Emergency Medical and Trauma Advisory Council Mutual Aid (RETAC) Regional Talkgroups may be included.
- The Applicable County Health Department (CHD) Talkgroups may be included.
- The Statewide Simplex Channels (SMPX1 through SMPX5) may be included.
- Regional Interoperability Channels (RIC) Talkgroups may be included for the All Hazards Regions that the Ambulance operates in i.e. North Central All Hazards Region ambulances should include the following RICs; Gold 1, Gold 2, RED NE, RED NW, RED SE, and RED SW, GREEN 1 and GREEN 2, the inclusion of the remaining North Central All Hazards Region RICs are also authorized and recommended additions.
- Ambulances should include Regional RIC's for their primary area of service.

14.1.3 LICENSED PRIVATE AMBULANCE SERVICE UNDER CONTRACT REQUIREMENTS

Private ambulance companies under contract, granted access to the Statewide DTR System shall have the following Channels and Talkgroups programmed into their subscribers for interoperable communications with public safety responders: (Refer to the CHAPTER 13 for appropriate MAC channel use). The Channels and Talkgroups required for all subscribers of the Statewide DTR System as listed in Section 12.1. The Channels and Talkgroups as listed in Section 12.1.2, "Licensed Private Ambulance Services". Talkgroups assigned to the agency it is under contract with as identified by the contracting agency.

14.1.4 PUBLIC SAFETY COMMUNICATIONS DISPATCH CENTERS

Public Safety Communications Dispatch Centers base station radios should be programmed with as many of the appropriate interoperability and mutual aid channels as the Center can accommodate.

All Public Safety Communications Dispatch Centers with direct connection to a Master Zone Controller shall have access to and monitor the first MAC talkgroup in their region. It is also desirable for Public Safety Communications Centers to monitor their regional Com to Com (NET) Talkgroup. While this is preferred, it is understood each agencies primary talkgroups will take precedence over mutual aid communication. CCNC recognizes the resource limitations that Public Safety Communications Dispatch Centers are faced with, but still recommend that they have access to as many MAC channels and the National Interoperability Channels as feasible.

14.2 AGENCY TALKGROUP SHARING

Agencies are encouraged to share their talkgroups with those agencies within their dispatch jurisdiction that they commonly interoperate with. You must receive and keep on file written authorization from the talkgroup's agency before programming subscribers with any talkgroup other than your own. A copy of the authorization letter must be presented to the subscriber programming agency and will be required upon requesting talkgroup programming codes from the WEBDTR.

CHAPTER 15 MUTUAL AID COMMUNICATION

Use of an Incident Command System compliant with the National Incident Management System (NIMS) is required for use of any interoperability resource. All Communications shall be in plain language. Encryption is not allowed on the CCNC Mutual Aid Channels!

Radio codes, acronyms and abbreviations are to be avoided as they may cause confusion between agencies. Requests for assistance or backup should clarify the reason for the request. Agency name shall precede unit identifier, i.e., CSP 6A.

15.1 HIERARCHY

The lowest common mutual aid talkgroup should always be utilized. The mutual aid talkgroups are ranked from lowest to highest as follows:

- *Individual User Agency and local mutual aid talkgroup, Countywide Mutual Aid talkgroups,*
- *Regional Interoperability talkgroups (RICs)*
- *Regional Mutual Aid talkgroups, (MACs, RETACS) Statewide Mutual Aid talkgroups.*

Finally, the use of STAC and the National Interoperability channels (7CALL and 8CALL, 7TAC and 8TAC) should be used if and where available. In the case of a large-scale multi-agency incident when NIMS has been activated and the Communications Unit Leader determines that communication resources beyond those assigned to the region are required, resources from other regions may be coordinated for use by notifying the CSP Dispatch center in that region or by contacting the DTRS Program Manager.

15.1.1 PUBLIC SAFETY COMMUNICATIONS DISPATCH CENTER RESPONSIBILITIES

The Public Safety Communications Dispatch Center of the Agency initiating the incident is responsible for all primary dispatch tasks unless the decision is made by the Incident Commander or the Incident Dispatch Center to transfer the responsibilities to another Center. The Incident Dispatch Center is responsible for audio patching of talkgroups and relaying pertinent information including; who is involved; which talkgroups are patched; and who is in command.

15.1.1.1 PUBLIC SAFETY COMMUNICATIONS DISPATCH CENTER (COM TO COM) TALKGROUPS

Five regional talkgroups have been established to provide direct communication between communication centers and mobile command vehicles to effectively supply necessary information for any public safety situation that arises for the safety and welfare of the citizens of the State of Colorado. The talkgroup will only be placed on Public Safety Communications Dispatch positions or mobile dispatch/command vehicles. These talkgroups are configured as “Fast Start” talkgroups in the Zone Controller; therefore, subscriber units in mobile command vehicles or non-connected Public Safety Communications Dispatch positions will only receive audio for these talkgroups if resources are available for their site affiliation. The Talkgroups are identified as:

- *Metro Net - Includes Adams, Arapahoe, Boulder, Broomfield, Clear Creek, Denver, Douglas, Elbert, Gilpin, and Jefferson counties.*

- *NE Net - Includes Cheyenne, Kit Carson, Larimer, Lincoln, Logan, Morgan, Phillips, Sedgwick, Washington, Weld, and Yuma counties.*

- *SE Net - Includes Baca, Bent, Chaffee, Crowley, Custer, El Paso, Fremont, Huerfano, Kiowa, Lake, Las Animas, Otero, Park, Powers, Pueblo, and Teller counties.*

- *NW Net - Includes Eagle, Garfield, Grand, Jackson, Mesa, Moffat, Pitkin, Rio Blanco, Routt and Summit counties.*

- *SW Net - Includes Alamosa, Archuleta, Conejos, Costilla, Delores, Delta, Gunnison, Hinsdale, La Plata, Mineral, Montezuma, Montrose, Ouray, Rio Grande, Saguache, San Juan, and San Miguel counties.*

The agencies contained in each regional group will be responsible for the recording of any interchange on their talkgroup.

To call within the same region use the agency name and talkgroup identification. Always state the called agency first. Example: "Douglas from Arapahoe on Metro Net." To call outside of your talkgroup region, go to that agency's regional talkgroup using the agency name and talkgroup identifier.

15.1.1.2 AUDIO PATCHING

Audio Patching is most effective for patching like resources, i.e., conventional resource to conventional resource, 700/800 MHz talkgroups to 700/800 MHz talkgroups. CCNC does not recommend patching conventional UHF or VHF channels to 700/800 MHz talkgroups as conventional users do not hear trunking system status tones, may start their voice traffic before trunking voice channels are granted and therefore are not guaranteed their transmission has been sent.

Audio Patches have a risk factor for adversely affecting trunked radio system operations. If temporary audio patches are required to the Statewide DTR System, it is highly recommended that the personnel implementing the Audio Patch be trained in the operational techniques necessary for proper patch communications. Audio patches shall be removed as soon as the need for the patch has ended.

One example of an approved temporary patch is SchoolSAFE: It is specific to a location and deployed with specialized equipment to interface with Statewide DTR System. A patch using SchoolSAFE is typically under the control of a local PSAP of the agency responding and is activated as directed by Incident Commander. The patch is dropped as soon as a response has concluded.

No Permanent Audio Patches shall be implemented on the Statewide DTR System without a recommendation from the CCNC Technical Committee and approval from the CCNC Executive board. If an Agency desires to have a permanent or even a reoccurring Audio Patch, they need to contact their representative on the CCNC Executive Board.

The CCNC Technical Committee will review the request at the next scheduled meeting and make a recommendation to the CCNC Executive Board. If the CCNC Technical Committee recommends approval of the application, the application shall be forwarded to the Executive Board of Directors who may approve the application. If the Executive Board of Directors does not approve the application, the

CCNC Technical Committee will notify the applicant as to the reason(s) for the denial.

15.1.2 CCNC COUNTY MUTUAL AID/EMERGENCY TALKGROUPS

Each county is assigned a specific County Mutual Aid/Emergency Talkgroup (County MAC) for intra-county communication activity including but not limited to:

- *Activities and uses for the direct benefit of a county's public safety agencies to include (not limited to) EOC/EOP operations, training, simulations, and travel.*

- *School Districts and their public transportation vehicles for communication to an emergency communications center; or in support of school district transportation resources utilized by public safety personnel during an emergency event.*

All County MAC talkgroups are intended for the utilization by a county and/or intra-county communication activity, and are not to be utilized in lieu of an agency(s) establishment of participation in the CCNC, or to serve as a primary channel for an entity.

The Primary PSAP in the county with the annual largest call volume shall be the agency authorized to provide written authorization for non-county agencies to have the County Mac programmed in their subscriber units. Refer to section 12.2.

County MACs that have been shared with surrounding counties may also be used for inter-county mutual aid responses with coordination from the PSAP handling the incident.

CCNC, its Operations committee may request that the System Administrator suspend use of the talkgroup; if any individual, agency, or organization is improperly using the County MAC talkgroup.

15.1.3 REGIONAL INTEROPERABILITY CHANNEL (RIC) TALKGROUPS

Each All Hazards Region may request RIC Talkgroups to be utilized for interoperable communications within their All Hazards Region by following the process in Section CHAPTER 13 Current User Modifications Each region may also request specialized talkgroups for encrypted communications. These could be assigned to SWAT, HAZMAT, Task Forces, or other specialized disciplines. The region requesting the encrypted talkgroup will be responsible for managing the encryption keys for that talkgroup but will follow the procedure in section 13.2, ENCRYPTION, for determining the Encryption Key ID.

15.1.3.1 NORTH CENTRAL ALL HAZARDS REGION INTEROPERABILITY TALKGROUPS –ISSI

The following talkgroups have been set aside specifically for use by agencies that are a part of the North Central All-Hazards Region. These talkgroups interconnect users from various systems (i.e., VHF, UHF, 800 MHz, etc.) for interoperability among various disciplines. These talkgroups are only to be used within the ten (10) county (Adams, Arapahoe, Boulder, Broomfield, Clear Creek, Denver, Douglas, Elbert, Gilpin and Jefferson) North Central All Hazards Region.

With this interconnectivity, there are some special operational caveats that users need to be aware of:

- These Talkgroups cannot be patched to each other or any other talkgroups from a console,

ACU-1000 or similar device. Radio coverage is limited to the users "Home" system coverage area. These talkgroups will not extend your normal radio coverage. There will be a noticeable delay in the radio transmission between systems. Avoid speaking immediately after pressing the push to talk button. An extra few seconds should be allowed before speaking. Not all Communications Centers will routinely monitor these talkgroups. DTR Communications Centers that are hard wire connected to a Zone Controller console port are required to monitor Metro Net.

- Trunking control features and indicators (i.e., talk permit tone) are not passed between disparate systems. These talkgroups are to be used for inter-agency and inter-discipline use as a means of direct communications. It is recommended that these talkgroups be programmed into subscriber units along with the appropriate MAC channels wherever possible with the exception of Metro Net.

The talkgroup descriptions and allocations are recommended for operational use; however individual events will govern the actual assignment and usage of any interoperability channel.

For **Day-to-Day Usage** follow the defined descriptions as listed in Talkgroup/channel Descriptions below. For **Incident Command Usage** the talkgroups channels will be assigned by the Incident Commander following the priorities listed in the Incident Response/Usage Section following the Talkgroup/channel descriptions. The North Central All Hazards Region has been divided into four quadrants, using Interstate 70 (I70) as the North and South dividing line and Interstate 25 (I25) as the East and West dividing line.

Procedures for establishing communications connectivity include the following:

- *Utilize your agency's internal procedures for establishing connectivity between the agencies. Verify operation of the ISSI resource by conducting radio checks between participating dissimilar radio systems, (i.e. Macom system radio to VHF radio and/or UHF Radio and/or DTR System Radio).*

- *The ISSI resource should be checked for activity prior to use; either by the dispatcher or Scene Commander.*

- *Users should identify themselves on the interoperability channel using their agency name and unit identifier (e.g., Boulder PD 125, North Washington Engine 32, etc.).*

15.1.2 NORTH CENTRAL REGION TALKGROUPS

The following talkgroups have been set aside specifically for use by agencies that are a part of the north Central All-Hazards Region. These talkgroups interconnect users from various systems (i.e., VHF, UHF, 800 MHz, etc.) for interoperability among various disciplines.

Currently, users of the following systems are interconnected:

- *Harris/P25 users*
- *Colorado DTR (CCNC) users*

- *FRCC (Adams, Wells Counties)*
- *City of Aurora*
- *Boulder Conventional VHF users*
- *Federal Government Agencies (FBI, US Marshals)*

The area has been divided into four quadrants, using Interstate 70 (I-70) as the North and South dividing line and Interstate 25 (I-25) as the east and west dividing line. The talkgroup descriptions and allocations are recommended for operational use; however individual events will govern the actual assignment and usage of any interoperability channel. With this interconnectivity, there are some special operational caveats that users need to be aware of;

- *These Talkgroups cannot be patched to each other from a console, ACU-1000 or similar device.*
- *Radio Coverage is limited to the "Home" system coverage area*.
- *There will be a delay in the radio transmission between systems. Avoid speaking quickly after pressing the push to talk button. An extra few seconds should be allowed before speaking.*
- *Not all Communications Centers (other than METRO NET) will routinely monitor these talk groups.*
- *Trunking control features and indicators (i.e., talk permit tone) are not passed between disparate systems.*

Procedures for establishing communications connectivity include:

- *Selection of a channel or talkgroup on your home system if necessary*.
- *As with any other Interoperability Talkgroup, the INTEROP channel should be checked for activity prior to use; either by the dispatcher or field personnel. This must be done prior to coordination of any movement to the intended talkgroup. For planned or scheduled incident, operations, training or events coordinate the use of the ISSI talk groups through the DTRS Program Manager at 720-402-0858 or the Denver Electronic Engineering Bureau at phone: 720-865-0062*
- *Verifying system-wide availability of required resources – coordination among control point dispatchers.*
- *Providing radio call sign/designator information to connected agencies as needed.*
- *Assigning the requested unit/agency to that channel or talkgroup.*

- *Utilizing your agency's internal procedures for establishing connectivity between the agencies.*
- *Announcing to users that interoperability is activated.*
- *Users should identify themselves on the interoperability channel using their agency name and unit identifier (e.g., Boulder 125, etc.).*
- *The dispatcher for the jurisdiction where the event is being worked shall monitor the interoperability channel to address requests.*

These talkgroups are to be used for inter-agency and inter-discipline use as a means of direct communications. It is recommended that these talkgroups be programmed into subscriber units along with the appropriate MAC channels wherever possible. These talkgroups shall not be used by a single agency for operation needs, or to expend agency coverage needs outside the parameters of the agency home system.

GOLD 1: This talkgroup has been established for interoperability for Command and Control between agencies within the North Central Region. This also has been designated the contact channel for users.

SILVER: This talkgroup has been established for interoperability between Denver, Auraria, Glendale and the State.

GRAY: This talkgroup has been established for interoperability between Federal agencies and agencies within the North Central Region.

BLUE NE: This talkgroup has been established for interoperability between Law Enforcement Agencies within the North Central Region that lay north of I-70 and east of I-25.

BLUE NW: This talkgroup has been established for interoperability between Law Enforcement Agencies within the North Central Region that lay north of I-70 and west of I-25.

BLUE SE: This talkgroup has been established for interoperability between Law Enforcement Agencies within the North Central Region that lay south of I-70 and east of I-25

BLUE SW: This talkgroup has been established for interoperability between Law Enforcement Agencies within the North Central Region that lay south of I-70 and west of I-25.

RED NE: This talkgroup has been established for interoperability between Fire Agencies within the North Central Region that lay north of I-70 and east of I-25.

RED NW: This talkgroup has been established for interoperability between Fire Agencies within the North Central Region that lay north of I-70 and west of I-25.

RED SE: This talkgroup has been established for interoperability between Fire Agencies within the North Central Region that lay south of I-70 and east of I-25.

RED SW: This talkgroup has been established for interoperability between Fire Agencies within the North Central Region that lay south of I-70 and west of I-25.

GREEN 1: This talkgroup has been established for interoperability between EMS agencies, dispatch, and hospitals

GREEN NE: This talkgroup has been established for interoperability among EMS Agencies within the North Central Region that lay north of I-70 and east of I-25.

GREEN NW: This talkgroup has been established for interoperability among EMS Agencies within the North Central Region that lay north of I-70 and west of I-25.

GREEN SE: This talkgroup has been established for interoperability among EMS Agencies within the North Central Region that lay south of I-70 and east of I-25.

GREEN SW: This talkgroup has been established for interoperability among EMS Agencies within the North Central Region that lay south of I-70 and west of I-25.

METRO NET: In addition to the above talkgroups, the Metro Net talkgroup has been set up for communications center-to-communication center interoperability. It is not intended for this talkgroup to be programmed into field subscriber units, except for mobile dispatch/command vehicles.

Additionally, a CHD NC talkgroup has been established for interoperability between ESF 8 and NCR.

Incident Response/Usage

In response to incidents, which cross over political jurisdictions, there will potentially be competing demands and priorities for interoperable communications assets. Until such time as Incident Command is established, the lead agency designee (i.e., communications supervisor/command personnel), in collusion with their counterparts in other involved agencies, will have the authority to designate the use of interoperable assets. Once Incident Command has been established, Communication Unit Leaders can be contacted for further coordination and delegation of the interoperable communications. When the same resources are requested for two or more incidents, resource assignments should be based on the priority levels below:

- Disaster, large-scale incident or extreme emergency requiring mutual aid or interagency communications
- Incidents where imminent danger exists to life or property
- Incidents requiring the response of multiple agencies
- Pre-planned events requiring mutual aid or interagency communications
- Incidents involving a single agency where supplemental communications are needed for agency use

- Drills, tests and exercises

In the event of multiple simultaneous incidents within the same priority, the resources should be allocated according to the following:

- Incidents with the greatest level of exigency (e.g., greater threat to life or property, more immediate need…) have priority over less exigent incidents.
- Agencies with single/limited interoperable options have priority use of those options over agencies with multiple interoperable options.
- When at all possible, agencies already using an interoperable asset during an event should not be redirected to another resource.

These are interoperability channels in the region that are reserved for intercommunication in situations requiring the coordination of multiple public safety entities.

Examples of Proper Use of the Interoperability Channels:

- As working channels for multiple fire departments fighting a fire together.
- For coordination during a police chase through multiple jurisdictions where agencies have no other communications link with each other
- For Communications during extended joint operations between multiple police agencies such as drug operations, riots, etc.
- For coordination during recover operations after a disaster such as a tornado when local, state, and federal officials require a common communications link.

Examples of Improper Use of the Interoperability Channels:

- To support the administrative functions of a fire department which has a mutual aid agreement with an adjacent fire department to provide “move-up” capability when a fire unit leaves its own coverage area.
- To provide an extra working channel for a public safety agency supporting a special event.
- To provide a surveillance channel for use between members of the same public safety agency.

Other rules of use:

- National Incident Management System – Use of an Incident Command System compliant with the National Incident Management System is required for use of any regional interoperability resource.

- Plain language – All Communications shall be in plain language. Radio codes, acronyms and abbreviations are to be avoided as they may cause confusion between agencies. Requests for assistance or backup should clarify the reason for the requests.

- Unit Identification – Agency name shall precede unit identifier, i.e., operations, logistics, command, information, liaison, i.e., "Denver 211.

Procedures for establishing communications connectivity include:

- Selection of a channel or talkgroup on your home system if necessary

- Verifying system-wide availability of required resources – coordination among control point dispatchers.

- Providing radio call sign/designator information to connected agencies as needed.

- Assigning the requested unit/agency to that channel or talkgroup

- Utilizing your agency's internal procedures for establishing connectivity between the agencies.

15.1.3 REGIONAL RIC'S ARE IDENTIFIED IN CHAPTER 14.1.1 ABOVE

The RIC talkgroups have been set aside specifically for use by agencies that are a part of their respective All-Hazards Region are to be used according to their user policies.

15.1.4 REGIONAL MUTUAL AID CHANNEL (MAC) TALKGROUPS

CCNC has geographically divided the state into five (5) Mutual Aid Communication Areas;

- ***METRO*** *comprised of Adams, Arapahoe, Boulder, Broomfield, Clear Creek, Denver, Douglas, Elbert, Gilpin, and Jefferson counties;*

- ***NORTHEAST*** *comprised of Cheyenne, Kit Carson, Larimer, Lincoln, Logan, Morgan, Phillips, Sedgwick, Washington, Weld, and Yuma counties;*

- ***SOUTHEAST*** *comprised of Baca, Bent, Chaffee, Crowley, Custer, El Paso, Fremont, Huerfano, Kiowa, Lake, Las Animas, Otero, Park, Powers, Pueblo, and Teller counties;*

- ***SOUTHWEST*** *comprised of Alamosa, Archuleta, Conejos, Costilla, Delores, Delta, Gunnison, Hinsdale, La Plata, Mineral, Montezuma, Montrose, Ouray, Rio Grande, Saguache, San Juan, and San Miguel counties;*

- ***NORTHWEST*** *comprised of Eagle, Garfield, Grand, Jackson, Mesa, Moffat, Pitkin, Rio Blanco, Routt and Summit counties.*

Each MAC Region has four (4) mutual aid talkgroups assigned to the geographic area for multi-agency

coordination. All Regional MAC Talkgroups (MAC 1 through MAC 20) are available for use within their geographic area by all CCNC agencies operating in that area. The following MAC talkgroup descriptions and allocations are recommended for operational usage. However, individual events will govern the actual assignment and usage of any MAC channel within its operating area.

Use of MAC Channels for planned events will be coordinated at a minimum of 72 hours prior an event to allow for notification to CCNC users, when possible and practical. This coordination will be through the DTRS Program Manager or their designee if the primary POC is not available. MAC channels shall not be utilized for reoccurring events where agencies are reluctant to share talkgroup resources.

It is important for all users to understand that MAC talkgroups are non-encrypted and may be scanned by the public on multiple media sources. Operations requiring secure communications should not be conducted on any MAC.

While the following talkgroups have been outlined for use in these regions, not all counties or agencies within those counties are operating on the Statewide DTR System.

The first MAC in each of the five MAC regions shall be monitored by dispatch centers in that MAC region. The first MAC in each region is designated as a calling or hailing channel for units outside their home region to have direct communications with a dispatch center in a region they may be traveling through for purposes of reporting emergencies or to request cover or mutual aide from local agencies.

15.1.4.0 MAC 1 MET THRU MAC 4 MET (METRO)

MAC Talkgroups for use in Adams, Arapahoe, Boulder, Broomfield, Clear Creek, Denver, Douglas, Elbert, Gilpin, and Jefferson counties.

15.1.4.1.1 MAC 1 MET

This talkgroup will be used for regional calling or hailing for the METRO MAC Region. Dispatch centers located in the METRO MAC region shall monitor MAC 1 MET for emergency traffic. The talkgroup will be left in the clear and available for units outside their normal response area and in the METRO MAC Region, to have a direct line of communication with a metro area dispatch center for reporting emergencies or to request assistance, if needed. MAC 1 MET shall not be assigned or utilized for special operations or events, and will not be assigned to preplanned or scheduled operations or events.

15.1.4.1.2 MAC 2 MET

This talkgroup has been initially allocated to Fire Agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.1.3 MAC 3 MET

This talkgroup has been initially allocated to Law Enforcement Agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.1.4 MAC 4 MET

This talkgroup has been initially allocated to EMS Agencies for mutual aid coordination and

communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.2 MAC 5 NE THRU MAC 8 NE (NORTHEAST)

MAC Talkgroups for use in Cheyenne, Kit Carson, Larimer, Lincoln, Logan, Morgan, Phillips, Sedgwick, Washington, Weld, and Yuma counties.

15.1.4.2.1 MAC 5 NE

This talkgroup shall be used for regional calling or hailing for the NE MAC Region. Dispatch centers located in the NE MAC region shall monitor MAC 5 NE for emergency traffic. The talkgroup will be left in the clear and available for units outside their normal response area and in the NE MAC Region, to have a direct line of communications with the NE area dispatch center for reporting emergencies or to request assistance, if needed. MAC 5 NE shall not be assigned or utilized for special operations or events, and will not be assigned to replanned for scheduled operations of events.

15.1.4.2.2 MAC 6 NE

This talkgroup has been initially allocated to Fire agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.2.3 MAC 7 NE

This talkgroup has been initially allocated to Law Enforcement agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.2.4 MAC 8 NE

This talkgroup has been initially allocated to EMS agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4. MAC 9 SE THRU MAC 12 SE (SOUTHEAST)

MAC Talkgroups for use in Baca, Bent, Chaffee, Crowley, Custer, El Paso, Fremont, Huerfano, Kiowa, Lake, Las Animas, Otero, Park, Powers, Pueblo, and Teller counties.

15.1.4.3.1 MAC 9 SE

This talkgroup shall be used for regional calling or hailing for the SE MAC Region. Dispatch centers located in the SE MAC region shall monitor MAC 9 SE for emergency traffic. The talkgroup will be left in the clear and available for units outside their normal response area and in the SE MAC Region, to have a direct line of communications with the NE area dispatch center for reporting emergencies or to request assistance, if needed. MAC 9 SE shall not be assigned or utilized for special operations or events, and will not be assigned to replanned for scheduled operations of events.

15.1.4.3.2 MAC 10 SE

This talkgroup has been initially allocated to Fire agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.3.3 MAC 11 SE

This talkgroup has been initially allocated to Law Enforcement agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.3.4 MAC 12 SE

This talkgroup has been initially allocated to EMS agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.4 MAC 13 SW THRU MAC 16 SW (SOUTHWEST)

MAC Talkgroups for use in Alamosa, Archuleta, Conejos, Costilla, Delores, Delta, Gunnison, Hinsdale, La Plata, Mineral, Montezuma, Montrose, Ouray, Rio Grande, Saguache, San Juan, and San Miguel counties.

15.1.4.4.1 MAC 13 SW

This talkgroup shall be used for regional calling or hailing for the SW MAC Region. Dispatch centers located in the SW MAC region shall monitor MAC 13 SW for emergency traffic. The talkgroup will be left in the clear and available for units outside their normal response area and in the SW MAC Region, to have a direct line of communications with the SW area dispatch center for reporting emergencies or to request assistance, if needed. MAC 13 SW shall not be assigned or utilized for special operations or events, and will not be assigned to replanned for scheduled operations of events.

15.1.4.4.2 MAC 14 SW

This talkgroup has been initially allocated to Fire agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.4.3 MAC 15 SW

This talkgroup has been initially allocated to Law Enforcement agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.4.4 MAC 16 SW

This talkgroup has been initially allocated to EMS agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.5 MAC 17 NW THRU MAC 20 NW (NORTHWEST)

MAC Talkgroups for use in Eagle, Garfield, Grand, Jackson, Mesa, Moffat, Pitkin, Rio Blanco, Routt and Summit counties.

15.1.4.5.1 MAC 17 NW

This talkgroup shall be used for regional calling or hailing for the NW MAC Region. Dispatch centers located in the SW MAC region shall monitor MAC 17 NW for emergency traffic. The talkgroup will be left in the clear and available for units outside their normal response area and in the NW MAC Region, to have a direct line of communications with the SW area dispatch center for reporting emergencies or to

request assistance, if needed. MAC 17 NW shall not be assigned or utilized for special operations or events, and will not be assigned to replanned for scheduled operations of events.

15.1.4.5.2 MAC 18 NW

This talkgroup has been initially allocated to Fire agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.5.3 MAC 19 NW

This talkgroup has been initially allocated to Law Enforcement agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.4.5.4 MAC 20 NW

This talkgroup has been initially allocated to EMS agencies for mutual aid coordination and communications. This MAC may be assigned for interoperability to other incidents, as needed or required.

15.1.5 CO MAC 21 (STATEWIDE)

MAC Talkgroups for use in any county or counties. This talkgroup will be used for intra-state mutual aid coordination and communications. This talkgroup is available for use when no other Mutual Aid Talkgroups are available to meet the communications needs.

15.1.6 REGIONAL EMERGENCY MEDICAL AND TRAUMA ADVISORY COUNCIL (RETAC) REGIONAL MUTUAL AID

The following talkgroups have been assigned for Emergency Medical Services (EMS) mutual aid coordination and communications within the various RETAC regions as assigned throughout Colorado. While the following talkgroups have been outlined for use in these regions, not all counties or agencies within the region are operating on the Statewide DTR System.

15.1.6.1 EMS MH

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Mile-High RETAC Mutual Aid Region: Adams, Arapahoe, Broomfield, Denver, Douglas, and Elbert counties.

15.1.6.2 EMS NE

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Northeastern Colorado RETAC Mutual Aid Region: Jackson, Larimer, Logan, Morgan, Phillips, Sedgwick, Washington, Weld, and Yuma counties.

15.1.6.3 EMS PP

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Plains to Peaks RETAC Mutual Aid Region: Cheyenne, El Paso, Kit Carson, Lincoln, and Teller counties.

15.1.6.4 EMS SE

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Southeast Colorado RETAC Mutual Aid Region: Baca, Bent, Crowley, Kiowa, Otero, and Prowers counties.

15.1.6.5 EMS S

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Southern Colorado RETAC Mutual Aid Region: Custer, Fremont, Huerfano, Las Animas, and Pueblo counties.

15.1.6.6 EMS FH

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Foothills RETAC Mutual Aid Region: Boulder, Clear Creek, Gilpin, Grand, and Jefferson counties.

15.1.6.7 EMS CM

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Central Mountain RETAC Mutual Aid Region: Chaffee, Eagle, Lake, Park, Pitkin, and Summit counties.

15.1.6.8 EMS NW

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Northwest Colorado RETAC Mutual Aid Region: Garfield, Mesa, Moffat, Rio Blanco, and Routt counties.

15.1.6.9 EMS SLV

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the San Luis Valley RETAC Mutual Aid Region: Alamosa, Conejos, Costilla, Mineral, Rio Grande, and Saguache counties.

15.1.6.10 EMS SW

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Southwest RETAC Mutual Aid Region: Archuleta, Dolores, La Plata, Montezuma, and San Juan counties.

15.1.6.11 EMS W

This talkgroup has been initially allocated for EMS mutual aid coordination and communications within the Western RETAC Mutual Aid Region: Delta, Hinsdale, Gunnison, Montrose, Ouray and San Miguel counties.

15.1.6.12 EMS MAC

This talkgroup has been initially allocated for EMS mutual aid coordination and communications Statewide.

15.1.6.13 ER MAC

This talkgroup has been initially allocated to EMS agencies for mutual aid coordination and

communications with Hospital Emergency Departments Statewide.

15.1.7 COUNTY HEALTH DEPARTMENTS

The following talkgroups have been assigned for County Health Departments (CHD) emergency management, mutual aid coordination and communications within the All-Hazards Emergency Management Regions as assigned throughout Colorado. While the following talkgroups have been outlined for use in these regions, not all counties or agencies within the region are operating on the Statewide DTR System.

15.1.7.1 CHD NE

County Health Department Northeast has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the Northeast All-Hazards Emergency Management Region: Cheyenne, Kit Carson, Larimer, Lincoln, Logan, Morgan, Phillips, Sedgwick, Washington, Weld, and Yuma counties.

15.1.7.2 CHD NC

County Health Department North Central has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the North Central All-Hazards Emergency Management Region: Adams, Arapahoe, Boulder, Broomfield, Clear Creek, Denver, Douglas, Elbert, Gilpin and Jefferson counties.

15.1.7.3 CHD SC

County Health Department South Central has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the South-Central All-Hazards Emergency Management Region: Chaffee

15.1.7.4 CHD S

County Health Department South has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the South All-Hazards Emergency Management Region: Custer, Fremont, Huerfano, Las Animas, and Pueblo counties.

15.1.7.5 CHD SE

County Health Department Southeast has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the Southeast All-Hazards Emergency Management Region: Baca, Bent, Crowley, Kiowa, Otero, and Prowers counties.

15.1.7.6 CHD NW

County Health Department Northwest has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the Northwest All-Hazards Emergency Management Region: Eagle, Garfield, Grand, Jackson, Mesa, Moffat, Pitkin, Rio Blanco, Routt and Summit counties.

15.1.7.7 CHD W

County Health Department West has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the West All-Hazards Emergency Management Region: Delta, Gunnison, Hinsdale, Montrose, Ouray, and San Miguel

counties.

15.1.7.8 CHD SW

County Health Department Southwest has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the Southwest All-Hazards Emergency Management Region: Archuleta, Dolores, La Plata, Montezuma, and San Juan Counties.

15.1.7.9 CHD SL

County Health Department San Luis Valley has been initially allocated to County Health Departments (CHD) emergency management, mutual aid coordination and communications within the San Luis Valley All-Hazards Emergency Management Region: Alamosa, Conejos, Costilla, Mineral, Rio Grande, and Saguache counties.

15.1.8 School Bus Talkgroups

The following talkgroups have been assigned for School Bus emergency management, mutual aid coordination and communications within the five (5) regions of the DTRS.

While the following talkgroups have been outlined for use in these regions, not all counties or agencies within the region are operating on the Statewide DTR System.

The following talkgroups are to be used for out-of-region travel by member schools; school districts and other educational facilities when in the course of transporting students to and from school related events and activities outside of their normal area of operations.
(Example: School District XYZ operating in Lamar, Colorado and traveling to Ft. Collins, Colorado would utilize MAC BUS SE for communications back to their district while in the process of transporting students).

Day-to-day transport operations are not authorized on these talkgroups. Excessive and non-activity related communications is prohibited and any violation may result in the offending radio being inhibited. Educational transport vehicles should be equipped with the appropriate equipment for their individual operational area. Only that Bus talkgroup for that region for which the educational facility physically resides will be programmed into mobile/portable equipment. No other Bus talkgroups will be authorized for programming.

- **MAC BUS MET**
  For use within the DTRS Metro Region
  (Adams, Arapahoe, Boulder, Broomfield, Clear Creek, Denver, Douglas, Elbert, Gilpin, Jefferson counties)

- **MAC BUS NE**
  For use within the DTRS Northeast Region
  (Cheyenne, Kit Carson, Larimer, Lincoln, Logan, Morgan, Phillips, Sedgwick, Washington, Weld, Yuma counties)

- **MAC BUS SE**
  For use within the DTRS Southeast Region
  (Baca, Bent, Chaffee, Crowley, Custer, El Paso, Fremont, Huerfano, Kiowa, Lake, Las Animas, Otero, Park, Powers, Pueblo, Teller counties)

- **MAC BUS SW**
  For use within the DTRS Southwest Region
  (Alamosa, Archuleta, Conejos, Costilla, Delores, Delta, Gunnison, Hinsdale, La Plata, Mineral, Montezuma, Montrose, Ouray, Rio Grande, Saguache, San Juan, San Miguel counties)

- **MAC BUS NW**
  For use within the DTRS Northwest Region
  (Eagle, Garfield, Grand, Jackson, Mesa, Moffat, Pitkin, Rio Blanco, Routt, Summit counties

15.2 ENCRYPTION

Encryption is the process of encoding "Plain language" messages into "Secure" messages that are broadcast over the air in a format that is unintelligible to anyone not authorized to receive it. To receive the message information, you must have the proper Encryption Key to decode the message. To use encryption, the radio must be model capable and programmed for encrypted operation.

Encryption may be a software-based option, such as Motorola's "Advanced Digital Privacy" (ADP) or a hardware-based option such as "Data Encryption Standard" (DES), "Advanced Encryption Standard" (AES) or other variations. Encryption can be used on conventional channels or trunked talkgroups unless prohibited by rules and/or regulations. Encryption is not permitted on CCNC Mutual Aid Channels or on Calling Channels such as 8CALL90. Agencies using encryption can only communicate with other encrypted agencies if they have the same type of encryption and the same Encryption Key. The Encryption Key is a parameter used in conjunction with a cryptographic algorithm to encode "Plain language" into "Secure" or to decode "Secure" into "Plain language." The Encryption Key can be changed by the using agency whenever they see the need to change it.

Encryption Keys are identified by a numeric label known as the "Encryption Key ID." The "Encryption Key ID" is used in equipment programming to associate a particular Encryption Key with the proper channels and/or talkgroups. When an "Encryption Key" is changed the "Encryption Key ID" doesn't change. To effectively assign your "Encryption Keys" to the desired channels/talkgroups, each "Encryption Key" must have a unique "Encryption Key ID". The unique "Encryption Key ID" also allows you to share your encrypted functionality with other users that have equipment with the same encryption functionality by sharing only the "Encryption Key ID". The authorized user can program their equipment for encryption using your "Encryption Key ID" and you can load the actual "Encryption Key", keeping the "Encryption Key" secure.

Agencies wishing to use encryption on their talkgroups should contact the DTR Monitoring Center (DTRMC) @ (303) 764-7975 to receive a unique "Encryption Key ID". The DTRMC will need to know:

How many encryption keys your agency will be using, what talkgroups will be encryption capable, what keys will be used for what talkgroups.

The DTRMC does not manage your actual "Encryption Keys", they only assign a range of "Encryption Key IDs" for you to use with your talkgroups. They assign the range of "Encryption Key IDs" to avoid duplication of "Encryption Key IDs" which could cause communications problems for the DTR system or its users.

CCNC recommends that you use an Encryption Key Management Plan such as those outlined by PSWN The DTRMC will assign a "Common Key" for each type of encryption used on the DTR System. Encryption is allowed on the "Five Statewide Simplex Channels" but only in the "Operator Selectable" configuration.

The "Common Key" may be used for interoperable communications on the "Five Statewide Simplex Channels" or other talkgroups that you have in common with other agencies that have the same type of encryption capability. When using encryption in mutual aid situations you should ensure that all the responding agencies are capable of the same type of encryption.

The following Statewide Encrypted channels are available to allow for coordination of resources for a major event with multiple agencies, jurisdictions and or disciplines responding:

- *ADP EC – Statewide encrypted coordination talkgroup using ADP encryption,*
- *DES EC – Statewide encrypted coordination talkgroup using DES encryption,*
- *AES EC– Statewide encrypted coordination talkgroup using AES encryption.*

Any CCNC agency that has the corresponding encryption capability in their subscriber equipment may use the talkgroup for coordination of resources for a major event with multiple agencies, jurisdictions and or disciplines responding:

Encryption is never permitted on the CCNC Mutual Aid Channels!

15.3 TRAVELING BETWEEN MUTUAL AID REGIONS

All users traveling across mutual aid regions including Prisoner/Jail transport vehicles are required to change to an agency defined talkgroup for traveling that does not broadcast their primary dispatch traffic while traveling when leaving their immediate jurisdiction. This is due to system loading considerations. Agencies should avoid broadcasting their dispatch channel around the state in areas that were not designed for the additional talkgroup loading. This includes "monitoring the primary dispatch talkgroup while outside their area of response. This is considered 'talkgroup dragging' and in emergency situations or large events, radios found to be talkgroup dragging may be inhibited.

15.4 HOSPITAL TALKGROUPS

Many Hospitals/Trauma centers throughout the state have been assigned talkgroups (Hospital Talkgroups). Check with the State of Colorado EMS Telecommunications Liaison, (303) 692-2536, for the current listing of hospital talkgroups available for your response area. If in the PPRCN region, contact the PPRCN System Manager for guidance in hospitals in that region.

15.5 STATEWIDE SIMPLEX CHANNELS

Five statewide simplex channels have been assigned for on scene direct radio to radio communications as needed. Channels must use APCO 25 Common Air Interface digital signaling, use a channel spacing of 12.5 KHz, a transmit deviation of 2.5 KHz, be programmed for Network ID 293 and operated at Output power levels of 3 Watts or less. Encryption is allowed on these channels using the "Common Key" for your encryption type. The "Common Key" may be used for interoperable communications on these channels. When using encryption in mutual aid situations you should ensure that all the responding agencies are capable of your type of encryption and are using the "Common Key."

The naming convention for these channels is as follows:

- *SMPX1 (Subscriber Frequency RX 851.1000 TX 851.1000)*
- *SMPX2 (Subscriber Frequency RX 851.7500 TX 851.7500)*
- *SMPX3 (Subscriber Frequency RX 852.3000 TX 852.3000)*
- *SMPX4 (Subscriber Frequency RX 852.5500 TX 852.5500)*
- *SMPX5 (Subscriber Frequency RX 853.6875 TX 853.6875)*

These channels will have a 12.5 KHz channel spacing, a transmit deviation of 2.5 KHz, a programmed Network ID of 293, an output power of 3 watts or less, and use the APCO 25 (P 25) Common Air Interface digital signaling.

15.6 800 MHz NATIONAL INTEROPERABILITY CHANNELS

These channels are allocated as required channels under the FCC Rules & Regulations as well as the Region 7 800Mhz RPC plan for all users in the NPSPAC (National Public Safety Planning Advisory Committee) frequency band. These channels may be used in Repeater Mode as described below or in Direct Mode for on scene conventional radio to radio communications. These Channels will have 25 KHz channel spacing and a transmit deviation of 5.0 KHz with a continuous tone coded squelch of 156.7 Hz.

15.6.1 CHANNEL USE

Plain language will be used on all five National Interoperability Channels at all times, and the use of unfamiliar terms, phrases or codes will be kept to a minimum, unless deemed necessary for security purposes. The use of these channels for intra-system normal dispatch and routine agency operations is strictly prohibited. Normally, the five National Interoperability Channels are to be used only for activities requiring communications between agencies not sharing any other compatible communication system. Under emergency situations, one or more Tactical Channels (Section 13.6.3) may be assigned by the controlling agency at the time of the incident.

15.6.2 CALLING CHANNEL – 8CALL90

This channel will have a 25 KHz channel spacing and a transmit deviation of 5 KHz with transmit and receive continuous tone coded squelch of 156.7 Hz.

The calling channel shall be used to contact other users in the Region for the purpose of requesting incident related information and assistance. This channel shall not be used as an ongoing working channel. Once contact is made, an agreement upon which tactical channel to use is recommended for continued communications.

Contact the DTRMC for current location of the 8CALL90 repeaters.

- 8CALL90Subscriber Frequency RX 851.0125 TX 806.0125
- 8CALL90D Subscriber Frequency RX 851.0125 TX 851.0125

15.6.3 TACTICAL CHANNELS 8TAC91 - 8TAC94

8TAC91-8TAC94 AND 8TAC91D – 8TAC94D channels are reserved for use by those agencies in need of conducting inter-agency communications. Incidents requiring multi-agency participation will be coordinated over these channels by the agency controlling the incident. Individual tactical channels may be designated for use by various services on an incident basis by the controlling agency. In the event of multiple incidents requiring the use of these channels, channels shall be designated by mutual agreement between controlling agencies.

15.6.4 8TAC91

This channel will have a 25 KHz channel spacing and a transmit deviation of 5 KHz with transmit and receive continuous tone coded squelch of 156.7 Hz.

Contact the DTRMC for current location of the 8TAC91 repeaters.

- 8TAC91 Subscriber Frequency RX 851.5125 TX 806.5125
- 8TAC91D Subscriber Frequency RX 851.5125 TX 851.5125

15.6.5 8TAC92

This channel will have a 25 KHz channel spacing and a transmit deviation of 5 KHz with transmit and receive continuous tone coded squelch of 156.7 Hz.

Contact the DTRMC for current location of the 8TAC92 repeaters.

- 8TAC92Subscriber Frequency RX 852.0125 TX 807.0125
- 8TAC92D Subscriber Frequency RX 852.0125 TX 852.0125

15.6.6 8TAC93

This channel will have a 25 KHz channel spacing and a transmit deviation of 5 KHz with a transmit and receive continuous tone coded squelch of 156.7 Hz.

Contact the DTRMC for current location of the 8TAC93 repeaters.

- 8TAC93 Subscriber Frequency RX 852.5125 TX 807.5125
- 8TAC93D Subscriber Frequency RX 852.5125 TX 852.5125

15.6.7 8TAC94

This channel will have a 25 KHz channel spacing and a transmit deviation of 5 KHz with transmit and receive continuous tone coded squelch of 156.7 Hz.

Contact the DTRMC for current location of the 8CALL90 repeaters.

- 8TAC94 Subscriber Frequency RX 853.0125 TX 808.0125
- 8TAC94D Subscriber Frequency RX 853.0125 TX 853.0125

15.7 700 MHZ NATIONAL INTEROPERABILITY CHANNELS

These channels are allocated under the FCC Rules & Regulations as required channels by the Region 7 700 MHz Regional Plans for all users using the public safety 700 MHz frequency band. These channels must comply with the ANSI/TIA/EIA-102 (Project 25) Common Air Interface. These Channels will have 12.5 KHz channel spacing and a transmit deviation of 2.5 KHz with a Network ID of $293.

All subscriber units will use the following defaults:

- *Talkgroup ID is $0001*
- *Manufacturer's ID is $00.*
- *Message ID for unencrypted messages is $0000.*
- *Encryption Algorithm ID for unencrypted messages is $80.*
- *Encryption Key ID for unencrypted messages is $0000.*

These channels may be used in Repeater Mode as described below or in Direct Mode for on scene conventional digital radio to radio communications. Both Repeater Mode and Direct Mode are required in the subscriber. Plain language will be used on all National Interoperability Channels at all times, and the use of unfamiliar terms, phrases or codes will be kept to a minimum, unless deemed necessary for security purposes. The use of these channels for intra-system normal dispatch and routine agency operations is strictly prohibited. Normally, the National Interoperability Channels are to be used only for activities requiring communications between agencies not sharing any other compatible communication system. Under emergency situations, one or more Tactical Channels may be assigned by the controlling agency at the time of the incident. Encryption is not allowed on the Calling Channel but may be used on the other channels by complying with the procedures stated in the Region 7 700 MHz Regional Plan.

15.7.1 CALLING CHANNEL - 7CALL50 & 7CALL70

The calling channel shall be used to contact other users in the Region for the purpose of requesting incident related information and assistance. These channels shall not be used as ongoing working channels. Once contact is made, an agreement upon which tactical channel to use is recommended for continued communications. These channels may be used in Repeater Mode as described above or in Direct Mode for on scene conventional digital radio to radio communications. Both Repeater Mode and Direct Mode of both channels are required in the subscriber.

- 7CALL50Subscriber Frequency RX 769.24375 TX 799. 24375
- 7CALL50D Subscriber Frequency RX 769.24375 TX 769.24375
- 7CALL70Subscriber Frequency RX 773.25625 TX 803.25625
- 7CALL70D Subscriber Frequency RX 773.25625 TX 773.25625

Currently there are no repeaters for this channel installed for operation in Colorado.

15.7.2 GENERAL PUBLIC SAFETY TACTICAL CHANNEL - 7TAC55 & 7TAC75

These channels are reserved for use by those public safety agencies in need of conducting inter-

agency communications. These tactical channels may be designated for use by various services on an incident basis by the controlling agency under NIMS. Incidents requiring multi-agency participation will be coordinated for this channel by the agency controlling the incident. In the event of multiple incidents requiring the use of these channels, channels shall be designated by mutual agreement between controlling agencies. These channels may be used in Repeater Mode as described above or in Direct Mode for on scene conventional digital radio to radio communications. Both Repeater Mode and Direct Mode of both channels are required in the subscriber.

- 7TAC55 Subscriber Frequency RX 769.74375 TX 799.74375
- 7TAC55D Subscriber Frequency RX 769.74375 TX 769.74375
- 7TAC75 Subscriber Frequency RX 773.75625 TX 803.75625
- 7TAC75D Subscriber Frequency RX 773.75625 TX 773.75625

Currently there are no repeaters for this channel installed for operation in Colorado.

15.7.3 OTHER PUBLIC SERVICE TACTICAL CHANNEL – 7GTAC57 & 7GTAC77

This channel is reserved for use by those public service agencies in need of conducting inter-agency communications. This tactical channel may be designated for use by various services on an incident basis by the controlling agency under NIMS. Incidents requiring multi-agency participation will be coordinated for this channel by the agency controlling the incident. In the event of multiple incidents requiring the use of these channels, channels shall be designated by mutual agreement between controlling agencies. This channel may be used in Repeater Mode as described above or in Direct Mode for on scene conventional digital radio to radio communications. Both Repeater Mode and Direct Mode of both channels are required in the subscriber.

- 7GTAC57Subscriber Frequency RX 770.99375 TX 800.99375
- 7GTAC57D Subscriber Frequency RX 770.99375 TX 770.99375
- 7GTAC77 Subscriber Frequency RX 774.85625 TX 804.85625
- 7GTAC77D Subscriber Frequency RX 774.85625 TX 774.85625

Currently there are no repeaters for this channel installed for operation in Colorado.

15.7.4 MOBILE REPEATER TACTICAL CHANNEL – 7MOB59 & 7MOB79D

There are no fixed repeater sites for these channels. These channels are dedicated to operating on scene portable repeaters for temporary operations or for Direct Mode on scene communications. In no case shall control of these channels remain with any single agency beyond the termination of a declared event. These channels may be used in Repeater Mode as described above or in Direct Mode for on scene conventional digital radio to radio communications. Both Repeater Mode and Direct Mode of both channels are required in the subscriber.

- 7MOB59 Subscriber Frequency RX 770.89375 TX 800.89375
- 7MOB59D Subscriber Frequency RX 770.89375 TX 770.89375
- 7MOB79Subscriber Frequency RX 774.50625 TX 804.50625
- 7MOB79D Subscriber Frequency RX 774.50625 TX 774.50625

15.8 STATEWIDE CHANNEL – STAC, STACD

There are no fixed repeater sites for this channel. Portable repeaters are also allowed to use STAC for temporary repeater operations. In no case shall control of these channels remain with any single agency beyond the termination of a declared emergency event.

This channel may also be utilized with the ACU-1000 to patch VHF/UHF channels. An ACU100 Resource list can be found in the Colorado Tactical Communications Field Operation Guide (CO-TICFOG) issued by the North Central Region All Hazards group.

STACD is intended to be used at low power in simplex analog mode for SWAT, DIVE teams, etc. This channel may be used to communicate with medical aircraft in the area. This channel will have a 12.

KHz channel spacing and a transmit deviation of 2.5 KHz with transmit and receive continuous tone coded squelch of 156.7 Hz.

STAC	Subscriber Frequency RX 853.7875	TX 808.7875
STACD	Subscriber Frequency RX 853.7875	TX 853.7875

CHAPTER 16 AIRCRAFT COMMUNICATIONS

Use of trunked talkgroups on DTR by aircraft is only allowed for authorized radios which are installed as fixed radios in the aircraft. The operation of DTR radios onboard aircraft is governed by Title 47 of the Code of Federal Regulations (CFR) Part 90 Private Land Mobile Radio Services §90.423. As authorized in §90.423(a) (4), to minimize the interference potential to the DTR system, radios operated in aircraft must be limited to 3 watts Effective Radiated Power (ERP), shall not be used when the aircraft's elevation exceeds 3,000 feet above ground level (AGL), and shall have the radio ID assigned to the "Aircraft" Radio User Site Access Profile in the User Configuration Manager (UCM). The "Aircraft" Radio User Site Access Profile will only allow aircraft radios to be used at a pre-determined set of sites on the DTRS. Aircraft radio operators should be aware that the Doppler Effect may significantly degrade their aircraft's DTR radio performance when traveling at speeds greater than approximately 150 knots.

Due to frequency reuse, statewide coverage for DTR radios in aircraft is not guaranteed, and operators of aircraft DTR radios are encouraged to become familiar with the coverage of the system in their normal operating area while in the air and on the ground. Due to the limited number of sites available for use by aircraft DTR radios, once an aircraft gets close to the ground, DTR coverage may be degraded depending on its proximity to the available sites. If DTR coverage is not available the only channels available for aircraft air to ground communications are conventional analog simplex channels STACD, 8CALL90D, 8TAC91D, 8TAC92D, 8TAC93D, 8TAC94D and conventional simplex P25 digital channels SMPX 1 through SMPX 5.

Any portable radio that can operate on DTR carried aboard an aircraft shall be turned off prior to the aircraft taking off, this includes any radio typically assigned to units that perform duties on the ground including but not limited to all law enforcement radios, fire service radios or EMS radios. These radios may only be turned back on once the aircraft has landed.
A request to use a radio on DTR in an aircraft shall first be presented to the CCNC Technical Committee by submitting the ***COLORADO STATEWIDE DIGITAL TRUNKED RADIO (DTR) SYSTEM AIRCRAFT OPERATION APPLICATION*.**

The request will be reviewed and a recommendation passed on to the CCNC Executive Board. The CCNC Executive Board will receive this recommendation from the CCNC Technical Committee, and has the final approval authority for the request.

CHAPTER 17 SYSTEM IMPROVEMENTS

Due to the complexity of the Statewide DTR System; replacements, additions, modifications, or equipment upgrades must be evaluated for their impact on the System. At a minimum, proposals for additions, modifications, or equipment upgrades must be reviewed to ensure compliance with system version, system capacities, availability of proper system licensing, possible impacts on system loading, effects on system coverage, system security concerns and proper permissions from infrastructure equipment/site owners.

System improvements need to be coordinated with all DTRS Engineering Groups and the CCNC Technical Committee and affected system infrastructure owners/stakeholders. Agencies wishing to replace, add, modify, or upgrade infrastructure or infrastructure equipment must be a User Member of CCNC. Members of The Pikes Peak Regional Communications Network (PPRCN) are considered User Members of CCNC by Letter of Agreement between PPRCN and CCNC.

17.1 SYSTEM UPGRADES

System Release Version upgrades and other technology implementations shall be presented to all DTRS Engineering Groups, the CCNC Technical Committee and the CCNC Board of Directors for consideration and recommendation to the CCNC Executive Board. The CCNC Executive Board shall make the final decision. Upgrade and technology presentations shall be presented in both written and oral form. They shall include detailed information on the benefits of the upgrade, equipment replacement, financial obligations, and a projected upgrade time schedule to include training opportunities and end user responsibilities. The proposal must also include verification that all impacted infrastructure equipment/site owners have agreed to participate in the project. The CCNC Technical committee will evaluate the proposal and make a recommendation to the CCNC Executive Board identifying the pros and cons associated with the upgrade. The CCNC Executive Board will consider the proposal and the CCNC Technical Committee's recommendation to determine the feasibility of implementing the proposal and to determine how to fund the project. If funding can be secured, the CCNC Executive Committee will make a decision on the approval of the project recommendation.

17.2 RF SITE ADDITIONS

Procedure is being finalized.

17.3 MODIFYING RESOURCES AT AN EXISTING RF SITE

Procedure is being finalized.

17.4 DISPATCH CONSOLES

Procedure is being finalized.

17.5 INFRASTRUCTURE REPLACEMENT

Procedure is being finalized.

CHAPTER 18 MAINTENANCE

18.1 PROBLEM REPORTING BY USER/S

Users experiencing communication problems that they believe are system related should follow any agency operating procedures for trouble reporting. If your agency has no established procedure, contact your agency radio representative, programming agency or the DTRMC (303-764-7975).

18.2 SUBSCRIBER UNITS

User agencies are responsible for coordination of their agency subscriber unit maintenance and programming. Users experiencing communication problems that they believe are subscriber unit related should follow any agency operating procedures for maintenance.
Any radio sent to the vendor for repair may be sent with the programming intact. Whenever possible, the sending agency should archive the file from the radio prior to shipping. When radios are returned from Vendor repair, they should be verified for correct codeplug information and that they are write protected if capable.

18.2.1 SUBSCRIBER PROGRAMMING

Only ID(s) and talkgroups that have received prior authorization from CCNC may be programmed. All radios will be programmed for write protect file access if the equipment supports the write protect function. All radios will be programmed to allow Radio Inhibit from the System Management Terminal.

All programming agencies shall maintain current and accurate records of all programming performed. The recommended format is a spreadsheet with 19 columns labeled:

- Radio Type (13-characters);
- Radio ID (8-characters);
- Serial Number (12-characters);
- Radio Alias (20- characters);
- Radio User (20-characters);
- Organization (20-characters);
- Owner (15-characters);
- Model (15-characters);
- Flash Code (15-characters);
- HOST Version (12-characters);
- DSP Version (12-characters);
- County (9-characters);
- System Zone (6-characters);
- System Pkg (6-characters);
- Memory Size (6-characters);
- Govt. Level (9-characters);
- Jurisdiction (20-characters);
- Programming Agency (8-characters);
- Radio Technicians Initials (8-characters).

Records shall be made available upon request to the State of Colorado or CCNC. Any programming agency with Access to the UCM will provide electronic updates to the DTR Monitoring Team for any radios they have added, removed or modified in the UCM. **This update should be sent via email within five (5) days of the change and follow the format described above.**

Agencies programming shared talkgroups into subscribers shall provide documentation to the DTRMC at webdtr@state.co.us from the talkgroup owner showing that permission was granted for sharing the talkgroup.

18.2.2 AUTHORIZED SUBSCRIBER PROGRAMMING AGENCIES

Agencies that demonstrate the necessary technical knowledge and responsibility for security of system information may become Authorized System Key holders and are therefore authorized to program subscriber units, see Section 7.3. Contact webdtr@state.co.us for a list of Authorized System Key holders is available here and may be updated as needed without formally revising this document.

Authorized programming agencies are required to keep an accurate database of subscriber units they have programmed. An annual review of this database shall be conducted by the Technical Committee.

These Authorized System Key holders are also responsible for keeping system information secure from general publication.

18.2.3 LOANER SUBSCRIBER UNITS

Loaner subscriber units are not the responsibility of CCNC. Users should provide their own loaner subscriber units or check with the agency providing their subscriber maintenance for the availability of loaner equipment.

18.2.4 SUBCRIBER RADIO PERFORMANCE SPECIFICATIONS

All subscriber radios used on the system must conform to all pertinent FCC rules and regulations set forth in CFR 47, Part 90. Specifically, subscriber radios should be maintained and serviced “as often as may be necessary to ensure proper operation.” Per 90.433(c) This shall include testing for transmitter frequency stability. Since many of the CCNC system frequencies lie within the 700MHz public safety narrowband portion of the spectrum, subscriber transmitters shall follow frequency stability specifications set forth in 90.539(c). CCNC recommends subscriber radios to be serviced once per year and be tested for transmitter performance. The DTRS, PSCN, and other infrastructure owners have deployed test equipment to verify radio calibration known as DiagnostX. If your agencies radios are reported to your agency as failing a DiagnostX receiver test you are required to have them serviced as soon as possible (ASAP) but not later than 60 days and report back to the entity reporting the failure acknowledging the radios have been serviced. Failure to make reasonable efforts to maintain and service your radios is grounds for discipline up to and including loss of permission to operate those radios on the DTRS. Incidents of repeated failure to keep radios calibrated and serviced will be investigated and dealt with on a case-by-case basis.

18.2.4 DISPOSAL OR TRANSFER OF SUBSCIRBER RADIOS

All subscriber radios to be disposed of or transferred to another agency shall have all system programming removed, which includes the System ID, Home WACN ID, Unit ID, Trunking Personalities to include Talkgroup ID from the radios. If the radio IDs are managed by the DTRS monitoring group, the decommissioning of the radios and IDs will be made known to the monitoring group so that system records can be updated. If you are a user of another infrastructure owners managed Radio IDs you are responsible to inform that infrastructure owner. Failure to comply with notification and decommissioning of system and unit and talkgroup information from a radio is grounds for discipline up to and including loss of permission to operate radios on the DTRS. Any cost associated with correcting the issues will also be the responsibility of the agency in violation. If your radio equipment becomes too obsolete it may leave you with the possibility of having to destroy the equipment or have a vendor who is capable, provide a certification the radio, by serial number, is wiped clean of all required information.

18.3 WIRELINE DISPATCH CONSOLES

User agencies are responsible for coordination of their agency console maintenance. Users experiencing communication problems that they believe are console related should follow any agency operating procedures for maintenance. Monthly Console software updates are pushed to the wireline consoles monthly by the system administrator. User agencies are responsible for rebooting the computer for each console position after the 7th day of the month but no later than the 15th day of the month to install the updates. It is recommended that the console positions be updated one position at a time.

18.4 SYSTEM INFRASTRUCTURE

The owners of system site equipment and/or connectivity equipment between sites are responsible for the maintenance of such equipment. Today service and maintenance on the Statewide DTR infrastructure is provided by a variety of methods and agencies. This includes State staff, local government agency staff and private contractors. The Service Level Agreement (SLA) adopted by CCNC is included in this document in its entirety in this section:

18.4.1 SERVICE LEVEL AGREEMENT (SLA)

The various components of the system infrastructure include:

- *Zone Controllers including Servers, Switches/Routers, Digital cross connect systems, Common console system components, System monitoring and reporting components*
- *Microwave systems*
- *Leased fiber and phone lines*
- *Primary and remote site buildings, towers, HVAC, primary and backup power systems*
- *Remote site electronics including Site Controllers, Site switches/routers, Repeaters, Channel* banks, *Remote monitoring equipment*
- *Antenna systems including Tower top amplifiers, Transmitter combiners, Receive multicouplers*

- *Local dispatch consoles, Consolettes, Control stations*
- *Site access*

18.4.1.1 SEVERITY LEVELS

With the 24/7 mission critical requirements for CCNC, it is absolutely necessary to strive for maximum system availability with minimum down time, service impairment or disruption. The overall design of the DTR provides several levels of redundancy that enables meeting this objective however, failures of varying degrees will occur. Depending on the location and type of failure or outage, the impact to the system and users can range from no impact to the total loss of service. Failures and outages must be defined in several levels according to the impact on the system and users. The level will then drive the type of response required.

The table below outlines the levels and definitions that have been established. The initial failure/outage level shall be determined by the affected agency/user using the table on the following page.

Severity Level		Description
Critical	Level 1	A system failure or outage that creates total system unavailability to one or more sites, one or more coverage areas, or one or more groups of users.
Severe	Level 2	A system failure or outage that impacts or reduces the coverage, the capacity, or the operational capability of the system, site, coverage area or group of users. (Approximately 1/3 or more of the available resources have failed)
Impaired Service Effecting	Level 3	A system failure or outage that reduces the coverage, capacity, operational capability of the system, sites, coverage area or group of users. (Approximately less than 1/3 of the available resources have failed.)
Impaired Non Service Effecting	Level 4	A system failure or outage that has little or no reduction in coverage, capacity, operational capability of the system, sites, coverage area or group of users.

Specific failure and outage are listed in the Table of Severity Definitions on the following page. The level may be escalated or de-escalated as described in section 18.4.3.

DTR SLA SEVERITY LEVELS		REPONSE REQUIREMENTS				
Classification	**Level**	**Failure or Outage Type**	**Initial Mobilization Plan**	**Initial Follow-up After Mobilization**	**Subsequent Follow-up Notifications**	**Maximum Restoring time Upon Arrival**
Critical	1	Entire Zone Down	1 hour	2 hour	4 hour	4 hour
Critical	1	Multiple Sites Down	1 hour	2 hour	4 hour	4 hour
Critical	1	Single Site Down with no Overlapping Coverage	1 hour	2 hour	4 hour	4 hour
Critical	1	Dispatch Center Down (all consoles)	1 hour	2 hour	4 hour	4 hour
Critical	1	Microwave Backbone Down Effecting 2 or More Sites	1 hour	2 hour	4 hour	4 hour
Critical	1	More than 66% of Site Channels Down	1 hour	2 hour	4 hour	4 hour
Critical	1	No Interzone Traffic	1 hour	2 hour	4 hour	4 hour
Severe	2	Single Site Down with Overlapping Coverage	2 hour	2 hour	4 hour	8 hour
Severe	2	More than 33% of Site Channels Down	2 hour	2 hour	4 hour	8 hour
Severe	2	Microwave System Down at a Single Site	2 hour	2 hour	4 hour	8 hour
Severe	2	Primary Power Outage, No Generator	2 hour	2 hour	4 hour	8 hour
Impaired – Service Effecting	3	Single Channel Down at High Traffic Site	4 hour	2 hour	4 hour	8 hour
Impaired – Service Effecting	3	Single Site Reduced Coverage	4 hour	2 hour	4 hour	8 hour
Impaired – Service Effecting	3	Interference a 1 or More Sites	4 hour	2 hour	4 hour	8 hour
Impaired – Service Effecting	3	HVAC Alarm	4 hour	2 hour	4 hour	8 hour
Impaired – Service Effecting	3	Single Dispatch Console Down	4 hour	2 hour	4 hour	8 hour
Impaired – Non Service Effecting	4	Single Channel Down	4 hour	NA	24 hour	72 hour
Impaired – Non Service Effecting	4	Primary Power Outage, Generator Running	4 hour	NA	24 hour	72 hour
Impaired – Non Service Effecting	4	Primary Power Up, Generator Out of Service	4 hour	NA	24 hour	72 hour

Terms of Severity Definitions

18.4.2 MAINTENANCE RESPONSE AND SERVICE RESTORATION

In order to meet the system availability objectives, a specific response and service restoration level must also be defined based of the failure/outage level. Due to the remote locations of DTR sites and the access conditions, methods and seasonal changes, it is not possible to provide specific or guaranteed service restoration times. It is however reasonable and necessary to provide specific response plans including target service restoration times, depending on the failure/outage level. The above Table of Severity Definitions provides examples of various failures and their corresponding response requirements.

18.4.2.1 CRITICAL *(Level 1)*

Upon notification of a failure/outage by either automatic or manual means, the responsible agency shall immediately begin investigation into the reasons, location and system/user impact. Additional notifications should be made as soon as practical to the DTRMC at 303-764-7975, affected areas, users and/or other service providers as necessary. Service personnel shall strive to have the location and failure/outage identified within 1 hour after the initial notification.

Mobilization of the required resources necessary for service restoration should begin within 1 hour after the location and failure is determined. Initial follow up notifications should take place within 2 hours after initial notification to the affected areas, users and/or other service providers as necessary and every 2 hours thereafter until service is fully restored or the level reduced to Impaired Non Service Affecting. The follow up notifications shall include the estimated time for service personnel to be on site at the failure/outage location, overall system impact, temporary work around if applicable. Within 1 hour after arrival at the failure/outage site a restoration plan and time estimation shall be communicated to the affected areas, users and/or other service providers as necessary.

Follow up notification on the progress with revised restoration time estimates shall be made every 2 hours. If the estimated restoration time frame exceeds 4 hours from arrival on site, a notification call with details of the failure/outage and the restoration plan including estimated time to repair shall be made to all affected parties and all service providers. Once service is restored the affected areas, the DTRMC, users and/or other service providers shall be notified to confirm system restoration prior the leaving the site or demobilization. Outage reporting and documentation shall be completed and submitted as required in section 18.4.4.

18.4.2.2 SEVERE *(Level 2)*

Upon notification of a failure/outage by either automatic or manual means, the responsible agency shall immediately begin investigation into the reasons, location and system/user impact. Additional notifications should be made as soon as practical to the DTRMC, affected areas, users and/or other service providers as necessary. Service personnel shall strive to have the location and failure/outage identified within 2 hours after the initial notification.

Mobilization of the required resources necessary for service restoration should begin within 2 hours after the location and failure is determined. Initial follow up notifications should take place within 2 hours

after initial notification to the affected areas, users and/or other service providers as necessary and every 4 hours thereafter until service is fully restored or the level reduced to Impaired Non-Service Affecting. The follow up notifications shall include the estimated time for service personnel to be on site at the failure/outage location, overall system impact, temporary work around if applicable. Within 1 hour after arrival at the failure/outage site a restoration plan and time estimation shall be communicated to the affected areas, users and/or other service providers as necessary.

Follow up notification on the progress with revised restoration time estimates shall be made every 4 hours. If the estimated restoration time frame exceeds 8 hours from arrival on site, a notification call with details of the failure/outage and the restoration plan including estimated time to repair shall be made to all affected parties and all service providers.

Once service is restored the affected areas, the DTRMC, users and/or other service providers shall be notified to confirm system restoration prior the leaving the site or demobilization. Outage reporting and documentation shall be completed and submitted as required in section 18.4.4.

18.4.2.3 IMPAIRED SERVICE EFFECTING *(Level 3)*

Upon notification of a failure/outage by either automatic or manual means, the responsible agency within 1 hour shall begin investigation into the reasons, location and system/user impact. Additional notifications should be made as soon as practical to the DTRMC, affected areas, users and/or other service providers as necessary. Service personnel shall strive to have the location and failure/outage identified within 2 hours after the initial notification.

Mobilization of the required resources necessary for service restoration should begin within 4 hours after the location and failure is determined. Initial follow up notifications should take place within 2 hours after initial notification to the affected areas, users and/or other service providers as necessary and every 4hours thereafter until service is fully restored or the level reduced to Impaired Non-Service Affecting. The follow up notifications shall include the estimated time for service personnel to be on site at the failure/outage location, overall system impact, and a temporary work around if applicable. Within 1 hour after arrival at the failure/outage site a restoration plan and time estimation shall be communicated to the affected areas, users and/or other service providers as necessary.

Follow up notification on the progress with revised restoration time estimates shall be made every 4 hours. If the estimated restoration time frame exceeds 8 hours from arrival on site, a notification call with details of the failure/outage and the restoration plan including estimated time to repair shall be made to all affected parties and all service providers. Once service is restored the affected areas, the DTRMC, users and/or other service providers shall be notified to confirm system restoration prior the leaving the site or de-mobilization. Outage reporting and documentation shall be completed and submitted as required in section 18.4.4.

18.4.2.4 IMPAIRED NON-SERVICE EFFECTING *(Level 4)*

Upon notification of a failure/outage by either automatic or manual means, the responsible agency within 4 hours shall begin investigation into the reasons, location and system/user impact. Additional notifications should be made as soon as practical to the DTRMC, affected areas, users and/or other service providers as necessary. Service personnel shall strive to have the location and failure/outage identified within 24 hours after the initial notification.

Mobilization of the required resources necessary for service restoration should begin within 24 hours or the next business day after the location and failure is determined. If the estimated restoration time frame exceeds 72 hours from the initial notification, a notification call with details of the failure/outage and the restoration plan including estimated time to repair shall be made to affected areas, users and/or other service providers as appropriate.

Once service is restored the affected areas, the DTRMC, users and/or other service providers shall be notified to confirm system restoration prior the leaving the site or demobilization. Outage reporting and documentation shall be completed and submitted as required in section 18.4.4.

18.4.3 ESCALATION/DE-ESCALATION

The initial failure/outage level shall be determined by the affected agency/user as described in section 16.4.1.1. Due to the complexity of the system, the initial determination may not be correct or the circumstances, current events or actual failure/outage may require the level to be changed.

18.4.3.1 USER ESCALATION

At any time during the failure/outage, agencies may request that the level be escalated to a higher level. The escalation request should be made to the service agency responsible for the site/equipment causing the failure/outage. The escalation request shall include the information on what has changed since the initial level determination and how the request meets the criteria for the requested level as defined in 18.4.1.1. The responsible service agency shall evaluate and discuss the escalation request with the requesting agency. If the request meets the criteria for the higher level as defined in 18.4.1.1, the level shall be escalated and the appropriate response and restoration plan implemented. If the request does not meet the criteria for the higher level as defined in 18.4.1.1, the level shall not be escalated. If an agreement cannot be reached between the affected agency and the service provider, the level shall be escalated and the appropriate response and restoration plan implemented. All escalations shall be documented and reported as required in section 18.4.4.

18.4.3.2 SERVICE PROVIDER ESCALATION/DE-ESCALATION

After the actual failure/outage cause has been determined, a service provider may raise or lower the level as appropriate if failure/outage meets the criteria in 18.4.1.1 for the new level. If the initial level is changed, a new notification should be made to the affected areas, users and/or other service providers as necessary and the appropriate response and restoration plan implemented.

18.4.4 MAINTENANCE HISTORY REPORTING

Any agency that has a service disruption, outage or failure should report the problem to the DTRMC at 303-764-7975 during the DTRMC normal hours of operation or directly to their maintenance provider. The monitoring center will enter the failure or outage in a Failure/Outage Log, assist with classifying the

severity level of failure/outage and obtain other relevant information. Based on the location and type of failure/outage the DTRMC will then contact the appropriate agencies to initiate the response if necessary. All required follow up notifications should be communicated to the DTRMC so they can be entered into the Failure/Outage Log Action Plan. The DTRMC may assist with the notifications.

If the maintenance provider is contacted directly by the agency experiencing the failure/outage, then the maintenance provider will classify the severity level of the failure/outage and make the appropriate contacts. The maintenance provider will transfer the Failure/Outage Log information to the DTRMC as soon as reasonably possible. The DTRMC may be contacted via telephone or email.

In order to validate the SLA, track response, service restoration, history, reporting and root cause analysis for failures and outages, it is necessary to establish a common reporting methodology.

- *The State DTRMC will be the primary entry point for maintenance history reporting. All failures/outages should be reported to the DTRMC.*
- *At a minimum the following information will be entered into the Failure/Outage* Log:
- *Reported failure, outage or trouble*
- *Date & time reported*
- *Reporting person, agency and contact information*
- *Effected Site or area*
- *Initial Severity Classification*
- *Responsible service provider*
- *Action plan for responding to or correcting the failure/outage (Action Plan)*
- *The maintenance provider will provide updates to the "Action Plan" as they are required according to the severity level of the failure/outage.*
- *Failure/Outage corrected date & time*.
- *The Failure/Outage Log information may be shared among all service providers to establish a knowledge base for future issues.*

18.4.5 MAINTENANCE TRAINING

In order to provide effective and efficient service and meet the SLA response and restoration objectives, it is necessary to set minimum training levels for all service personnel. The training levels will be established by The Public Safety Communications Network (the State), and the CCNC Technical committee based on Motorola recommended training for the type of equipment for which each provider is responsible.

Training Levels are listed in the following Table. The Table is a training guideline only. Actual courses offered by Motorola vary annually. It is recommended that technicians be trained with the most current courses available that are equivalent to, or replacements of, those courses in the Table.

Each entity that is responsible for service and/or maintenance on the Statewide DTR infrastructure will maintain documentation of the training of their personnel. This documentation may be certificates of completion from vendor provided training courses, or letters from agency supervisory personnel stating that the identified technician has demonstrated his competency through on-the-job training or prior experience. This includes State staff, local government agency staff and private contractors. The training documentation shall be available for review by CCNC during normal business hours.

Colorado Statewide Digital Trunked Radio System **Service Level Agreement Training**		
Training Title	**Recommended for**	
	RF Sites	**Master Site (Zone)**
Bridging The Knowledge Gap	X	X
Networking for Astro 25 IV&D Systems	X	X
Astro 25 IV&D System Overview	X	X
Astro 25 IV&D System Introduction to Network Management		X
Astro 25 IV&D System Radio Network Management Workshop		X
Astro 25 IV&D System Master Site Workshop		X
Astro 25 IV&D System Repeater Site Workshop	X	
Astro 25 IV&D Digital Simulcast Workshop	X	
MOSCAD Network Fault Management Programming		X
MOSCAD Network Fault Management Maintenance	X	

Table 18 A – Training Levels

18.4.6 PRIMARY SERVICE RESPONSIBILITY AND BACK UP SUPPORT

Each site will be designated with a primary service provider. In most cases this will be the site/equipment owner. In some cases, it may be a designated service provider under a service contract or service agreement (MOU). The DTRMC will maintain a database for each site with the designated primary service provider. It is the responsibility of the site/equipment owner to notify the DTRMC with any update or changes. The primary service provider is responsible for compliance with this SLA.

There may be times when the primary service provider does not have the required resources to meet the SLA requirements. When those cases occur, the primary service provider may request back up support from other service providers as appropriate. The request and agreement for backup support is the responsibility of the primary service provider. The use of back up support does not relieve the primary provider of the SLA response, restoration or reporting requirements. The back- up provider may complete these actions on behalf of the primary provider, but is still remains the primary provider's responsibility. The primary provider may pre-establish agreements with other providers for their back up support. Any pre-established back up providers shall be communicated to the DTRMC for inclusion into the database.

18.4.7 MAINTENANCE SAFETY

Regardless of the categorized condition, times can be delayed or given an alternate suspense time/date if the repair would jeopardize the safety of response personnel. i.e., if the repair would require the climbing of an icy tower, or taking a Sno-Cat across a snowfield that undercuts a cornice - the response can be delayed until safe passage and work conditions can be achieved. Or, a risk analysis needs to be performed.

CHAPTER 19 USER TRAINING

It is the responsibility of each user agency to ensure that all their subscriber users are properly trained in the use and functions of their subscriber units as well as the standard operating procedures for the Statewide DTR system. System infrastructure overview training is available upon request from the CCNC training committee.

Guidance for end user training program development is available from the CCNC Training Committee but the actual development of the training program and end user training is the responsibility of the user agency.

CHAPTER 20 CALL AUDIO RECORDING

CCNC does not carry the responsibility for the recording of talkgroup information exchanges. Each agency is responsible for their own recording of any interchange of information from or to their personnel on their agency talkgroups, on any MAC talkgroups, or other channels they utilize.

CHAPTER 21 BI-DIRECTIONAL AMPLIFIERS (BDAS)

Agencies may deploy Bi-directional amplifiers (BDAs) to improve coverage within buildings or in isolated geographic areas that have minimal system coverage. Design and installation of any BDA/DAS should closely follow International Fire Code 2012 Section 510 standards.

Any agency deploying or approving use of a BDA should provide the Location, Model or Type, and Repair Agency Contact Information to the CCNC Technical Committee.

In the event that a BDA is causing system interference, the Installing Agency will be asked to discontinue the BDA's operation until repairs are made and/or the interference is eliminated.

CHAPTER 22 CONTINGENCY PLANS

Currently there is no CCNC contingency plan for a total system failure. Each user agency should develop their contingency plan depending on their individual needs and resources.

CHAPTER 23 SYSTEM INFORMATION

System information including:

- *System Overview*
- *Statewide DTR System Implementation*
- *Supporting Documentation and links,*

May be acquired from the following sources: State of Colorado Telecommunication Services Please send email to: webdtr@state.co.us Contact the team by phone: (303) 764-7975
State of Colorado Web page:

or

CCNC
40 West Littleton Blvd.
Suite 210-129
Littleton, CO 8 0 1 2 0

CCNC Web Page:

or

EMTS Communications Coordinator ***www.coems.info*** (303)692-2536

CHAPTER 24 STATE PRICING TABLES

Information on State Pricing is available on the State Web Page see CHAPTER 23.

CHAPTER 25 TRUNKING FEATURES

This section describes the trunking features available and the equipment and/or processes needed to utilize them. For specific information on features consult with your subscriber programming agency.

25.1 DYNAMIC REGROUPING

Dynamic Regrouping is a feature that allows subscriber units to be temporarily redirected to a specific talkgroup. Zone Controller connectivity with access to a network management terminal running the "Radio Control Manager" (RCM) of the Motorola system manger software suite is required. This feature also must be enabled in the subscriber units. Currently there are no known agencies within CCNC using this feature.

25.2 DISABLING SUBSCRIBER UNITS

If a radio is Lost, Stolen, or otherwise not accounted for this feature allows a network management terminal to disable a subscriber unit over-the-air. The subscriber unit appears to be dead to the users. Zone Controller connectivity with access to a network management terminal running the "Radio Control Manager" of the Motorola system manger software suite is required. This feature is available through the state telecommunication services at (303) 764-7975 or through a subscriber programming agency with access to a network management terminal.

The user agency must provide the State or other network management terminal owners with the subscriber ID and serial number of the unit to be disabled. If the radio is recovered the user agency must notify the network management terminal owner that disabled the subscriber unit.

25.3 EMERGENCY BUTTON

The Emergency Button is an optional feature that may or may not be utilized depending on the user agency needs. Agencies should discuss the various capabilities of the Emergency function with their subscriber unit template developer and programmer. If programmed the Emergency Button may do one or both of the following:

- *Send an Emergency Alarm (no voice message) to a network connected dispatch console or a Network*
- *Management RCM Terminal,*
- *Send an Emergency Call (voice message) to a properly equipped dispatch console, a Network*
- *Management RCM Terminal, and other subscriber units.*

25.3.1 USE OF EMERGENCY BUTTON

The Emergency button should only be used in case of imminent personal danger.
Emergencies should be cleared as soon as possible to minimize system impacts. This does not restrict nor does it supersede individual agencies policies.

25.3.2 MONITORING EMERGENCIES

CCNC is not responsible or liable for monitoring Emergency Activations. It is responsibility of each user agency to monitor or coordinate monitoring with another user agency. The user agency must keep an accurate account of subscriber Ids/Aliases and their assignments. This information must be provided to the monitoring agency and kept up to date. The monitoring agency will ensure the system databases are updated.

When radios are sent in for repair it is advised that user agencies notify the agency monitoring their Emergencies that this radio is out of service for repair. When the radio is returned to service the monitoring agency should also be notified.

25.4 SCAN

Scan is an optional programmable feature that allows for monitoring of multiple talkgroups. Scan DOES NOT guarantee delivery of audio to the subscriber units. Audio for the talkgroup selected by your mode/channel selector is always routed to the subscriber unit; however, audio for talkgroups in your scan list may or may not be routed to the subscriber unit. Therefore, CCNC doesn't recommend agencies rely on scan for daily operations.

25.5 PRIVATE CALL

Private Call is a feature that allows a voice call to be conducted between two subscriber units. Currently Private Call is not supported by the Statewide DTR System.

25.6 CALL ALERT

Call Alert allows a non-voice notification to be sent to a subscriber unit. This will cause a tone to be heard at the subscriber and a CA display message with an ID number on the subscriber unit. Call Alert must be enabled at the Zone Controller and programmed into the subscriber unit. Users should be trained to understand the difference between Call Alert and Emergency Call Receive messages.

25.7 TELEPHONE INTERCONNECT

Telephone Interconnect allows telephone calls to be transmitted from subscriber units. Currently this feature is not supported by the Statewide DTR System.

25.8 SITE TRUNKING

Site Trunking is a failure scenario that occurs when a trunking site is no longer capable of communicating with the system. In Site Trunking mode a subscriber unit will only be able to communicate with other subscribers on the same site. The subscriber unit will always try to move to another site that is not in Site Trunking. Site Trunking is commonly seen during the Statewide DTR system upgrades/maintenance. Subscriber units may be programmed to display and/or emit an alert tone during this condition.

25.9 FAILSOFT

Failsoft is a failure scenario whereby site channels are assigned in conventional mode if all trunking capabilities have failed. Currently Failsoft is not supported on the Statewide DTR system.

25.10 STATUS MESSAGING

Status Messaging allows for preprogrammed text messages to be sent from a subscriber unit to a properly equipped and connected dispatch console. User agencies should check with their

dispatch facility for availability of this feature.

CHAPTER 26 GLOSSARY

700 Megahertz	A new public safety frequency band for voice and data including wideband data channels. Channels between 764-806 Megahertz.
800 Megahertz	The frequency band where public safety trunked systems operate. The channels between 806 and 869 Megahertz.
Agency	Lowest level of structure within the member structure of CCNC. Each agency must sign a Participation Agreement. Examples include fire department or police department.
Alias	Proper names representing a Unit ID – Example "?PD Smith" or ?FD Eng.32"
All Call	Console feature which allows dispatcher or supervisor to communicate to all system subscribers at one time. Used for major traumas or emergencies.
Amplifier	A device for obtaining an increase in voltage, current, or power.
Amplitude	The maximum departure of the value of an alternating current or radio wave from the average value.
Analog	A signal that may vary continuously over a specific range of values.
Announcement Group	This is the same as All Call above.
Antenna	A device (usually metallic) for radiating or receiving radio waves.
Antenna Gain	The effectiveness of a directional antenna expressed as the ratio in decibels of standard antenna input power to the directional antenna input power that will produce the same field strength in the desired direction.
APCO	Associated Public Safety Communications Officials, Inc. An international professional organization with members from federal, state, local government and equipment vendors in all aspects of public safety communications.
Automatic Vehicular Locations (AVL)	Sub-system which interfaces with radio system to communicate actual location of a vehicle in a pre-mapped geographic grid via RF.
Bit	Abbreviation for binary digit (either a 0 or a 1), the basic unit for storing data in a computer.
BSI	Base Station Identifier. The BSI, which usually operates at the lowest frequency, is the Morse Code identification that automatically occurs at regular intervals from one of the trunked repeaters.
CAD	Computer Aided Dispatch. The current convention in public safety radio communications dictates use of computers in order to answer requests for emergency service more efficiently.
Call Alert	The ability of a dispatcher to selectively page an individual unit.
Call Queuing Call Queuing Cont.	When all channels on the system are busy, the call request is held in a first-in-first-out queue. The caller and all members of the groups are notified that a call request has been queued. Upon channel assignment, the caller is alerted and is allowed to proceed with push-to-talk (PTP)
Call Retry	Feature which is used by subscriber when unsuccessful in acquiring a requested channel. The subscriber will continue to request a channel until successful or has attempted 8 times. This is not apparent to the subscriber operator.
Cavity Filter	A device used to shield the receiver from the transmitter and to form a circuit called a duplexer.
CCIC	Colorado Crime Information Center

CCNC	Consolidated Communications Network of Colorado
Channel	A band of frequencies of sufficient width to allow a single communication.
Channel Access Time	The time between depression of the PTT switch by the subscriber operator and the presence of audio at the receiving subscribers. Fast access time contributes to system efficiency.
Channel Drop Time	The time between subscriber un-key and when the channel is actually available for another call. Fast drop time contributes to system efficiency.
Combiner	A device used to combine the output signals from a number of transmitters connected to the same antenna.
Console	Equipment in dispatch center tailored to dispatcher needs.
Control Channel	This is the channel of the system upon which outbound system updates and responses to service requests occurs; and it is the conduit for all interactions to gain access to trunking resources by subscriber units.
Conventional	Assigning a specific channel/frequency for a specific dedicated use. A non-trunked channel.
Coverage	The amount of percentage of area reached by a communications medium.
Cycle	One complete performance of a vibration, electric oscillation, current alternation, or other periodic process.
Digital	Encoding analog information into a code made up of 0's and 1's. Also, a slang term for garbled audio in a digital system.
Digitalization	The conversion of continuous analog waveform to binary digital data. See vocoder.
Dipole	A radio antenna consisting of two horizontal rods in line with each other, with their ends slightly separated.
Dispatch Point	Location where information is relayed to a mobile unit. Normal operating mode of the system. Communications are limited to single group and dispatcher. All in group hear only own group and dispatcher is communicating to single group.
Dynamic Regrouping	The ability to change a subscriber unit's active talkgroup over-the-air while the subscriber is operating in the field.
Dynamic Site Assignment	Allows a channel assignment only at sites necessary to reach all active talkgroup members.
Effective Radiated Power	A term for describing subscriber power levels.
Emergency Alarm	Data signal transmitted over a control channel to allow a dispatch to be notified of emergency conditions.
Emergency Button	Emergency buttons are available on every subscriber. When depressed, the available channel is assigned to the user – highest priority is assigned to an emergency user. Emergency indicators are lit on user group radios if programmed.
Encryption	Digitalization and scrambling of the voice signal to prevent unauthorized monitoring of the message over the airwaves.
Ethernet	A protocol used to develop a Local Area Network (LAN) of PC's.
Fail Soft	This is automatic fall-back mode of communication offered in the event that the trunking central controller fails, all control channels fail, or failure of all voice channels. The repeaters independently enter the fail-soft mode when the central zone controller no longer controls them; this is a form of carrier squelch community repeater operation.

Fault Tolerant Architecture	A design and implementation philosophy that permits a system to continue operating in the event of failure of major components.
FCC	Federal Communications Commission.
FDMA	Frequency Division Multiple Access. A method for improving spectrum efficiency by splitting an existing channel into 2 or more separate channels based on frequency.
FIFO	First In, First Out of Queue. Based upon priority. In the case of a busy trunked system, individual request for service will be handled in a FIFO manner.
Firmware	Hardware component, such as EEPROM's, which are programmed to contain software-like instruction are commonly referred to a Firmware.
Group	Combination of subscriber users which have been linked together for communications. May be system entity. May be defined from the system Manager position or dynamically reconfigured as needed.
Hang Time	The time a channel remains keyed after release of the PTT.
Hertz	Hz. Abbreviation for cycles per second.
Historical Reporting	A function performed by the zone controller. Records each transmission id and group as well as time of day and duration. Is sent to system manager terminal for data management.
IMBE	Improved Multi-Band Excitation. A method used to change an analog signal to a digital signal. Vocoding.
Infrastructure	The underlying permanent installations required for radio communications. Repeaters, microwave and site equipment.
Intellisite Repeater	ISR. Trunked repeater with computer capability to perform trunking functions.
Interface	Confusion of received radio signals due to stray or undesired signals. Can cause distorted audio.
Master Site Master Site Cont.	The term applies to the primary equipment site of a trunked simulcast system where all audio processing occurs. RF channel resource management also take place here; the Central Site Controller (CSC) in the Prime Site controls the Remote Site Controller (RESC) in the Remote Site with a data link message which is usually send via microwave (should simulcast be implemented). Location where the zone controller and related networking equipment reside.
MDT, MDC Data Terminals	Terminals which support the transmission of data via radio signals. Include a display and keyboard.
Message Trunking	The working channel remains assigned to a call for the duration of the group transmission. When the caller unkeys, the channel remains active until the group conversation is completed or the channels hang time is reached. The channel is not available for reassignment until the group conversation is done or the channel times out.
Modem	An acronym for modulator/demodulator, which is a device that translates digital signals coming from your computer into analog signals that can be transmitted over standard telephone lines. The modem also translates the analog signal back into a digital signal that your computer can understand.
Multi-Select	A feature available to console dispatcher. Two or more groups are simultaneously selected for the same transmission from the dispatcher – but remain separate groups. Response from radio users is by group and only members of each unique groups are able to hear the response.
Multisite	A network of multiple sites in a system.

NCIC	National Crime Information Computer.
Noise	An unwanted signal or disturbance (e.g., static) in a radio communication system.
NPSPAC	National Public Safety Planning Advisory Committee that developed a plan for use of 821-824 and 866-869 MHz portion of band. Included in the plan is a channelization scheme.
Omnidirectional	Receiving or sending radio waves equally well in all directions.
Patch	This is a form of group regrouping which the joined groups are allowed to carry on normal message trunking operations between and among all the separate members groups of the call, upon a single channel resource. A feature which allows a console operator to connect a talkgroup(s) to a conventional group or another system of system resources.
Preferred Site	Determines which site a subscriber unit wants to be on when there are overlapping sites.
Operation Priority	Preassigned levels (up to 10) which determine the order in which users are assigned channels on a system. Emergency, if used, is the highest level of priority.
Priority Scan	Operation is determined by mode of operation. In conventional mode, system operated by sampling channels for activity and opening squelch to received messages. In trunked mode, the radio may receive audio for the groups programmed in the scan list (up to 10)
Propagation	The action of traveling and spreading through space, in reference to wave energy.
PTT	This acronym is short for "Push to Talk."
Rebanding	Moving of frequencies within the same band.
Receiver	The portion of a subscriber unit that converts the radio waves into audible signals.
Refarming	An administrative process being conducted by the FCC to reduce channel bandwidths and, as a result, promote spectrum efficiency.
Remote Site	In a simulcast system, the remote site repeater is configured the same as that of the prime site. The main difference between prime and remote sites is the fact that the repeater site is slaved to the prime site.
Repeater	A transmitter and a receiver operating on different frequencies and often connected to a common antenna. Mobile Relay
Selective (Radio) Inhibit	An important feature to public safety users which allows an operator to instantly and effectively "put to sleep" a mobile or portable unit in the field. Lost or stolen radios, over which sensitive communications could be heard, can be effectively silenced permanently by the operator. The target radio must be turned on and within system range in order for the feature to be effective.
Simplex	Transmitting and receiving on the same frequency. Direct radio or radio communications. Also known as Direct or Talkaround.
Simulcast	A wide are coverage system configuration which makes use of simultaneous transmission of the same information upon the same frequencies throughout a large coverage area; parameters of the transmitted information is matched for each repeater of a given frequency.
Site Controller	Computer system located at the site which controls all system activity, channel assignments, logging, supports test and alarm unit, and communicates to master site via dedicated T-1 line.
Skip	The phenomenon by which a radio wave reflects from the ionosphere during the height of the sunspot cycle, often resulting in sever interference problems.
Smartzone	Trunking system using multiple sites with variable number of repeaters. Currently

	what CCNC is using.
SMR	Special Mobile Radio. FCC classification used by entrepreneurial operators of 700/800 MHz trunked systems that service the business and industrial markets. Nextel uses.
Spectrum	The rage of electromagnetic signals in which radio transmission and detection techniques may be used.
Standalone Repeater	Base station designed to cover on geographical area with on frequency pair.
Status Messages	Use to communicate without voice to users or dispatchers.
Storm Plan Storm Plan Cont.	A contingency plan that may be used by trunked systems for special situations, like natural disasters. This feature allows the user to preset dynamic regrouping parameters for radios. By having this plan available to the system manager and terminals, emergency situations are more likes to be handled in a quicker and more logical manner.
Subscriber ID	Distinct number assigned to each subscriber unit allowing the subscriber unit to operate on the system. Also known as Individual ID or Radio ID. The Subscriber ID is transmitted at the beginning and end of each transmission and is logged by the Zone Controller.
Subscriber Unit	Individual serialized devices operating on the trunked system. Commonly referred to as radio, packset, portable, mobile, etc. system.
ID	This is the special identification upon the control channel to identify the particular trunking system using this control channel; this is used by the subscriber units to verify they are operating upon the correct trunking system; it is sent about every 3 seconds on the control channel.
System Management Terminal	Computer used for system configuration, dynamic reconfiguration, down load of data to/from site, analysis of logging information, and other managements tasks.
Talk-Around	Talk-Around by-passes the repeater and talks directly to another unit. Units in the talk-around mode are operating in a convention mode. See Simplex.
Talkgroup	A talkgroup is the primary level of organization of users on a trunked radio system. Talkgroup activity is not heard by other talkgroups. Often referred to as channel.
Talkgroup ID	A distinct number assigned to each talkgroup allowing it to operate on the system.
TDMA	Time Division Multiple Access. A method for improving spectrum efficiency in an existing channel by allocating specific time slots to each user.
Transmitter	The portion of a radio device that sends out the radio signal.
Trunking	The sharing of a number of talk paths among many users. A method by which multiple channels are accessed for user needs. Channel assignments are more efficient that systems where channel access is limited to a single channel or require manual user channel switching. Creates spectrum efficiency.
UHF	Ultra-High Frequency. The frequencies between 450 and 470 Megahertz.
VHF	Very High Frequency. The frequencies between 15 and 174 Megahertz.
Vocoder	Abbreviation for voice encoder/decoder, a circuit that samples a voice frequency and then changes the sampled information into binary digits to modulate the carrier and decodes the digital signal back to voice audio.
Voice Channel	In a trunked system, a Voice Channel is an RF channel that is an available voice communication channel resource. For example, a ten-channel trunked system has

	one control channel and nine voice channels.
Voting Voting Cont.	The process by which geographically separated receivers pass their received signals to a common point at which the signals are compared and only the best signal is passed on for use.
VOX	Voice Operated Transmit is a process for activating PTT by electronic recognition of a voice signal.
Working Channel	All repeater channels except the single control channel. Radios communicate in all modes via a working channel. Also known as a voice channel.
Yagi Antenna	A directional antenna that normally has a minimum front to back ratio of 20dB.
Zone Controller	Fault tolerant computer with hardware and software necessary to control the system.
Zone Watch	A diagnostic software tool used to monitor zone activity, providing real time display of all call activity as it occurs.