JOINT AGREEMENT

FOR THE OPERATION, MAINTENANCE AND FINANCIAL MANAGEMENT OF THE ORANGE COUNTY

800-MEGAHERTZ COUNTYWIDE COORDINATED COMMUNICATIONS SYSTEM

This agreement is entered into on _____, 2021, by and between the executing Partner agencies. This agreement replaces the 2005 Agreement as amended, and to the extent there is a conflict, this Agreement controls.

RECITALS:

Whereas, the Next Generation installation and implementation of the 800 MHz Countywide Coordinated Communications System (800 MHz CCCS) has been completed; and,

Whereas, the original Joint Agreement for the Operation, Operation Maintenance, and Financial Management of the Orange County 800 MHz Countywide Coordinated Communications System was executed September 19, 1995, and related Amendments Nos. 1, 2, 3, 4, 5, and appropriate change orders thereto followed (the “1995 Joint Agreement”), and;

Whereas, a subsequent Joint Agreement for the Operation, Operation Maintenance, and Financial Management of the Orange County 800 MHz Countywide Coordinated Communications System was executed in November 2005, and related Amendments Nos. 1 and appropriate change orders thereto followed (the “2005 Joint Agreement”), thereby superseding the original 1995 Joint Agreement, and;

Whereas, the Partner agencies now desire to execute a new Joint Agreement (the “2021 Joint Agreement”) to supersede all previous Joint Agreements; and,

Now, therefore, in consideration of the mutual covenants, conditions, agreements, and stipulations hereinafter expressed, the Partner agencies hereby agree as follows:

Contents

1.0 GENERAL

1.1 System

The 800 MHz Countywide Coordinated Communications System (800 MHz CCCS) will be referred to as the "System." The System shall be maintained by the Orange County Sheriff-Coroner Department's Technology Division (hereinafter referred to as "Lead Agency").

1.2 Definition of Terms

- "System" is defined as a multichannel digital trunked radio communications system enabling interoperability among all participating City and County law, fire, public works, and lifeguard/marine safety departments. The System components also include transmitting /receiving sites, microwave networks, IP networks, dispatch consoles, control stations, and field equipment (mobile and portable radios).

- "Governance Committee" is established by the Board of Supervisors and Partner Agencies to the Joint Agreement to facilitate the operation, maintenance, and financial management of the system. The Governance Committee is comprised of nine (9) members as identified in the Governance Committee Bylaws, attached hereto as Attachment A.

- "Governing Authorities" are the City Councils, the Orange County Board of Supervisors, and the Orange County Fire Authority Board of the Partner Agencies, responsible for approving certain substantive modifications or amendments to this agreement where such approval authority has not been expressly delegated to the Governance Committee.

- "Law Enforcement Agency" is defined as all governmental Law Enforcement Agencies operating primarily within the limits of Orange County, including, but not limited to: Orange County Sheriff-Coroner Department, Orange County City Police Departments, Orange County District Attorney's Office, and Orange County Probation Department.

- "Lead Agency" is designated to be the Orange County Sheriff's Department (OCSD) Technology Division that will be responsible to manage, maintain, and enhance the System and its respective Standard Operating Procedures (SOP).

- "Marine Safety" is defined as and shall include all governmental and private lifeguard agencies operating primarily within the limits of Orange County.

- "Member Agency" is defined as an agency authorized by the Governance Committee to use the System. Members include the Lead Agency and Partner Agencies.

- "Mobile Radio" is defined as two-way radio equipment installed in a vehicle to provide communications for the vehicle operator.

- "Mutual Aid Provider" is any governmental organization not otherwise defined in this Agreement that will provide short term assistance across jurisdictional boundaries during an emergency or planned event that exceeds local resources. Mutual aid use of the System will be restricted to the timeframe of the mutual aid incident.

- "New Partner Agency" are Partner Agencies added after the adoption of this Joint Agreement.

- "Parties" are all those entities that are authorized users of the System and have signed this agreement.

- "Partner Agency" are authorized subscribers to the system who agree to share in the System Operational Costs to administer, maintain, and upgrade the technology by providing recurring rate schedule payments.

- "Portable Radio" is a two-way radio equipment that is rechargeable, and handheld or belt carried.

- "Radio Site" is defined as a location, which consists of a building, systems within the building, and a tower.

- "Sponsored Agency" is any agency approved to use the System under sponsorship of a Partner Agency.

- "Sponsoring Partner Agency" is a Partner Agency that wishes to sponsor a Sponsored Agency.

- "Subscriber Unit" is defined as the subscriber radios and other devices that utilize the System. This includes dispatch operator positions, mobile radios, portable radios, cellular based devices and any other device that allows a user to communicate over the System.

- "System infrastructure" is defined as all associated radio and support equipment required to establish a radio network on which user radios can operate to communicate throughout the County of Orange. System infrastructure includes, but is not limited to, servers, switches, routers, data lines, base station radios, microwave technology, and firewalls.

- "System Operational Costs" are the expenses required to administer, maintain, and update the System.

- "System Modification" is any change in operational procedure or technology that requires alteration to the System.

- "System Subscriber Equipment" is defined as all equipment used to support user access to the System including Subscriber Units and other supporting equipment such as dispatch center console equipment, antennas, batteries, etc.

- "System User" is defined as an individual or agency authorized to access the System.

- "System Watch Network Operation Center" is a Lead Agency staffed support center responsible for the 24/7 support of the System. This includes but not limited to, live monitoring, notifications, troubleshooting, callouts, and repair.

- "Talkgroups" are used to identify groups of users who communicate together on a trunked radio system.

1.3 Amendment Process

The Governance Committee is authorized to make future updates, amendments, or modifications to the Agreement and its attachments without further action of the Governing Authorities, so long as the updates, amendments, or modifications to the Agreement and its attachments would result in minor, non-substantive changes that do not create or increase the financial obligations of the Partner Agencies. Where the Governance Committee is authorized to make such updates, amendments, or modification, such delegated authority shall be expressly granted in this agreement.

This agreement may also be amended or modified by the consent of all of the Governing Authorities representing the Partner Agencies.

1.4 Liability

Each Party of this Agreement (the "Indemnitor") shall indemnify, defend, and hold all other Parties, and their agents and employees (the "Indemnitees") harmless from all claims, liabilities, damages, and losses to the Indemnitees arising out of any acts or omissions of itself and its agents and employees in connection with the performance of this agreement which acts or omissions constitute gross negligence.

1.5 Withdrawal from System

Any Party may withdraw from this Agreement by serving written notice to the Governance Committee of their intent to withdraw. Due to the cost distribution model used to fund the operation of the System, any Party withdrawing from this Agreement will financially impact the remaining Parties. As such, Parties wishing to withdraw from this Agreement shall do the following:

1) Withdrawing Party provides written notice twelve months prior of withdrawal after meeting its financial obligations under this agreement.

2) Withdrawing Party will attend the Governance Committee meeting following their submittal to discuss withdrawal process.
3) Withdrawing Party will work with the Lead Agency to effect the withdrawal.
4) Withdrawing Party will make all Operational Cost payment obligations for the full fiscal year of the withdrawal.
5) Withdrawing Party will be responsible for all Lead Agency Costs associated with the withdrawal process.

Withdrawing Party will not be responsible for any financial obligations assumed by the other Partner agencies subsequent to withdrawal and upon fulfillment of existing financial obligations. Similarly, it is understood that the County of Orange has ownership of the System and certain sites as well as FCC licenses presently issued to the County, and upon any withdrawal by any Parties to the Agreement, any and all right, title, and interests in the System, those sites and FCC licenses shall remain with the County. Should the County of Orange wish to withdraw, an orderly transition to the remaining Parties must be affected.

2.0 GOVERNANCE COMMITTEE

2.1 Governance Committee Authority

The Governance Committee shall be governed in accordance with the Governance Committee Bylaws attached hereto as Attachment A. Any future updated revisions or amendments to the Governance Committee Bylaws shall be deemed adopted by this agreement without further action of the Governing Authorities.

2.2 Governance Committee Member Appointment

The Governance Committee shall be comprised of nine (9) members, as identified below. It will also be responsible for coordinating with their appropriate associations/agencies on issues involving the appropriate Governing Authorities approvals:

- Four City Managers appointed by the Orange County City Managers' Association
- Orange County Chief Executive Officer, or Designee
- Orange County Sheriff-Coroner, or Designee
- Orange County Public Works Deputy Director, or Designee
- Orange County Chief of Police & Sheriffs Association (OCCOPSA) Chief or Designee not from a city currently represented on the governance committee
- Orange County Fire Chiefs Association (OCFCA) Fire Chief or Designee not from a city currently represented on the governance committee

2.3 Governance Committee Purpose

The Governance Committee oversees all aspects of the implementation, operation, and fiscal management of the system, including but not limited to, the following:

- Approving System operational policies
- Addressing System operational issues

- Resolving operational policy or fiscal matter disputes of Partner Agencies.
- Addressing System facilities development
- Reviewing and approving modification and enhancement plans
- Approving contract pricing changes
- Approving Annual System Operational Budget and Cost Sharing Allocations.
- Approving 10 year capital plans and allocation of Reserve Fund for required upgrades.
- Approving New Partner Agencies.
- Approving Sponsored Agencies.

3.0 MEMBERS TO THE SYSTEM

Members are all agencies authorized by the Governance Committee to use the system and who have signed this agreement.

3.1 Lead Agency

The lead agency is designated to be the Orange County Sheriff's Department Technology Division and will manage, maintain, and enhance the system. Lead Agency is responsible for System Administration as outlined in Section 4 below.

3.2 Partner Agencies

Partner Agencies are authorized subscribers to the System who have signed this Joint Agreement or added as New Partner Agencies via the process outlined in 3.2.1 below. Partner agencies agree to share in the System Operational Costs and System Maintenance Costs as outlined in Section 5 below.

3.2.1 New Partner Agencies

Agencies that wish to become an authorized subscriber to the System may be added as a New Partner Agency via the following steps:

1) The prospective New Partner Agency submits an official request, in writing, to the Lead Agency requesting to join as a Partner Agency.
2) Lead Agency gathers additional information from requesting New Partner Agency to determine the feasibility of the request and the potential impact on the System operation and the existing Members.
3) The Lead Agency processes the request to obtain approval.
4) Lead Agency presents the request to the Governance Committee along with previous approvals from appropriate Governing Authorities. Governance Committee will determine final approval or denial of the request.
5) Once all approvals have been obtained, requesting New Partner Agency will execute a copy of this agreement along with the associated New Partner Agency forms identified in Attachment B.
6) The approved New Partner Agency will purchase necessary radio equipment and arrange to pay associated New Partner Agency costs described in in 5.2 below.

3.2.2 Sponsored Agencies

Partner Agencies may, with Lead Agency review and Governance Committee Approval, sponsor non-partner agencies to participate in the system.

3.2.2.1 Sponsored Agencies Approval Process:

1) Sponsoring Partner Agency submits to the Lead Agency an official written request to add a Sponsored Agency.

2) Lead Agency gathers relevant information from Sponsoring Partner Agency to determine the feasibility of the request and the potential impact on the System Operation and the existing Members.

3) Lead Agency reviews all available information to determine the feasibility of the request to add the Sponsored Agency. Lead Agency shall work with the Sponsoring Partner Agency to determine the additional costs to the Sponsoring Partner Agency.

4). Lead Agency presents the request to the Governance Committee at a Governance Committee Meeting. Governance Committee shall approve or deny the addition of the Sponsored Agency.

3.2.2.2 Sponsored Agency Access and Limitations

Sponsored Agencies are only allowed access to use the common talkgroups/channels and select agency specific talkgroups/channels of the sponsoring Partner Agency, as recommended by the Lead Agency and approved by the Governance Committee. Sponsored Agencies do not have a role in defining the operation of the System. The inclusion or exclusion of Sponsored Agencies in the System will be determined by the Governance Committee and will be reviewed annually or as needed. Partner Agencies shall be responsible for any System use by a Sponsored Agency. Sponsored Agencies must use the same common talkgroups as the sponsoring Partner Agency.

3.2.2.3. Sponsored Agency Financial Responsibilities

Sponsored Agency financial responsibilities are outlined in section 5.2.4 below.

3.3 Mutual Aid Agencies

Certain governmental agencies may, with Lead Agency review and Governance Committee Approval, be granted access to the System for the express purpose of providing mutual aid to Partner Agencies. Mutual Aid agencies are limited to and identified within ATTACHMENT C

3.3.1 Mutual Aid Agency Approval Process:

1) Any Partner Agency may submit to the Lead Agency an official written request to add a Mutual Aid Agency.

2) Lead Agency gathers relevant information to determine the feasibility of the request and the potential benefit to existing Partner Agencies and overall public safety in Orange County.

4) Lead Agency presents the request to the Governance Committtee at a Governance Committee meeting. The Governance Committee shall approve or disapprove the addition of the Mutual Aid Agency.

3.3.2 Mutual Aid Agency Access and Limitations

Mutual Aid Agencies are only allowed access to use the common talkgroups/channels and the mutual aid channels associated with other systems that are included in our radio programming. Mutual Aid Agency use of the System is restricted to the actual duration of a mutual aid incident. Mutual Aid Agencies do not have a role in defining the operation of the System. The inclusion or exclusion of Mutual Aid Agencies in the System will be determined by the Governance Committee and will be reviewed annually or as needed.

3.3.3 Mutual Aid Agency Financial Responsiblities

Mutual Aid Agency financial responsibilities are outlined in section 5.2.5 below.

4.0 SYSTEM ADMINISTRATION

The Lead Agency shall have the authority and responsibility to maintain the proper operation of the System. The Lead Agency shall be responsible for maintaining, managing, and operating the System, which includes staffing the System Watch Network Operations Center on a continual basis (e.g., 24x7x365), assuring the seamless operation of the System.

4.1 System Equipment

The Lead Agency shall approve and evaluate all equipment and new technology for use with the system to ensure that it meets the requisite technical standards and requirements. Approved equipment must meet the standards set by the Federal Communication Commission as well as any Federal, State, and Local Laws.

4.2 System Subscriber Equipment

Each Member Agency is responsible for the maintenance, management, and operation of its System Subscriber Equipment. A Member Agency may establish a System Subscriber Equipment maintenance contract with the Lead Agency.

Prior to making any modifications to System Subscriber Equipment, including but not limited to adding radios or alteration to dispatch center equipment, Member Agencies must request such modifications to be reviewed and approved by the Lead Agency as outlined in section 4.4.

4.3 Dispatch Centers

Member Agencies may operate their own Dispatch Centers at their discretion. Individual Member Agencies that manage their own Dispatch Centers shall be responsible for the day to day maintenance, management, and operation of those Dispatch Centers, equipment and associated facilities. Day to day dispatch operations and protocols shall be left to the individual Members

Agencies. The Lead Agency will not be responsible for the maintenance or management of Members Agencies' individual Dispatch Centers unless a Member User contracts with the Lead Agency for maintenance, management, or operations.

4.3.1 Dispatch Center Equipment

Dispatch Center Equipment must meet the technical standards as outlined in Section 4.1.

4.3.1.1 Dispatch Center Required Equipment Upgrades

The Governance Committee may mandate equipment upgrades for Member Agencies Dispatch Center Equipment. If the Governance Committee mandates an Equipment Upgrade to Members Agencies' Dispatch Center Equipment, then the Members Agencies must upgrade their equipment as directed by the Governance Committee.

4.3.1.2 Dispatch Center Non-Required Equipment Upgrades

Members Agencies may upgrade their Dispatch Center equipment and associated facilities at their own cost without coordination with the Lead Agency so long as the upgrade will not adversely affect the System itself. However, Member Agencies must coordinate with the Lead Agency as outlined in the System Modifications section 4.4, below, when upgrading or modifying any Dispatch Center equipment vital to the operation of the System. Dispatch Center Equipment modification requiring coordination with the Lead Agency includes, but is not limited to: computer equipment, software, consoles, routers, switches, gateways, firewalls, control stations, and antenna systems.

4.4 System Modifications

The System will require occasional routine modifications, which shall be conducted as outlined in this section.

4.4.1 System Modifications requiring Governance Committee Approval

The following System Modifications require the pre-approval of the Governance Committee, as outlined in the Governance Committee By-Laws:

A. Addition of any New Member Agencies to the System.

B. Any modification that adds a financial burden shared by the Member Agencies.

C. Any modification that would affect a System User other than the requesting Member Agency.

The Lead Agency is required to provide a report and recommendation to the Governance Committee on any proposed System Modification that requires Governance Committee approval. The Lead Agency report and recommendation must provide a financial analysis of the System Modification, if appropriate, and an estimated timeline to complete the System Modification.

The Lead Agency is responsible for implementing any Governance Committee approved modification.

4.4.2 System Modification by Lead Agency

The Lead Agency is authorized to perform System Modifications, as necessary. The Lead Agency has the discretion to implement System Modifications without prior Governance Committee Approval, so long as the modification does not require Governance Committee approval as listed in Section 4.4.1 of this agreement, and does not cause unanticipated or unbudgeted costs to Member Agencies.

4.4.3 System Modifications requested by Partners Agencies

Partner Agencies may request system modifications. System Modification requests from Partner Agencies must be submitted in writing to the Lead Agency for review and approval.

If the Lead Agency grants a Partner Agency modification request, and the request does not require Governance Committee Approval as outlined in Section 4.4.1, then the Lead Agency shall provide the Partner Agency with a formal approval, including all costs of the requested modification. If a Member Agency agrees with the official permission, the Member Agency may request the Lead Agency to implement the System Modification. Any and all costs associated with implementing the System Modification will be the sole responsibility of the System User requesting the modification.

If a Member Agency modification request requires Governance Committee approval per Section 4.4.1 above, then the Lead Agency and the Member Agency requesting the modification shall present the modification request to the Governance Committee for approval. The modification request shall include the reason for the modification, the Lead Agency's recommendation and cost analysis of implementing the modification.

4.4.4 Appeal of Modification Request Denial

If the Lead Agency denies a Member Agency's modification request, the Lead Agency shall provide the Member Agency, in writing, the reasons for the denial. Members Agencies may submit a written appeal of the decision of the Lead Agency to the Governance Committee within 90 days of the denial notification. The Lead Agency will ensure the appeal is added to the next Governance Committee meeting agenda for action.

4.4.5 Notification of System Modifications to Governance Committee

Lead agency is required to provide a list of implemented, pending and requested System Modifications at each Governance Committee Meeting.

4.5 Security

The Lead agency has in place a Security Plan for the System (Attached as Attachment D.) Member Agencies and System Users are required to protect the security of the System as set forth in the Security Plan.

System Users are required to contact System Watch for any actual or potential security breach to the System as soon as the actual or potential security threat is known. The Lead Agency must evaluate any reported security breaches and is authorized to implement measures to remediate the

security breach. If appropriate, the Lead Agency shall inform the Governance Committee of any reported breach and steps taken to remediate.

4.6 Maintenance & Service Contracts

Within approved and adopted budget, the Lead Agency is authorized to enter into contracts with vendors as needed for the ongoing execution of this agreement. Such contracts include, but are not limited to, the purchase or lease of equipment, installation of equipment, service and/or maintenance of equipment, and System upgrades. All contracts shall comply with applicable law and purchasing policies and guidelines. Appropriate shared costs will be included in System Operational Costs cost-sharing allocations. The Lead Agency shall negotiate and enter into contracts with vendors as intended in this agreement and shall make payments due and payable under such contracts on behalf of the parties.

The Lead Agency will serve as an administrative liaison between the other Member Agencies and the contracted vendors.

4.7 System Standard Operating Procedures

The Lead Agency is responsible for the development and maintenance of the Standard Operating Procedures ("SOP") (Attachment E) for the system. The Lead Agency shall coordinate with System Users, including but not limited to Law Enforcement, Fire Services, Marine Safety, and Public Works in developing and updating the SOP. The SOP, and any amendments to the SOP, must be approved by the Governance Committee. All Member Agencies must follow the SOP and any amendments to the SOP once approved by the Governance Committee.

4.8 Partner Agency Operational Policies and Procedures

Member Agencies must inform the Lead Agency of any changes to their operational policy or procedures, in writing and prior to any implementation of such changes, if the change of operational policy or procedure affects or may affect the System. The Lead Agency will work with Member Agencies to ensure that operational policies and procedures are compatible with the System. The Lead Agency shall work collaboratively with Member Agencies to settle any disputes regarding Member Agency Operational Policies and Procedures. The Lead Agency shall bring any dispute to Member Agency Operational Policies and Procedures to the Governance Committee for review and resolution if a dispute cannot be resolved between the Lead Agency and the Member Agency.

5.0 FINANCIAL ADMINISTRATION

5.1 Governance Committee Financial Authority

The Governance Committee shall have the authority to allocate available budgeted funds as they deem appropriate for the operation, maintenance, and management of the system. Governance Committee has the authority to approve the System Operations Budget, set rates and fees, and approve use of the Reserve Fund for necessary expenditures and upgrades. Governance Committee has the authority to approve capital expenditure funding and approved sources of the reserve fund.

5.2 Partner Agencies Financial Obligations

Partner Agencies and New Partner Agencies are responsible for certain financial obligations including, but not limited to, the following.

5.2.1 System Operational Costs

All Partner Agencies shall contribute to the System Operational Costs via the Systems Operations Budget and administered as described in section 5.3 below.

5.2.2 System Entry Fees/Upgrade Fees

Some Partner Agencies must pay System Entry Fees when they enter/register a radio into the System for activation based on the System Entry Fee established by the Governance Committee. The Lead Agency shall submit their recommendation of the System Entry Fees for Governance Committee approval at the same time the System Operations Budget (Section 5.3) is submitted for approval annually.

The System Entry Fees are necessary to recoup/offset costs that were required during the previous System upgrade Partner Agencies that financially contributed to the previous System Upgrade are not required to pay System Entry Fees. Legacy Partner Agencies that are not required to pay System Entry Fees are listed in attachment C. Partner Agencies not listed in attachment C and any New Partner Agencies are required to pay the System Entry Fee for each radio they add to the System.

System Entry Fees are billed on a per radio basis. The Lead Agency shall invoice the Partner Agency or New Partner Agency for any System Entry Fees at the approved per radio rate when a new radio is entered into the System on behalf of that Partner or New Partner.

System Entry fees shall be deposited into the Reserve Fund as outlined in section 5.6 below.

Over-the-air upgrade programming of radio equipment will not be charged and limited to two annually per Member Agency. Any additional upgrades past the two annually will incur a cost.

5.2.3 Miscellaneous Rates and fees

As stated in 5.1 above, the Governance Committee has authority to set rates and fees as necessary. The Lead Agency may charge Partner Agencies and New Partner Agencies via invoice. Partner Agencies shall pay invoice within thirty (60) days of the date of the invoice.

Governance Committee shall set any Miscellaneous Rates and Fees annually. Lead Agency shall submit their recommendation for Miscellaneous Rates and Fees at the same time they submit the System Operations Budget (Section 5.3) for approval.

5.2.4 Mutual Aid Agencies

Mutual Aid Agencies are not authorized to use the System for day-to-day communications but are limited to use of the System only when providing emergency assistance to Partner Agencies. As such, Mutual Aid Agencies are not included in the System Operations cost share calculations or System Entry Fees. Mutual Aid Agency equipment and programming costs will be the responsibility of the Mutual Aid Agency.

5.2.4 Sponsored Agencies

The sponsoring Partner Agency is responsible for the costs, rates, and fees of any Sponsored Agency it sponsors on the System, unless otherwise approved by the Governance Committee. System Entry Fees per 5.2.2 above shall not apply to System Subscriber equipment for a Sponsored Agency.

5.3 System Operations Budget

The Lead Agency will submit the proposed System Operations Budget for approval to the Governance Committee no later than one hundred and twenty (120) days prior to the beginning of the fiscal year. Governance Committee shall be responsible for approving the System Operation Budget no later than ninety (90) days prior to the fiscal year.

5.3.1 Partner Agency Cost

The Lead Agency shall submit the Partner Agency Cost Share to the Governance Committee along with the System Operations Budget in 5.2 above. The Governance Committee shall be responsible for approving the Partner Agency Cost Share, along with the System Operations Budget.

Partner Agency Cost Share shall be calculated based on the number of Subscriber Units each agency operates on the System as a percentage of the total number of Subscriber Units operating on the System. This will determine the agency's share of the annual System Operations Budget.

5.3.2 Payment Remittance

Partner Agencies are required to remit payments to the Lead Agency for their contribution for use of the System. The Lead Agency shall invoice Partner Agencies quarterly. Lead Agency shall issue invoices no later than thirty (30) days after the beginning of each quarter. Partner Agencies shall pay invoice within thirty (30) days of the date of the invoice.

5.4 Year End Settlement

At the end of each fiscal year, the Lead Agency shall submit a financial review with the actual System Operational Costs from the previous fiscal year to the Governance Committee. The findings of the financial review shall be reported in writing to the Partner Agencies on the system. Thereafter, to the extent there have been contributions made by the Partner Agencies which exceed the actual System Operations Costs, the number of said excess contributions shall be deposited into the Reserve Fund (see 5.5), unless the Governance Committee deems otherwise. In the event of a shortfall, each Partner Agency shall be billed its pro-rata share of the shortfall, which shall be paid in the first quarter payment for the next fiscal year following the fiscal year of the shortfall.

5.5 Ten-Year Plan

The Governance Committee, in conjunction with the Lead Agency, will be responsible for evaluating and planning for future upgrades. Doing so will ensure the continued structural

integrity of System equipment and Sites and any necessary maintenance or repairs, and allocating for unforeseen events which may lead to additional expenses outside of the standard operational costs. Such items will be defined within a Ten-Year Plan, which will be presented to and approved annually by the Governance Committee.

The Lead Agency shall submit an updated Ten-Year Plan to the Governance Committee annually for review and approval.

5.6 Reserve Fund

The Governance Committee shall review and approve a long-term financial plan to ensure funds are available for the System's capital needs as defined in the annually updated Ten-Year Plan, as well as for any unforeseen emergency expenses. A Reserve Fund has been established to ensure adequate funds are available for ongoing maintenance, upgrades, and unforeseen expenses which may arise outside of operational costs.

5.6.1 The Reserve Fund shall be funded in the following manner:

5.6.1.1 Contributions by Partner Agencies

The Partner Agencies are responsible for providing funds for deposit to the Reserve Fund. The Lead Agency shall submit the cost of each Partner Agency along with the Fiscal Year Budget described in section 5.3. The Governance Committee shall approve the Reserve Fund contributions as part of the annual budget review and adoption process.

5.6.1.2 System Entry Fees

All System Entry Fees collected per 5.2.2 of this Agreement shall be deposited into the Reserve Fund.

5.6.1.3 System Operation Budget Surplus

In the event of a System Operation Budget Surplus at the Year-End Settlement, that System Operation Budget Surplus shall be deposited into the Reserve Fund.

5.7 System Modification Cost

Any costs associated with System Modifications shall be addressed as outlined is section 4.4 of this agreement.

IN WITNESS WHEREOF, the Partner agencies hereto have set their hands and seals on the date set forth opposite their respective signatures on identical counterparts of this instrument, each which shall for all purposes be deemed an original thereof.

COUNTY OF ORANGE

By: _____

Board of Supervisors

Dated: _____

Approved As to Form:

County Counsel

_____

CITY OF: _____

ATTEST:

By: _____

By: _____

_____

City Clerk

Dated: _____

Approved As to Form:

City Attorney

_____

By: _____

Chairman

Dated: _____

ATTEST:

_____

Clerk of the Authority

ORANGE COUNTY AGENCY

APPROVED AS TO FORM:

By: _____

Authority Counsel

Dated: _____

By: _____

Chairman

Dated: _____

ATTEST:

_____

Clerk of the Authority

ATTEST:

_____

Clerk of the Authority

APPROVED AS TO FORM:

By: _____

Authority Counsel

Dated: _____

APPROVED AS TO FORM:

By: _____

Authority Counsel

Dated: _____

BYLAWS
800 MHz GOVERNANCE COMMITTEE

Article 1 Name

Section 1. The name of this body is the 800 MHz GOVERNANCE COMMITTEE, hereinafter referred to as the "Governance Committee."

Article 2. Purpose and Authority

Section 1. It is the purpose of the Committee to oversee implementation and operation of the 800 MHz Countywide Coordinated Communications System (the "System"), including Member Agency compliance with payment schedules, addressing operational issues affecting System operation and site development, reviewing and approving conversion, modification and enhancement plans, approving contract pricing changes, resolving disputes between Member Agencies, operational and fiscal matters necessary for the operation and maintenance of the System, and performing any other responsibilities required to implement the Joint Agreement. The Governance Committee shall be responsible for approving the 800 MHz Project System Operations Budget operating and Reserve Fund that are jointly funded by the Parties to the Joint Agreement.

Section 2. The Governance Committee was established November 23, 2004, and amended June 2, 2015, by the Orange County Board of Supervisors (the "Board") and Parties to the Joint Agreement to facilitate the operation, maintenance and financial management of the 800 MHz CCCS.

Section 3. This Governance Committee will operate under the revised Board authorization of the re-written Joint Agreement to facilitate the operation, maintenance, and financial management of the 800 MHz CCCS established on _____

Article 3. General Operating Mandated Regulations and Statutes

Section 1. The Governance Committee must adhere to all local, state and federal regulations and statutes that may, from time to time, apply.

Section 2. The Committee shall be subject to the provisions of The Brown Act (commencing with Section 54950 of the Government Code) relating to public meetings of local governmental advisory boards.

Section 3. The Governance Committee must comply with the County's non-discrimination and zero tolerance sexual harassment policies.

Section 4. The Governance Committee must comply with the County's Code of Ethics, which outlines the County's clear expectations for behavior in relation to the members' duties as public servants.

Section 5. The Governance Committee shall operate strictly within its designated purpose.

Article 4. Membership and Term of Office

Section 1. Appointment. The Committee shall be comprised of nine (9) members, as identified below, and will also be responsible for coordinating with their appropriate associations/agencies on issues involving the appropriate Governing Authorities approvals:

- Four City Managers appointed by the Orange County City Managers' Association
- County Executive Officer, County of Orange, or Designee
- Sheriff-Coroner, or Designee
- Orange County Public Works Resources and Development Management Department Director, or Designee
- Orange County Chief of Police & Sheriffs Association (OCCOPSA) Executive Director, or Designee
- Orange County Fire Chiefs Association (OCFCA) Fire Chief or Designee

Each member must designate and name an alternate as a voting member if member cannot attend.

Section 2. Terms. Committee members shall be appointed for a two (2) year term. Members may serve for multiple additional two (2) year terms upon reappointment to each new term in accordance with Article 4, Section 1 above.

Section 3. Removal. The Governance Committee, by majority vote, may remove members of the Committee any time without cause. In addition, if a committee member misses three (3) consecutive Governance Committee meetings (whether regular or special meetings), said Governance Committee member will be deemed automatically removed without further Governance Committee action.

Section 4. Vacancies. A vacancy on the Governance Committee shall be filled by majority vote of the Governance Committee in accordance with Article 4, Section 1 above. Such vacancy should, if possible, be filled within 30 days of vacancy.

Article 5. Meetings

Section 1. Regular meetings shall be held on a quarterly basis. Governance Committee meetings shall be fixed on the first month of each quarter (January, April, July, and

October) on the fourth Wednesday at 1:30 PM unless a majority of the Committee members determine that an alternate fixed meeting day and time within the designated months is required to maximize member attendance. At least 72-hours prior to a regular meeting, an agenda shall be posted that contains a brief general description of each item to be covered in the meeting.

Section 2. Special meetings may be held on 24-hour public notice, including a binding agenda with brief general description of items to be covered at the meeting. Any special meeting notice must be publicly posted in accordance with all applicable laws and must be received by Committee members at least 24 hours in advance (Government Code Section 54956).

Section 3 A majority five (5) of the members shall constitute a quorum to conduct business.

Section 4. Only Governance Committee members may vote on items on the Agenda and each member may have only one vote.

Section 5. Governance Committee meetings may be rescheduled or canceled in accordance with the Brown Act. Orange County Sheriff Technology staff shall act as the Clerk of the Board for meeting rescheduling purposes.

Article 6. Officers

Section 1. The officers shall consist of a Chairperson and Vice Chairperson. The elected Chairperson shall conduct the meetings.

Section 2. The elected Vice Chairperson shall conduct regular Governance Committee meetings in the absence of the Chairperson; and do everything necessary to assist the Chairperson in related duties. In the event that both the Chairperson and the Vice Chairperson are absent from the same committee meeting, the remaining Governance Committee members present may appoint one of them to be the Chairperson for that meeting.

Section 3. Elections for Chairperson and Vice Chairperson shall be conducted by the full Governance Committee and shall occur in April of each year. The Chairperson shall call for nominations from the Governance Committee members and the Chairperson will initiate a vote. A majority vote of the Committee members present is required for each candidate to be elected as Chairperson and Vice Chairperson.

Article 7. Staffing

Section 1. Orange County Sheriff Technology staff secretary will provide secretarial support to the Governance Committee. Orange County Sheriff Technology staff secretary shall prepare and publish the Committee's agenda for each meeting. Orange County

Sheriff Technology staff shall call for attendance at the beginning of each meeting, keep the minutes, and perform other clerical duties as appropriate to the position. He/she shall retain the attendance records including the minutes.

Article 8. Compensation

Section 1. Governance Committee members shall receive no compensation for their service.

Article 9. Amendments. Review, Dissolution and Effective Date

Section 1. This Committee will operate as established by the Board of Supervisors on November 23, 2004 and revised by the Board of Supervisors in _____, 2021

Section 2. These Bylaws shall supersede all previous Bylaws and shall become effective on upon the approval of the Board of Supervisors.

Section 3. These Bylaws shall remain in effect until amended, revised or terminated by the Board of Supervisors and Parties to the Joint Agreement.

Section 4. The Board of Supervisors and Parties to the Joint Agreement may make amendments to the Bylaws at any time.

Section 5. This Governance Committee can be terminated at any time, without cause, by action of the Board of Supervisors and Parties to the Joint Agreement.

Project No:
Project Name:
Project Location:

NEW PARTNER AGENCY RIDER TO JOINT AGREEMENT FOR THE OPERATION, MAINTENANCE AND FINANCIAL MANAGEMENT OF THE ORANGE COUNTY 800 MEGAHERTZ COUNTYWIDE COORDINATED COMMUNICATIONS SYSTEM

This New Partner Agency Rider (**"NPA Rider"**) is entered into on _____, (**"Effective Date"**), by and between _____ (hereinafter referred to as **"NEW PARTNER AGENCY"**) and the Orange County 800 Megahertz Countywide Coordinated Communications System Governance Committee (hereinafter referred to as "**GOVERNANCE COMMITTEE).** For the purposes of this agreement, the GOVERNANCE COMMITTEE represents the Partners (hereinafter referred to as "**JOINT AGREEMENT PARTNERS**") of the Joint Agreement for the Operation, Maintenance and Financial Management of the Orange County 800 Megahertz Countywide Coordination Communications System (hereinafter referred to as **"JOINT AGREEMENT"**) (Section 1.4.1 of the JOINT AGREEMENT). GOVERNANCE COMMITTEE and NEW PARTNER AGENCY may be referred to individually herein as a "**Partner"** or collectively as the **"Partners."**

RECITALS

I. WHEREAS, JOINT AGREEMENT PARTNERS entered into the JOINT AGREEMENT in 2020; and,

II. WHEREAS, NEW PARTNER AGENCY, executed a copy of the JOINT AGREEMENT in accordance with Section 3.2.1 of the JOINT AGREEMENT on _____; and,

III. WHEREAS, NEW PARTNER AGENCY executed a copy of the New Partner Agency Agreement per Section 3.2.1 of the JOINT AGREEMENT on _____; and,

IV. WHEREAS, Section 2.1,"Governance Committee Authority", and Section 3.2.1, "Adding New Partner Agencies", of the JOINT AGREEMENT grants the GOVERANANCE COMMITTEE the authority to enter into a separate agreement with NEW PARTNER AGENCY to establish additional terms, conditions, and costs for entry into the Countywide Coordinated Communications System (the "CCCS"); and,

V. WHEREAS, the JOINT AGREEMENT in Section 1.4 "Liability" provides for indemnification only between those Partners listed in Exhibit A of the JOINT AGREEMENT (and would not include NEW PARTNER AGENCY); and,

VI. WHEREAS, Section 1.4.1 of the JOINT AGREEMENT, "New Agency Liability Rider", grants the GOVERNANCE COMMITTEE the authority to enter into a Liability Rider that shall, for all intents and purposes, make the NEW PARTNER AGENCY, a Partner in Section 1.4.

VII. WHEREAS, the GOVERNANCE COMMITTEE and NEW PARTNER AGENCY now desire to enter into a separate agreement (this NPA Rider) to establish additional terms and conditions by including NEW PARTNER AGENCY in the indemnity provision of the JOINT AGREEMENT per Section 1.4;

NOW THEREFORE, in consideration of the Recitals above, the receipt of which the Partners acknowledge herein, and which are incorporated herein by this reference, and the mutual covenants and agreements hereinafter contained, the GOVERNANCE COMMITTEE and NEW PARTNER AGENCY do hereby agree as follows:

A. NEW PARTNER AGENCY LIABILITY.

NEW PARTNER AGENCY shall now be included as a Partner as stated in Section 1.4 of the JOINT AGREEMENT.

Except as otherwise expressly set forth herein, all terms and conditions contained in the JOINT AGREEMENT, including any amendments/modifications, are hereby incorporated herein by this reference as if fully set forth herein and shall remain in full force and effect.

THE REMAINDER OF THIS PAGE WAS INTENTIONALLY LEFT BLANK

IN WITNESS WHEREOF, the Partners have executed this New Partner Agency Rider on the day and year first written above.

GOVERNANCE COMMITTEE	**NEW PARTNER AGENCY**
By: _____	By: _____
Date: _____	Date: _____

A. LEGACY PARTNER AGENCIES – Partner Agencies that financially contributed to the previous System Upgrade:

Aliso Viejo, Anaheim, Brea, Buena Park, Costa Mesa, Cypress, Dana Point, Fountain Valley, Fullerton, Garden Grove, Huntington Beach, Irvine, La Habra, La Palma, Laguna Beach, Laguna Hills, Laguna Niguel, Laguna Woods, Lake Forest, Los Alamitos, Metronet, Mission Viejo, Newport Beach, Orange, Placentia, Rancho Santa Margarita, San Clemente, San Juan Capistrano, Santa Ana, Seal Beach, Stanton, Tustin, Villa Park, West-Comm, Westminster, Yorba Linda, Orange County Fire Authority, CEO, District Attorney, Health Care Agency, John Wayne Airport, Animal Control, OC Lifeguard, OC Parks, OC Waste & Recycling, OC Public Works, Probation, OC Sheriff, Social Services Agency, Orange County Transportation District, Irvine Valley College Police, Santa Ana Unified School District Police, Saddleback College Police

B. MUTUAL AID AGENCIES

ATF, CA State Parks, California Corrections & Rehabilitation, CHP, Downey Fire, Lake Mission Viejo LG, Loaners, Long Beach Fire, Long Beach PD, Los Alamitos Armed Forces Reserve, LA County Fire, LA Sheriff, San Diego Sheriff Aviation, Santa Fe Springs Fire, Signal Hill PD, DOJ, UCI Irvine, US Marshals, USMC Camp Pendleton Fire

COUNTY OF ORANGE
CALIFORNIA

800 MHz CCCS

(Countywide Coordinate Communications System)

STANDARD OPERATING PROCEDURES

PREPARED AND DISTRIBUTED BY:

ORANGE COUNTY
LEAD AGENCY

January 2021

Table of Contents

1.0 INTRODUCTION

The 800 MHz Countywide Coordinated Communications System (CCCS) Standard Operating Procedures (SOP) provides National Incident Management System (NIMS) compliant procedures that are applicable to multi-agency, multi-discipline, all-hazard responses throughout the County of Orange. This SOP ensures consistent protocols and formalizes the operation and usage of the 800 MHz Radio System (System). This SOP will be utilized by CCCS emergency response and support personnel, communications operational and technical personnel, local/State/Federal government representatives, non-governmental organizations, and other System users as authorized by 800 MHz CCCS Governance Committee.

All System users shall comply with this SOP.

2.0 PURPOSE

The System is an 800 MHz trunked simulcast radio communications system designed to meet the needs of Orange County law enforcement, fire, lifeguard and public works responders and any other authorized users who are supporting these services.

This SOP addresses procedural and operational aspects of the System to include:

- Operational guidelines.
- Technology specifications and requirements.
- Usage guidelines.
- Training and exercises.
- Maintenance and repair.

2.1 Governance

The CCCS is governed by the 800 MHz CCCS Governance Committee which was established November 23, 2004 and amended June 2, 2015, by the Orange County Board of Supervisors and Parties to the Joint Agreement to facilitate the operation, maintenance and financial management of the 800 MHz CCCS. The Governance Committee is comprised of nine members including four City Managers, and designees from the County Executive Officer, Sheriff-Coroner, Public Works Director, Orange County Chiefs' of Police & Sheriff's Association and Orange County Fire Chief's Association. The Governance Committee responsibilities include the establishment and enforcement of these Standard Operating Procedures.

Additional information on the 800 MHz CCCS Governance Committee membership and responsibilities are documented in the 800 MHz CCCS Governance Committee Bylaws.

2.2 Users Group

The 800 MHz CCCS Users Group meetings occur once each quarter. The Users Group meetings allow for the sharing of information from the Lead Agency (Orange County Sheriff's Department Technology Division) regarding the System operations and any upgrade or enhancement projects proposed or in progress. These meetings also allow for Partner Agencies to discuss current concerns or provide input regarding future enhancements. All Partner Agencies are welcome to participate in the quarterly 800 MHz Users Group meetings.

2.3 800 MHz CCCS Radio System

The 800 MHz CCCS Radio System (System) is an advanced digital radio communications system built to the Association of Public-Safety Communications Officials (APCO) Project 25 (P25) digital radio standards. The System utilizes radio frequencies in the 800 MHz radio spectrum under the rules and regulations of the Federal Communications Commission (FCC). The System consists of the following major components:

- Radio Communications sites located throughout the County (towers, equipment shelters, generators & site security).
- Radio infrastructure (transmitters, receivers, combiners, antennas, etc).
- Radio spectrum in the 800 MHz frequency band and microwave radio frequency spectrum.
- Microwave radio links between the radio sites and the Loma Ridge Master Site.
- Subscriber Units (mobile radios, portable radios, control stations, dispatch consoles).
- System Watch Network Operations Center (NOC).

The System is designed to provide 95% portable radio coverage, 95% of the time within the Orange County operating area.

2.4 Eligible Users

The primary purpose for the System is to support Orange County public-safety and local government agencies' day-to-day operations by providing dependable, interoperable radio communication. Orange County public safety and local government agencies as well as applicable State and Federal government agencies may be eligible for access to the System. System access will be determined by the 800 MHz CCCS Governance Committee in compliance with the 800 MHz CCCS Joint Agreement and with consideration of System capacity.

2.5 Acceptable Usage / Radio Discipline

All System users shall follow these policies.

The System is to be used for day-to-day operations, emergency response calls, incidents, missions and disasters. The System may also be utilized for planned events, training and exercises with consideration of channel capacity and available talkgroups.

This policy clearly defines the discipline for agencies and individuals to follow when using radios on the System. Each Agency is responsible for ensuring their users adhere to proper radio discipline.

Misuse of the System shall be reported to the Lead Agency Director to handle directly with the Department Head of the agency involved. The reporting party's contact information should be provided in the notification. No profanity, playing music, personal conversations or activities not directly related to agency business will be permitted on the System.

All agencies and individuals shall utilize these communications resources professionally and keep radio conversations as concise as possible.

All agencies and individuals utilizing the System must abide by all FCC regulations as stated in Title 47 Part 90 Land Mobile Communications.

3.0 SCOPE

This SOP applies to the operational, technical and usage aspects of the System. It is therefore applicable to any user of the System, and applies to government agencies at the local, County, State and Federal levels, as well as authorized non-government users.

3.1 SOP Approval

This SOP and subsequent revisions require approval of the 800 MHz CCCS Governance Committee after review by the Lead Agency.

3.2 SOP Change Process

Annual Review Requirement

The SOP will be reviewed on an annual basis to assess the need for updates or revisions. The Lead Agency Director or designee will be assigned the task of reviewing the SOP, identifying applicable updates, and submitting a draft of the revised SOP for Governance Committee approval.

Operational Context

The 800 MHz CCCS Governance Committee is charged with approving standards, protocols and procedures for optimal operations between and among the users of the System.

Submitting Change Requests

Requests to delete, add, and/or change adopted standards, policies and/or procedures may be submitted in writing to the Governance Committee at any time. If the requested change is time critical, the Governance Committee may direct a request for immediate consideration to the Lead Agency Director.

Change Request Contents

A written request for any change to the SOP submitted to the Governance Committee shall include:

- A full description of the deletion, addition, or change including section and subsection references.
- The reason for the change (including the potential consequences if the request is not approved).

- A preliminary assessment of impact on other System users and an estimate of associated costs, if any.

The Governance Committee may direct the Lead Agency Director to conduct an assessment to address:

- Technical impact to current and future System performance including which system or subsystems will be or may be affected.
- Operational impact to current and future system performance including effects on System capacity and determination of those systems or subsystems that will be or may be affected.
- Degree of conformance with Governance Committee approved plans and standards.
- Cost impact to current participants.
- Potential alternatives.

The Lead Agency Director shall forward the completed assessment to the Governance Committee along with recommendations including strategies to mitigate negative impacts, if appropriate.

The Governance Committee shall notify all agencies of all requests along with potential impact and invite their comments.

The Governance Committee will approve, deny, or modify the requested SOP change.

If approved, the Governance Committee will incorporate the applicable SOP modifications and inform System users.

Management of Change Process

The Governance Committee Chair will manage this process.

4.0 RADIO SYSTEM MANAGEMENT

4.1 Radio System Architecture

The System is an advanced digital radio communications system built to the Association of Public-Safety Communications Officials (APCO) Project 25 (P25) digital radio standards. The P25 System is a standards based system, and different vendor subscriber radios may be able to access and use it. Due to manufacturer differences outside of the defined P25 standard, not all manufacturer radio features may work with the System. Some radios may interact differently with the existing infrastructure and can potentially exhibit undesirable operational characteristics.

As a result, the following procedures must be followed:

- All manufacturer's radios must be tested and approved by the Lead Agency prior to being used on the System.
- A listing of tested and approved radio models will be maintained by the Lead Agency.

Operational Context

The System is dedicated primarily to public safety agencies, the agencies that support public safety and public utility and service agencies.

Protocol / Standard

The System utilizes the APCO Project 25 Phase 1 digital radio standard for the voice and control channels. The microwave radio system is a digital system that adheres to Telecommunications Industry Association (TIA) / Electronic Industry Alliance (EIA) standards.

4.2 Radio System Management

The Lead Agency is responsible for System administration and the day-to-day management, operation and oversight of the System and for the maintenance of this SOP. While their specific duties are not detailed in this document, their general duties include:

- Monitoring the System and components for normal operations.
- Diagnosing System performance, problems, and developing corrective action recommendations.
- Dispatching appropriate repair services in the event of a malfunction of System equipment.
- Managing the database elements, including subscriber IDs, talkgroup IDs, and the various parameters that relate to their effective operation.
- Working with all agencies and their technical staff to diagnose and resolve problems that involve radio operations, maintenance or repair of the equipment.
- Serving as the point of contact (POC) with equipment manufacturers for issues related to the radio System.
- Providing timely information to System users on issues that arise, or repair/maintenance issues related to System equipment that would affect normal radio operations.
- Monitoring System databases for normal operations and conducting regular database backups.
- Programming of all subscriber radios and dispatch consoles with System access.
- Encryption management including managing and maintaining encryption keyloaders.

The Lead Agency makes decisions on issues related to the day-to-day operation of the System and addresses urgent or emergency operational, maintenance, or repair decisions.

An urgent or emergency situation is one where immediate decision authority is needed to allow the System as a whole, or any of the subsystem components, to continue supporting normal wide-area voice communications services. It is recognized that Lead Agency may have to obtain authorizations from the CCCS Governance Committee to make longer-term or non-emergency capital or repair expenditure decisions.

Due to the complexity and distributed administration and maintenance of the System, problems can typically occur when changes are made to hardware or software. In order to keep all System users informed of any updates, notifications will be sent to all dispatch centers and designated User Agency contacts when the following actions occur:

- Planned maintenance work is being performed on the System that will impact performance or System operations
- Equipment malfunctions or failures that affect System performance or operation
- Configuration changes in equipment or software by any user agency that may impact operations of any other agency

4.3 Network Management

Purpose or Objective

Defines the responsibilities for network management.

Technical Background

The System is comprised of, but not limited to, channel banks, hubs, switches, routers, servers, local area networks, and wide area network links connecting sites together. The network sites are interconnected by usage of microwave radio equipment, fiber, Ethernet or telecom T1 circuits. The radio network is monitored with network management tools provided by the equipment manufacturers and/or other vendors.

The radio System architecture is primarily constructed around the APCO Project 25 standard. The microwave system is composed of industry standard equipment, which also provides flexibility and a large variety of management and diagnostic tools.

The System network is complex. Unusual problems may be difficult to identify and resolve. System documentation shall be kept up to date or it will lose its value in supporting the System network.

The System is protected from all other agency data networks to manage the security and functionality of the System. If there is a connection to another data network, it shall be through a manufacturer specified and configured firewall, and approved by the Lead Agency.

Operational Context

The components of the System are considered as “owned” by the Partnership with responsibility for maintenance of the sites and equipment delegated to the Lead Agency by the authority of the 800 MHz CCCS Governance Committee and the 800 MHz CCCS Joint Agreement. Any required maintenance contractor agreements will be negotiated by the Lead Agency and presented to the 800 MHz CCCS Governance Committee for approval.

The backbone of the System is structured on an integrated network. Any infrastructure hardware and software upgrades or changes that may impact the System require reasonable discussion, approval and oversight by the Lead Agency, and the 800 MHz CCCS Governance Committee.

All maintenance work being scheduled that may affect System performance is preceded by reasonable and appropriate notification to the user agencies.

The configurations for each of the components of the System are documented primarily for the purpose of maintenance, but also affect future planning. The manufacturer provides the original 'as-built' documentation.

The other defined standards for maintenance, documentation, notification, changes, security, and training also pertain to the network portion of the System.

Procedure

The methods for performing detailed System operations are defined in the technical resource manuals and training documentation for the System. The technical resource manuals are classified as 'Restricted Information' and are not available to the general public except by formal written request approved by the 800 MHz CCCS Governance Committee, the Lead Agency and County Counsel.

Management

The Lead Agency is responsible for managing the System network.

4.4 Advanced System Keys

Purpose or Objective

To outline the procedures for the production, and usage of both the Software and Advanced System Keys (ASK) for the System.

Technical Background

A system key allows for the programming of a radio for use on the System and is used to maintain System security. The System key keeps unauthorized units from gaining access to the System. Most radio equipment manufacturers provide a software based system key unique to each trunked radio system. The System key is required for a radio (subscriber unit) to be programmed so that the radio can be recognized by the System and the user can access the System.

Operational Context

The Lead Agency will maintain and safeguard all Master ASKs, regardless of manufacturer and is responsible for the production and issuing of all secondary keys to authorized users. Manufacturers' radios that do not require a system key will not be approved for operation on the System.

An agency using subscriber radios other than the System manufacturer (Motorola) must acquire and provide to the Lead Agency the manufacturer's Master ASK for the 800 MHz System and all necessary software and key hardware to program secondary keys as needed.

The safeguarding of these keys is paramount and should at all times be treated as restricted, public safety sensitive information with access closely guarded.

Management

The Lead Agency Director is responsible for maintaining the security of and access to the System keys.

4.5 Database Management

Purpose or Objective

Defines the aspects and assignment of responsibilities for managing the System's databases.

Technical Background

The management of the System and subsystem databases is assigned to Lead Agency staff with responsibility for the various aspects of the System operations.

The databases contain information for the System and subsystems defining the operational characteristics of:

- Subscriber Radios
- Radio Users
- Talkgroups
- Profiles for Radio Users and Talkgroups
- System portion of the fleet map programming
- System and Subsystem equipment operational parameters
- Security Group structures
- Login User accounts and privileges

The databases contain the operational personality of the entire System. Because of this critical function, the data must be properly managed for System functionality and archived regularly in case of data loss or corruption.

Operational Context

The System databases are partitioned to facilitate the distributed management of the data contained in them. The database management responsibilities of the Lead Agency include the following:

- The Lead Agency is responsible for maintaining and archiving copies of all radio codeplug data and System databases.
- Database backups are made once per week and are stored "off-site" on a backed-up server in the event of a disaster.
- Database restoration will be performed by trained technical staff and only in the event of System software reloading and version changes, System database corruption, or as defined in the Disaster Recovery Plan.
- Database restoration is performed when a non-critical condition exists and if approved by the Lead Agency Director.
- The Lead Agency notifies agencies of any database issues that adversely impact their normal operations.

Procedure

The methods for performing the database operations are defined in the manufacturer's technical resource manuals. The technical resource manuals are classified as 'Restricted Information' and are not available to the general public except by formal written request to the Lead Agency.

The procedure for this standard is at the discretion of the Lead Agency.

Management

The Lead Agency is responsible for managing the data attributes and is responsible for backing up the System databases.

4.6 Subscriber Radio Inventory/Fleetmap

Purpose or Objective

Establishes the policy to ensure all radios activated on the System are properly accounted for, assigned, and managed.

Technical Background

Each radio operating on the System must be assigned a unique 7-digit IUID number allowing the radio to affiliate and communicate on the System. The System's controller provides individual access to the System for each assigned radio.

Operational Context

The Lead Agency manages the subscriber radio inventory and is responsible for assigning and tracking all IUID numbers. Each 7-digit IUID number can only be used with an individual radio and shall not be duplicated or "cloned" to another radio.

IUID management and subscriber radio inventory are critical to the operational integrity of the System. Accurate subscriber radio inventory is also important as this is the basis for the equitable distribution of the costs associated with System operations and maintenance.

Protocol / Standard

The Lead Agency is the only authorized source for IUID assignment and subscriber radio programming. The Lead Agency establishes and maintains the Fleetmap Inventory database and conducts annual inventory verification with each Partner Agency. This annual inventory is also provided to Lead Agency Financial for use in the various budget and billing calculations for Partner Agencies.

Management

The Lead Agency is responsible for IUID issuance and management of the subscriber radio inventory/Fleetmap.

4.7 Lost or Stolen Radio Notifications

Purpose or Objective

Establishes the policy to ensure the System's operational integrity and security by providing users with a procedure for reacting to incidents of missing, lost or stolen radio units.

Each agency shall develop internal guidelines for dealing with incidents of lost, stolen or missing radio equipment, to include notification to the Lead Agency.

Technical Background

The System's controller provides individual access to the System for each assigned radio. The controller provides the ability to disable the radio altogether with the 'inhibit' feature.

The target radio must be turned on and affiliated with the System for the actions to be processed. If the target radio is not active, the requested action can be put into the passive mode. When the target radio does attempt to affiliate with the System, the pending action is initiated.

Operational Context

All agencies are required to make immediate notification to the Lead Agency upon receiving information, notification, or recognition that an assigned radio is misplaced, lost or stolen. Delay in providing notification could result in unauthorized persons causing interference and/or receiving confidential information.

Protocol/Standard

The Lead Agency shall be immediately notified of the situation by a phone call and submission of a Lost/Stolen Radio Report Form.

The request to inhibit a lost/stolen radio must be specified on the Lost/Stolen Radio Report and must be accompanied by a copy of the Police report.

Lost and stolen radio information will be passed on to user agencies and local radio shops in case the radio is located or turned in.

The Lead Agency will invoice the agency for the replacement cost of the radio if owned by the Lead Agency (ie., a loan pool radio).

Management

The Lead Agency is responsible for managing this policy.

4.8 System Management Access

Purpose or Objective

Defines the types and areas of individual access to the management functions of the System.

Technical Background

Every login user of the System has a minimum of one login account and possibly more if multiple levels of access rights are needed for different purposes, such as administrative or general use. Every account can be individually set with the security and application rights needed to meet the needs of each user. All user account IDs shall be unique as the System's

databases do not permit the use of duplicate IDs. The user login aliases are limited to a specific length.

Operational Context

Personnel who log into the systems to use management applications and support tools are referred to as “Login Users”. These are technical support staff such as the System Manager, administrators, technicians, etc. This is different that “Radio User” as referred to in other standards. Every user’s login ID on the system is unique. Every login user of the System has a user ID that is only for that specific agency’s or individual’s use. Based on the types of access required an individual may need more than one login ID.

The types of access fall into the following areas:

- System Management
- Infrastructure Maintenance
- Subscriber Administration
- Dispatch Management
- Asset Management

The areas of access are based on the physical locations of the equipment and individual need.

Access to System, Network, and Asset Management terminals will be limited to Lead Agency staff and approved vendors.

Lead Agency may review personnel with System access at any time to ensure that only the appropriate levels of access have been granted based on their currently assigned business needs.

Protocol

Each Login User account must be requested from and approved by the Lead Agency Director. The account will be assigned a login name and access level based on the requirements of the request. Access will be immediately rescinded for any unauthorized actions or change of employment status.

Management

The Lead Agency is responsible for the creation of administrative accounts, designating the areas of access allowed for each account, and the review of access granted.

4.9 Requesting System Access

Purpose or Objective

To establish the procedure for an eligible agency to apply to participate on the 800 MHz CCCS.

Operational Context

The 800 MHz CCCS Governance Committee has determined the requirements and procedure for potential new applicants desiring access to the 800 MHz CCCS. Those procedures are documented in the 800 MHz CCCS Joint Agreement.

Management

The Lead Agency Director is responsible for managing the process of potential new System User applications in accordance with protocols established by the Governance Committee and documented in the 800 MHz CCCS Joint Agreement.

4.10 Alias List Standards

Purpose or Objective

To establish a standard for the use of Subscriber alias for identifying radio users.

Operational Context

An alias is a common alphanumeric name used to identify a radio, talkgroup, site, etc. rather than referencing the assigned 7-digit IUID number.

The Lead Agency does not maintain alias names for Partner Agencies.

Each Partner Agency shall maintain their own alias database and their alias names will only appear on their local dispatch consoles and subscriber radios.

Management

Each User Agency is responsible for establishing and maintaining any alias lists used by that agency.

4.11 Member Agency Operational Policy Changes

Purpose or Objective

Defines a process to mitigate negative impact to this SOP, other Member Agencies or the overall operation of the System when Member Agencies make changes to their individual Agency operational policies.

Operational Context

The 800 MHz CCCS Governance Committee is charged with approving standards and determining protocols and procedures for optimal operations between and among the users of the System.

Member Agency operational policies must not be contrary to this established SOP nor should they knowingly impact other Member Agencies in a negative manner. There will be occasions or incidents that might result in the need for a Member Agency to make changes to their operational polices. Member Agencies must ensure that any change made to their internal operational policies harmonizes with the established SOP and fellow Member Agencies.

Protocol

Member Agencies are expected to understand the potential for their policies to impact other Agencies on an integrated communications system. As a result, any Member Agency planning to make changes to their operational policy must take into account the impact on the System. If the operational policy change is likely to have an impact on the System and/or on other

Member Agencies, or, if it is unknown whether the change will have such an impact, the Agency planning to make the change shall submit the planned policy change in writing to the Lead Agency for evaluation.

The Lead Agency will address Member Agency policy change notices with respect to their impact on the System and other Agencies. The Lead Agency will inform the Governance Committee Chair of the decision regarding the policy change if it is determined that the change will impact the System or other Member Agencies.

A written notice of any planned operational policy change submitted to the Lead Agency shall include:

- Description of the policy being changed
- Reason for the planned policy change (including the potential consequences if the request is not approved)
- Preliminary assessment of impact to other System users, and an estimate of any associated costs to implement the request

An assessment shall be conducted by the Lead Agency technical and management staff and shall address:

- Technical impact to the current and future System performance including which systems or subsystems are affected
- Operational impact including capacity impact to current and future System performance
- The degree of conformance with established policies and standards
- Cost impact to current participants
- Potential alternative solutions

The Lead Agency Director shall forward the completed assessment to the requesting Member Agency along with recommendations including ways to mitigate negative impact where applicable. If the assessment reveals a negative impact to the System or to other Member Agencies, the Lead Agency will advise the requesting Agency against enacting the change. The requesting Agency may appeal the decision to the Governance Committee for resolution if desired.

The Governance Committee shall then review the requested policy change and approve, deny or modify the request. If approved or modified, the Governance Committee shall set forth operational and/or financial responsibility as appropriate and notify all affected parties of the decision.

Management

The Lead Agency Director, acting on behalf of the Governance Committee, shall manage this process.

4.12 Infrastructure Equipment Standards

Purpose or Objective

Sets the minimum technical and performance standards for infrastructure equipment operating on or interfacing with the System and establishes a policy preventing premature obsolescence of the same.

Technical Background

The 800 MHz CCCS is an APCO P25 standards-based System constructed by Motorola Solutions, Inc. It consists of radio communications sites utilizing 800 MHz radio spectrum. The Master Site is located at the Loma Ridge Facility where the Lead Agency Radio Microwave Unit is collocated along with the County Emergency Operations Center and the OCSD PSAP/Dispatch Center. Microwave links between the Master Site and the radio sites utilize redundant methods in the construction of the System to provide for a public safety grade of service.

Vendors' equipment often utilizes different operating software and may interact differently with the existing infrastructure which can potentially exhibit undesirable operational characteristics.

It is also possible that new, untested radios, equipment and/or software can exhibit performance and functionality characteristics that are destructive to the performance, capacity and/or security of the System.

Operational Context

Participants desiring to connect or interface with the System any type of fixed equipment such as a radio or console product must receive approval from the Lead Agency. Prior to approval, the System manufacturer must prove equipment compatibility. All equipment must be installed in compliance with all rules, regulations and codes applicable to its operation and location. Industry accepted radio site installation and equipment grounding practices, such as R56 or approved equivalent in effect at the time of installation, shall be used.

Protocol

To ensure the reliability of the System, all infrastructure equipment directly interfaced with the System's core must maintain the same level of software revision.

Requests shall be submitted in writing to the Lead Agency signed by the requesting agency director or department head.

Procedure

The request shall provide an outline of plans the requesting agency has developed for equipment integration. The written request shall indicate the name and contact information for the person designated to lead the project.

The Lead Agency Director will review the request and make the final decision.

If a technical use plan is already in place, the agency shall submit the plan to the Lead Agency for review to ensure compliance and compatibility with CCCS policy, standards and procedures. If a technical use plan is not in place, Lead Agency shall assist the requesting agency in developing a plan. Costs associated with the development of a technical plan are borne by the requesting agency. When the plan is complete it is submitted to the Lead Agency Director, who shall review the plan for compliance and compatibility with CCCS policies and procedures.

Management

The Lead Agency is responsible for management of infrastructure equipment standards and integration.

4.13 Subscriber Equipment Standards

Purpose or Objective

Sets the minimum technical and performance standards for subscriber radios operating on the System including:

- Establishing a policy to prevent premature obsolescence of subscriber radios.
- Establishing procedures for Lead Agency to measure, test, certify and publish a list of subscriber radios that are approved for use on the System.
- Ensuring that decommissioned subscriber radios are properly deprogrammed before disposal to prevent interference with public safety communications.

Technical Background

The System utilizes digital communication technology with the primary use being voice communications using the APCO P25 Phase 1 protocol with 9600-baud control channels.

Subscriber radios from various vendors often utilize different operating software providing a variety of services, features, functionality and performance to the users. Many of these radios interact differently with the infrastructure and can potentially exhibit undesirable operational characteristic. It is possible that untested radios and/or software can exhibit performance and/or functionality characteristics that are destructive to the overall performance, capacity and/or security of the System. Users are prohibited from using radios or accessories that may be destructive to the System.

Partner Agencies shall deliver any retired radio subscriber equipment to the Lead Agency for decommissioning and deprogramming. Decommissioned radios that are not properly deprogrammed could pose interference issues with public safety communications. Radios removed from the System for decommissioning purposes shall be deprogrammed so as to remove all System related information, ID's, and conventional channels, leaving only an idle frequency of 851.0000 MHz to prevent potential interference issues with public safety communications.

Management

The Lead Agency is responsible for maintaining all testing, managing radio equipment manufacturer initiated submittals, coordinating activities of the test team, and the proper deprogramming of subscriber radios. Any Agency purchasing new subscriber equipment is encouraged to work with the Lead Agency first to ensure the new equipment meets System standards and is properly equipped to operate on the System.

4.14 System Administrator Standards

Purpose or Objective

Establishes the minimum training standards for System administration and staff. This ensures that System functionality and integrity are maintained by restricting System administrative functions to trained, qualified and authorized personnel only.

Protocol

The Lead Agency is responsible for maintaining System configuration databases for System or subsystem infrastructure, subscriber databases and console configuration databases.

4.15 Dispatch Center Personnel Training

Purpose or Objective

Establishes minimum training standards for the public-safety dispatch center personnel with access to System resources. This ensures that personnel performing communications dispatch operations are properly trained by the Lead Agency.

Operational Context

System functionality and integrity shall be maintained by ensuring that only qualified personnel perform dispatch functions using console equipment connected to the System core.

Protocol / Standard

Public safety dispatch center personnel shall be familiar with all applicable mutual aid requirements, interoperability requirements, trunk system patching and all established SOPs.

Other recommended training that each agency's communications center personnel should have include:

- COML.
- ICS courses 100, 200, 700.B, 800 or others as required by employing agency

Recommended Procedure

This policy does not contain specific training procedures or training modules.

Management

The communications / 9-1-1 center manager within each agency is responsible to ensure personnel with radio console access to resources on the System comply with the following:

- Public safety communications / 9-1-1 center personnel receive the appropriate training before accessing System resources.
- Public safety communications / 9-1-1 center personnel maintain familiarity with features and functions of communications consoles in order to rapidly and effectively

communicate with public safety personnel and are able to identify and establish interoperability solutions when appropriate or directed.
- Only qualified personnel perform dispatch functions on System resources.
- Public safety communications / 9-1-1 center personnel maintain familiarity with all applicable sections of the SOP.

4.16 Incident / Tactical Dispatcher Training

Purpose or Objective

Establishes minimum training standards for those performing incident or tactical dispatch functions with access to System resources. This ensures that System communications incident/tactical dispatcher operations are performed by properly trained dispatch personnel.

Operational Context

System functionality and integrity shall be maintained by ensuring that only qualified personnel perform incident/tactical dispatch functions.

Protocol or Standard

Incident/tactical dispatch personnel shall successfully complete appropriate training on the console system, mobile radios or control stations in the Mobile Command/Communications Units. Appropriate training shall, at a minimum, include formal training either by an incident/tactical dispatch trainer who has completed the training from a qualified instructor or by a qualified radio technical staff member familiar with the Mobile Command/Communications Unit's (MCU) operations.

Incident/tactical dispatch personnel shall be familiar with all applicable mutual aid requirements, interoperability requirements, trunked system patching, gateway and other communications equipment in the MCU as well as all established standard operating procedures.

Other recommended incident/tactical dispatcher training should include:

- COML.
- COMT.
- ICS courses 100, 200, 300, 400, 700.B, 800 or others as required by their employing agency.
- Any other developmental, technical or safety courses deemed necessary by employing agency.

Procedure

This policy does not contain specific training procedures or training modules.

Management

The Communications Center Manager within each agency is responsible to ensure personnel with access to MCU resources on the System comply with the following:

- Incident/tactical dispatch personnel or those acting in that capacity receive the appropriate training before accessing System resources.

- Incident/tactical dispatch personnel maintain familiarity with features and functions of MCU in order to rapidly and effectively communicate with public safety personnel and are also able to identify and establish interoperability solutions when appropriate or directed.
- Only qualified personnel perform incident/tactical dispatch functions on System resources.
- Incident/tactical dispatch personnel maintain familiarity with all applicable sections of the SOP.

4.17 Radio (Subscriber) User Training

Purpose or Objective

Establishes the minimum training standards for radio users, which ensures proper operation of radios on the System.

Operational Context

System functionality and integrity shall be maintained by ensuring that only trained personnel operate radio equipment.

Protocol/Standard

Radio users shall successfully complete appropriate training on assigned radios before being allowed to operate on the System. Appropriate training shall include formal training from a qualified instructor or approved media and, at a minimum, include the following:

- Radio users shall be trained on the technical operation of assigned radios. Training will be required biennial.
- Radio users shall be trained on how to operate the radio within the System along with any special features of the System they will use, e.g., emergency button, call alert, etc.
- Radio users shall be trained on and demonstrate proficiency with all applicable mutual aid and interoperable communications resources and standard operating procedures.
- Radio users shall maintain awareness of the mutual aid, interoperability channels or talkgroups in their radios, as well as how to navigate to them when necessary.
- User agencies will make an effort to conduct ongoing refresher training for radio users periodically following their initial training (e.g., build into in-service training, dispatch centers conduct random tests, roll call training, on-shift training, etc.).

Lead Agency staff assists user agencies in identifying training needs and implementing training programs to meet those needs. The Lead Agency also employs a qualified training officer who is available to provide this training to authorized System users.

Procedure

This SOP does not contain specific training procedures or training modules, however, Lead Agency staff assists with radio user training when requested.

Management

Each User Agency is responsible to ensure that:

- Personnel assigned radios shall receive the appropriate training with emphasis on awareness of and how to navigate to mutual aid and interoperability channels or talkgroups (initial and ongoing refresher training).
- Only trained and qualified personnel shall operate radio equipment.
- Radio users are familiar with sections of the SOP.

4.18 Interoperability and non-CCCS Radio Users

Purpose or Objective

Establishes the minimum training standards for radio users having access to interoperable resources of the System. This ensures the proper operation of radios on the System and safeguards against improper utilization of interoperability resources.

Operational Context

System functionality and operability is maintained by ensuring that only properly trained personnel use the interoperable resources on the System for mutual aid communications. If agencies do not have appropriate training, then communications failure or a degradation of the System resources may occur.

Protocol/Standard

Radio users shall have a demonstrated knowledge of Section 6 Interoperability Standards, and have successfully completed appropriate initial and ongoing refresher training including:

- User training emphasizing:
    - The use of interoperable channels and how to navigate their radio.
    - How a user's radio experiences can be affected by the selected interoperability channel (digital, analog, non-trunked, etc.).
- Dispatch and supervisory training emphasizing:
    - The use of interoperable channels.
    - The use of patching and patch channels.
    - The use of cross band repeaters and gateway devices.
    - The use of RF control stations.
    - How a user's radio experiences can be affected by the selected interoperability channel (digital, analog, non-trunked, etc.).

Radio users with access to interoperable channels must be familiar with all applicable mutual aid and interoperable requirements and procedures.

Procedure

This SOP does not contain specific training procedures or training modules.

Management

The Lead Agency will provide training materials upon request for initial training and ongoing refresher training. Additionally, as resources permit, the Lead Agency will assist user agencies

with developing plans and methods on incorporating ongoing radio refresher training into various activities for the most effective delivery to personnel. The Lead Agency also employs a qualified training officer who is available to provide this training to authorized System users.

Agencies requesting and/or using the interoperable talkgroups are responsible to ensure that:

- The use of mutual aid/interoperability channels and talkgroups is properly coordinated and approved through the Control One.
- Radio users successfully complete appropriate initial and on-going refresher training and demonstrate knowledge of proper communications procedures before being allowed to operate the interoperable resources.
- Radio users are familiar with all applicable interoperable sections of this manual.
- Radio users are familiar with all applicable mutual aid requirements and interoperable SOPs.

4.19 System Upgrade Notification

Purpose or Objective

Establishes notification procedure prior to major System upgrades.

Protocol/Standard

System software upgrades will be performed as needed contingent upon available funding and/or technical requirements. The Lead Agency will be responsible for ensuring that all System user agencies that may be impacted by the upgrade are notified by email and/or other written form.

Recommended Procedure

Planned upgrade procedures will be communicated to all System users as follows:

- At least 30 days prior to a planned major System upgrade that will cause a System or site outage, the Lead Agency will notify all System user agencies that may be impacted by the upgrade.
- The Lead Agency will send an email reminder to all potentially impacted System user agencies a week prior to the System upgrade.
- Control One will communicate upgrade instructions and status to all System users before, during and upon completion of the upgrade.

User agencies must notify the Lead Agency Director in writing if the planned upgrade dates will interfere with any major planned events.

Management

The Lead Agency is responsible for managing System upgrades and the necessary notifications associated with each upgrade.

4.20 In-building Coverage (Bi-Directional Amplifiers)

Purpose or Objective

Establishes policy on usage of Bi-Directional Amplifiers (BDA) and awareness of all locations utilizing BDAs for the purpose of mitigating interference issues.

Technical Background

The System is designed for mobile and portable radio coverage but cannot provide 100% coverage in all places. BDAs are a device that aims to improve radio access within a confined space such as high-density buildings. Although the use of a BDA may improve in-building coverage, it may also create interference issues with the overall System. Tracking the locations of all BDAs will aid in quickly locating offending BDA equipment.

Protocol/Standard

It is not the intent for the Lead Agency or Governance Committee to approve or regulate BDAs. It is important for the Lead Agency to maintain a list of facilities that do have BDAs used with the System.

Any agency or department installing a BDA will provide the Lead Agency with the location of the device prior to installation if possible. This will include the physical address, emergency contact information, building name, location within the building, manufacturer and model number.

It is the responsibility of the equipment/facility owner to comply with all requirements of the FCC, including licensing, location reporting, and interference mitigation.

Recommended Procedure

Agencies installing BDAs will submit to the Lead Agency a list of locations where BDAs are installed that are supplementing the System. BDAs not supplementing the System do not need to be reported. This list will be updated periodically.

Management

The Lead Agency will maintain the list of BDAs supplementing the System. Each agency will maintain a list of BDAs within their jurisdiction along with contact information for the equipment/facility owner to allow access should the BDA interfere with the System.

4.21 Aircraft Radio Installations and Operation

Purpose or Objective

Sets the policy regarding aircraft subscriber radio installation, programming, and operation on the System.

Technical Background

Due to the elevated altitude of operation, aircraft radios have a greater coverage footprint. This allows a radio operated in the air to access sites as far away as 150 to 200 miles, while mobile radios operated in vehicles on the ground typically have ranges limited to 30 to 40 miles. Radios in aircraft operating with the System function slightly different than radios on the ground.

Due to the interference potential from the larger coverage footprint of aircraft operated radios, the FCC rules for operation of these radios limits the output power to help reduce interference, as frequency reuse is applicable in the CCCS and other radio systems.

Installation of aircraft mounted radios is governed by the Federal Aviation Administration (FAA) and permanent installations must be performed by FAA certified personnel.

Operational Context

Subscribers that acquire a large coverage footprint due to high altitude operations need to take into consideration potential interference due to frequency reuse in other systems. This could cause interference to their users. This interference could appear as an interruption, loss of communications, or as tailgating to other talkgroup transmissions on other sites.

Protocol / Standard

All permanently installed aircraft radios shall comply with the FCC 90.423 power output limitation of 10 watts, the Effective Radiated Power (ERP) being no more than 5 watts. Only unity gain antennas will be allowed.

Permanently mounted aircraft radios should be programmed with the following:

- BER threshold of 2.5%

For aircrews that are assigned portable radios, these portable radios should be programmed for the following:

- 2.5% or 2.9% BER threshold

These settings apply for both aircraft installed radios using remote mounted mobile or portable radios and Technisonic-type aircraft control panel mounted avionics packages using internal portable radios.

Procedures for landing zone areas where communications with ground personnel are conducted are recommended on a simplex, non-trunked, channel.

In addition to the SOP training requirement, training for users of aircraft radios shall include a description of the issues surrounding airborne operation of System radios including:

- Issues of potential interference to other systems due to frequency reuse;
- Personnel using portable radios in a limited capacity (observers, guests, etc.) and the potential for FAA and FCC rule violation, and interference.

Recommended Procedure

Installation and programming should be performed as outlined in this section. Operation of Aircraft landing zone coordination should be performed as outlined in this section. In-flight transmissions should be as brief as possible due to the potential interference.

Management

The Lead Agency Director will be responsible for the oversight and compliance of this standard. Due to the potential of interference issues to expand beyond a specific region or into another County, Lead Agency staff should also be notified if any interference is detected and is believed to have originated from a CCCS radio equipped aircraft.

4.22 In-building Coverage

Purpose or Objective

Establishes policy on the approval, usage and regulation of in-building coverage enhancement devices on System frequencies and the tracking of all locations utilizing these devices for the purpose of mitigating interference issues. In-building coverage systems include Emergency Responder Radio Communications Systems (ERRCS), Bi-Directional Amplifiers (BDA), and Distributed Antenna Systems (DAS).

Technical Background

The System is designed for mobile and portable radio coverage but cannot provide 100% coverage in all places. In-building coverage devices aim to improve radio access within a confined space such as high-density buildings. Although the use of in-building coverage devices may improve in-building coverage, it may also create interference issues with the overall System. Tracking the locations of all in-building coverage devices will aid in quickly locating offending equipment.

Protocol/Standard

The Lead Agency must approve and regulate in-building coverage systems on frequencies licensed to the County of Orange. It is important for the Lead Agency to maintain a list of facilities that have in-building coverage devices used with the System.

Any agency or department planning to install an in-building coverage system will submit their plans to the Lead Agency as described in the current OCSD ERRCS Guidelines document. This will include the physical address, emergency contact information, building name, location within the building, manufacturer and model number. The Lead Agency must review and approve operation of the installed in-building coverage system to ensure proper installation and operation and to mitigate any adverse effect on the System.

It is the responsibility of the equipment/facility owner to comply with all requirements of the National Fire Protection Association (NFPA), California Fire Code (CFC) and Federal Communications Commission (FCC) including licensing, location reporting, and interference mitigation.

Recommended Procedure

Agencies planning to install an in-building coverage system shall contact the Lead Agency for guidance and to begin the approval process. All agencies shall submit to the Lead Agency a list of locations where BDA, DAS or other ERRCS systems are installed that are supplementing the System. In-building coverage devices not supplementing the System do not need to be reported. This list will be updated periodically.

Management

The Lead Agency will manage the In-Building Coverage policy and maintain the list of in-building devices supplementing the System. Each agency will maintain a list of in-building coverage devices within their jurisdiction along with contact information for the equipment/facility owner to allow access should the equipment interfere with the System.

5.0 CONFIGURATIONS AND ALLOCATION

5.1 Zone and Talkgroup Naming Standards

Purpose or Objective

A well-defined method of naming radio programming zones and talkgroups/channels aids in user interoperability by allowing all users to understand the designated use of individual talkgroups/channels and how to find those talkgroups/channels in their radio.

Operational Context

In addition to agency-specific zones and talkgroups, all System users have certain talkgroups/channels programmed into their radios that are common to all System users to allow for operational interoperability. The ability to quickly locate these common talkgroups/channels for interoperability requires a uniform programming methodology to place the talkgroups/channels in specific zones in all radio on the System.

Protocol/Standard

The Lead Agency, in conjunction with User Agencies, and with the authority of the Governance Committee has established the zone and talkgroup naming structure used by all System users. The zone/talkgroup/Channel names and radio template structure is provided in the Official Communications Handbook (Radio Code Book) for each System Discipline (Law, Fire, Lifeguard/Marine Safety, Public Works).

Requests for additional zones or talkgroups must be submitted to the Lead Agency for consideration and analysis as to their potential impact on the System.

Management

The Lead Agency shall maintain the Official Communications Handbook and associated records related to zone and talkgroup/channel naming.

5.2 Radio IUID Allocation

Purpose or Objective

Allocates radio Item Unit Identification number (IUID) ranges for the individual agencies. This allows the Lead Agency to manage the pool of IUIDs as radio users and console positions are configured. This simplifies the management of the IUIDs and provides an easier indication of what IUIDs belong to which agency in the event that a radio user alias is not available.

Technical Background

These IUIDs are the same IUIDs that users type in for call alert pages. Also, these are the IUIDs that are displayed on the subscriber radios if the “ID Display” feature is enabled. These IUIDs are also displayed at the console if the console alias feature is not available.

Operational Context

The Lead Agency will allocate radio IUID ranges to agencies based on the number of units the agency will have active on the System and will be shown on the master agency IUID list.

Protocol/Standard

Only radio IUIDs allocated to an individual agency can be used in the programming of that agency’s radios and consoles. The Lead Agency is responsible for the programming of all radios on the System.

Procedure

The Lead Agency maintains the master list of IUID distribution and will allocate IUIDs to agencies based on each agency’s radio count and need. If an agency requires additional IUIDs beyond the initial allocation, a request shall be made to the Lead Agency. The Lead Agency will evaluate the request and conduct an analysis to determine impact to the System. Upon completion of the analysis, the Lead Agency may approve or deny the request, or ask for additional information.

Management

The Lead Agency manages the IUID ranges for day-to-day activities, and manages the IUID ranges for reserve or future allocation.

5.3 Fleetmap Standards

Purpose or Objective

Defines the process used to document the Fleetmap information for the effective management of the System.

System Fleetmap configuration information is classified as ‘Restricted Information’ and is not released to the public.

Technical Background

The Fleetmap is parameter information programmed into the System infrastructure and into the subscriber radios to control how those radios perform on the System.

The Fleetmap spreadsheet is a documented matrix of the talkgroups in the System and the departments or agencies that use and control user access to these talkgroups. The Fleetmap contains the following information:

- Talkgroup Name – Name of the talkgroup as it is programmed into the System.
- Talkgroup Alias – Abbreviated naming of the talkgroup to fit within the 8 or 14 character radio display.
- Talkgroup ID – Numerical designation of the talkgroup in decimal and/or hexadecimal.
- Failsoft Channel – The System channel designated for the talkgroup when in the failsoft mode.
- Owner – The primary user agency with access control of the talkgroup.
- Priority – Priority level of the talkgroup.
- On Console – If the talkgroup is available as a console resource.
- Trunked Alternate – A talkgroup to be used when the user's primary system is unavailable.

Operational Context

The Lead Agency will establish and manage the Fleetmap database information for all users of the System.

Protocol / Standard

A detailed matrix is maintained by the Lead Agency on the System database. Each agency's radio representative maintains a Fleetmap spreadsheet containing data on their talkgroups and the users for whom they are responsible.

Procedure

If an individual agency desires to make updates and changes to their Fleetmap standards, the changes shall be requested through the Lead Agency.

- The Lead Agency will evaluate any requests for changes and conduct an analysis to determine its feasibility and impact on the System.
- The Lead Agency will decide if the request will be approved or denied and proceed accordingly with notification to the requesting agency.

The disclosure of the Fleetmap configuration information, including talkgroup IDs, user IDs, user privileges and other related System information could substantially jeopardize the security of the System. This disclosure makes it more susceptible to sabotage and unauthorized access to the contents of confidential voice and data communications. Therefore, the master Fleetmap data shall be classified as 'Restricted Information' and is not available to the general public except by formal written request to the 800 MHz CCCS Governance Committee.

Management

The Lead Agency manages the Fleetmap and System programming for all agencies.

5.4 Subscriber Template Management

Purpose of Objective

Defines the process that is used to document the radio subscriber template information for the effective management of the System. The System contains a large number of talkgroups to support the various agencies that subscribe to the System. Subscriber template configuration information is classified as 'Restricted Information' and is not released to the general public.

Technical Background

The subscriber template is parameter information programmed into the individual subscriber radios to control how those radios perform on the System.

An agency's subscriber template is developed and maintained by the Lead Agency with the input of each agency's radio representative. This is to ensure the agency gets the talkgroups, features, and functionality desired from the radios, while maintaining the overall functionality and integrity of the System.

The radio subscriber template is usually specific to a particular agency, but an agency can elect to have different versions of the template based on the department's needs and operations.

The templates normally contain the following information:

- Radio Configuration – Specific information related to a particular model of radio, including but not limited to: button assignment, display options, menu items, and other radio wide parameters.
- Conventional – Personality information that determines the radio's operation in the conventional mode such as frequencies, tones, and signaling options.
- Trunking – Identifies System and talkgroup specifics that the subscriber radio has access to, as well as System and unit-specific ID numbers relating to the radios operation.
- Scan – Defines the limits and lists of the subscriber radio's scan function, when equipped.
- Zone Assignment – Where talkgroups are combined into specifically labeled 'zones' within the radio that represent or reflect operations of a particular agency or operation. The zone designation reflects an acronym, which should easily identify the zone as belonging to a particular agency.

Operational Context

The Lead Agency creates and manages all subscriber templates to ensure uniformity and proper operation on the System.

Protocol / Standard

User Agencies may have multiple subscriber templates based upon their operational needs. The Lead Agency shall maintain a subscriber template spreadsheet for each of the agency's template versions.

The Lead Agency will work with each user agency to develop the subscriber templates for that agency. All subscriber template creation and modification shall be done by the Lead Agency. The Lead Agency shall maintain all associated documentation for each subscriber template.

Procedure

If individual agencies desire to make updates and/or changes to their subscriber templates, those change requests shall be submitted to the Lead Agency for review. The Lead Agency will approve or deny the request after reviewing impact to the System and other users. If approved, the costs for template change and subsequent reprogramming of subscriber radios will be borne by the requesting agency.

The disclosure of the subscriber template configuration information, including talkgroup IDs, user IDs, user privileges and other related System information could substantially jeopardize the security of the System. This disclosure makes it more susceptible to tampering, sabotage, unauthorized use, jamming, hacking, unauthorized access to the contents of confidential voice and data communications. Therefore, the subscriber template spreadsheets shall be classified as 'Restricted Information' and are not available to the general public except by formal written request to the 800 MHz CCCS Governance Committee.

Management

The Lead Agency manages all subscriber templates and programming for all agencies and maintains records of the process. Access is strictly controlled and is considered 'Restricted Information'.

5.5 Talkgroup Assignments

Purpose or Objective

Defines the assignment/usage of agency-specific, common and interoperable/mutual aid talkgroups and resources, and provides a standard so that the Lead Agency will have a firm guideline on allowing particular talkgroups programmed into radios.

Operational Context

Talkgroups are considered assigned by the agency for which the talkgroup was specifically created. The process for pre-defined sharing authorizations is explained in Section 5.6.

Recommended Protocol/Standard

There are three types of talkgroups that are programmed into the System:

- **Agency-Specific** – Created for, and controlled by, individual agencies for their day-to-day operations. These talkgroups cannot be accessed by other System users without express permission granted by the assigned agency. The process for obtaining this permission is outlined in Section 5.6.
- **Common Resources** – Talkgroups/channels created for common use among discipline specific agencies (law, fire, general) as needed. These talkgroups/channels are not controlled by any individual agency but are available for use by all Partner Agencies and are coordinated by the Control One.

- **Interoperable/Mutual Aid Resources** – These talkgroups/channels are established interoperable or mutual aid resources available to all System users based upon specific discipline (law, fire, general) and allow communications with non-CCCS System agencies as needed. These talkgroups/channels include the ability to be patched to non-800 MHz resources for greater interoperability. These talkgroups/channels are coordinated locally through the Control One.

Procedure

The Lead Agency will control all talkgroup generation and access parameters. Agencies shall immediately notify the Lead Agency when changes to an agency-specific talkgroup are required or the talkgroup is no longer required.

Management

The Lead Agency is responsible for the management of the Talkgroup Ownership policy.

5.6 Talkgroup Sharing

Purpose or Objective

Defines how System Partner Agencies can permit other agencies to access to their agency-specific talkgroups.

Technical Background

Radios must be P25 compliant and compatible with the System. Refer to Section 4.13 of this SOP for additional details on subscriber equipment standards.

Operational Context

Partner agencies have the authority and control to define who is allowed access to their agency-specific talkgroups/channels. This process is accomplished with a formal written request to the Lead Agency from the requesting agency which is passed to the agency-specific talkgroup owner for approval. The request should include the specific talkgroup name desired and the intended purpose and potential users of the talkgroup.

Protocol/Standard

Agency-specific talkgroups/channels shall not be programmed into any other radios without the written permission from the controlling agency. Documented written approval letters shall be maintained by the Lead Agency for each talkgroup sharing agreement.

Procedure

The Lead Agency working with the talkgroup ‘owner’ will process the request and, upon approval, make the necessary modifications to the requesting agency template. The Lead Agency will maintain all supporting documentation regarding the requested change. All costs associated with the template change and reprogramming will be borne by the requesting agency.

Management

The Lead Agency is responsible for the management of this procedure.

5.7 Talkgroup and Radio User Priorities

Purpose or Objective

Establishes varying priority levels for talkgroups to assure the most critical talkgroups on the System are granted a channel as quickly as possible when the System is experiencing busy conditions.

Technical Background

The System priorities can be managed both at the radio user level and at the talkgroup level.

Operational Context

Priority levels in the System are managed at the talkgroup level. The goal is to distribute priorities across the System talkgroups in a way that maximizes the ability for critical groups to communicate and minimizes the number of talkgroups with high priority.

5.9 Failsoft Assignments

Purpose or Objective

Creates and assigns System resources in a manner which maximizes System utility to users consistent with each user's mission and needs for radio communications during certain System failure situations.

Technical Background

When the System's main controllers detect certain failure conditions in the radio System, all available channels revert from a trunking mode into a conventional repeater type of operation that is given the term 'failsoft'. During failsoft, talkgroups are assigned to a specific radio channel (frequency) if so programmed, which allows the users to continue voice communication while repairs are made to the System.

There are a limited number of channels available in the System, which results in a number of talkgroups being combined on each channel while in failsoft. This requires the radio users to share those channels between numerous agencies. This congestion of radio traffic happens only during the failsoft condition.

If a talkgroup is not given a failsoft assignment, radios using that talkgroup will hear the low pitched 'out-of-range' tone when the System is in failsoft, and will not be able to communicate on that talkgroup.

Operational Context

The radio programming template failsoft assignments are configured to balance the ability for users to achieve an acceptable level of communications while maintaining the individual agency's privacy when possible. While in the failsoft condition, effected radios will display the

word ‘FAILSOFT’ on the radio display and emit a short high-pitched tone every 10-15 seconds to indicate to the user that normal trunked operation is unavailable.

Protocol / Standard

It is the policy of the Lead Agency to provide a failsoft assignment for every ‘primary’ talkgroup on the System to prevent loss of communications for users. Failsoft channel assignments are based on the needs of System users consistent with each user’s mission and need for radio communications.

The Lead Agency makes determinations concerning Failsoft channel assignments.

During a Failsoft condition, dispatchers may need to announce instructions to radio users and remind them that operations may be combined among several agencies and to implement radio discipline to reduce radio traffic.

Management

The Lead Agency is the responsible authority for failsoft assignments and management. Agencies desiring additional information on failsoft assignments may request the information from the Lead Agency.

5.10 Scanning

Purpose or Objective

Identifies operational procedures and responsible authorities governing scanning System talkgroups.

Technical Background

The network infrastructure and subscriber units are configured to permit managed user scanning of talkgroups. Including a talkgroup in a non-priority scan list does not necessarily result in the user hearing traffic on that talkgroup. Talkgroups are only active if there is at least one user affiliated who has the talkgroup of interest as their selected channel.

Subscriber units can scan a talkgroup, a talkgroup in another zone, or another trunked radio system if compatible. An entire radio can be set up as receive only.

Operational Context

Scanning by multiple subscriber units can quickly overwhelm a trunked radio system creating system busies. As a result, scanning on the System has been limited to the Fire Services as a legacy feature allowing scanning of their Dispatch Talkgroup and primary tacticals.

Protocol / Standard

Before scanning and/or monitoring of System talkgroups is allowed, permission must be obtained from the Lead Agency and the agency ‘owning’ the talkgroup. Scanning must also be approved by the requestor’s agency in their template design.

Scanning can only be enabled in the programming template by the Lead Agency.

Management

The Lead Agency is responsible for authorizing, programming and managing scanning in subscriber templates.

5.11 Emergency Button

Technical Background

The emergency button feature allows a radio user to send an emergency notification by pressing a button on the radio. The notifications audibly and visually alert dispatch console positions that have the initiating radio's talkgroup in their active configuration. Other subscriber radios on the same talkgroup also receive the emergency notification once the 'emergency' radio is keyed which will display the IUID (or alias if available) of the radio generating the emergency.

Emergency calls are also automatically assigned the highest priority available by the System controller and are the first available from the queue if the System is in a busy situation.

Operational Context

The orange button on a portable or mobile radio will be programmed with the emergency feature for all agencies. Each agency should establish their own policy on how this feature might be used, taking into consideration how it will impact the System and other users including the Control One. The emergency feature can be used to alert dispatch and other users of an emergency situation and simultaneously allow the activated radio to have priority over other subscriber radios on the same talkgroup.

Protocol / Standard

The use of the emergency button as an emergency signaling option shall be available to any agency on the System, subject to certain conditions and provisions including:

- Agencies must provide training to all users to ensure the safe and effective use of this feature. The Lead Agency can also provide training and training materials.
- It is the individual agency's responsibility to determine how an emergency alarm will be deployed for their operation and the subsequent response to the alarm.
- If a user is temporarily assigned a radio other than their normal issued equipment, it is essential that their designated monitoring point be made aware of the radio identification to cross-reference it to the correct user in the event an emergency button activation occurs.
- All agencies implementing the emergency feature shall have a plan in place to respond to emergency button activation.

All emergency button response plans must include the following:

- An established radio monitoring point with the necessary console hardware/software to receive, display and acknowledge the alert.
- Established monitoring point must be capable of identifying which radio user pushed the button and capable of responding to the user in need. (Dispatch Center or Control One)

- In the event that the monitoring point is not the same agency as the radio user, an agreement on policy, monitoring, use, and response, shall be in place among the agencies.
- Established monitoring points shall be available during any/all hours that personnel are using the System, or have an established after-hours arrangement with another monitoring point.
- No dispatcher shall clear an emergency without ascertaining what action is necessary to handle said emergency and taking the appropriate actions to do so.

Control One receives all emergency button activations and will contact originating radio user's agency for follow-up when activations occur on common/interoperable talkgroups that are not assigned specifically to the agency in question.

Management

The Lead Agency will manage the overall Emergency Button policy. Agencies desiring to use the emergency key function shall coordinate with agency resources that receive the emergency calls. The receiving agencies shall have an appropriate plan in place and documented as to the process to handle the emergency calls.

5.12 Encryption

Purpose or Objective

Establishes guidelines for the use of encryption on the System.

Technical Background

Encryption is an option on digital radio equipment that must be specially ordered and manually configured. System users may or may not be capable of encryption depending on their equipment configuration and operational needs. AES is the approved standard for encryption on the System.

Operational Context

The use of encryption in the System is strapped to the specific talkgroups determined by the System users to provide secure communications. Encryption is not a feature that can be enabled or defeated at the user level. Each talkgroup is pre-determined to be either encrypted or clear and is programmed as such in the subscriber template.

Radios transmitting with encryption cannot be heard by non-encrypted radios.

An encrypted talkgroup that is patched to a non-encrypted talkgroup or channel is no longer considered secure communications as the encrypted audio is decrypted when pushed over the patched non-encrypted talkgroup/channel. Likewise, audio fed to an internet streaming application will not be secure.

Protocol / Standard

Only the Lead Agency is authorized to program encryption into radios on the System.

Each agency shall determine if encryption will be used on its own agency-specific talkgroups.

Certain common/interoperable talkgroups allocated to specific disciplines such as law/fire will be encrypted in all System radios. Non-encrypted common/interoperable talkgroups will also be available to System users who do not have encrypted radios.

Care should be taken when assigning encrypted talkgroups to incident communications to ensure all applicable users have encrypted radios.

Management

The Lead Agency manages the encryption policy and the programming of encryption into all radios on the System.

6.0 INTEROPERABILITY STANDARDS

6.1 Interoperable Communications Requirements

Purpose or Objective

Establishes a minimum requirement for interoperable communications resources for all radios using the System.

Technical Background

For the purpose of this document, the terms ‘mutual aid’ and ‘interoperability’ will be used interchangeably. The term ‘channel’ will refer to a conventional resource.

The planners of the System recognized the need to make common interoperable talkgroups available to all subscribers primarily for interagency and incident command communications. Therefore, in addition to agency-specific talkgroups, the System also provides talkgroups that are common to like-disciplined agencies (law, fire, public works, lifeguard) as well as talkgroups that are available to all System users to provide interoperability between disciplines.

In addition to common System talkgroups, subscriber radios will also be programmed with local, state and national conventional interoperable channels. Most of these conventional interoperable channels are not encrypted but there are a few 700MHz encrypted channels available in encryption-capable radios.

Operational Context

Interoperable talkgroups & channels are used when there is a need to coordinate activities between different agencies and/or personnel assigned to work an event. Efforts should be made to utilize the lowest level of interoperable talkgroup/channel first if possible. For example, OC law agencies needing to coordinate with other law agencies should use the CCCS law interoperability talkgroups/channels before considering national level interoperable channels. If the coordination includes agencies that do not have access to the CCCS interoperable law talkgroups, statewide or national interoperable channels would be selected.

Additional information on the operational use of these interoperable talkgroups/channels can be found in the ‘Official Communications Handbook’ (Radio Code Book).

Protocol / Standard

All radios will be programmed to include the 'general use' interoperable talkgroups and channels located in specific zones in the radio template. These talkgroups and channels will be programmed into predetermined specific zones in all System radios to provide uniformity in programming for ease of locating the talkgroups/channels when needed.

Radio templates will also include discipline-specific interoperable talkgroups (ie. Orange, Gray, Black talkgroups for Law) in templates for all like-discipline agencies (law, fire, lifeguard, public works). These discipline-specific interoperable talkgroups/channels will be programmed into predetermined specific zones in all like-disciplined agency radios to provide uniformity in programming and ease of use.

Additional information on the location of these interoperable talkgroups/channels in the radio programming templates can be found in the 'Official Communications Handbook' (Radio Code Book) for each discipline.

Procedure

Coordination of all interoperable talkgroups and channels in Orange County is managed by the Control One. Any agency requiring interoperable talkgroups or channels should contact Control One for assistance with selecting and reserving these resources to meet their needs.

Management

The Lead Agency is responsible for managing this policy and ensuring interoperable channels are available and operational.

The Countywide Coordinated Communication Center (Control One) is responsible for managing the assignment and use of the interoperable talkgroups and channels in Orange County.

6.2 Radio Console Patching of Talkgroups / Channels

Purpose or Objective

Establishes policy for use of a console patch between System talkgroups and/or other resources on the dispatch console.

Technical Background

Most public safety communications/9-1-1 centers have the capability to initiate a console patch but patches that include a common System resource shall be accomplished on a console at Control One. Console patches can be established between multiple System talkgroups and/or between a System Talkgroup and a non-System resource. The resources can be conventional or trunked but must be an existing radio resource on the dispatch console.

Patches can be established without a radio dispatch console by using a deployable audio gateway, such as an ACU-1000. Approval is required prior to creating any patch. A talkgroup can only be in one patch at a time. A conventional channel can only be in one patch at a time.

Great care must be used in deciding what talkgroups and other resources can be patched together as a patch can have an unexpected consequential impact on other System resources.

The patch shall be monitored for continued coordination through Incident Command and/or dispatch personnel.

Operational Context

Console Patches should only be used when there is an operational need for communications between personnel that cannot be accomplished using common communications resources. Use of conventional resources in a patch must be in compliance with the rules governing mutual aid channel usage. Console patching will only be permitted when approved by agency Watch Commander/Incident Commander and after notification to the Control One supervisor.

A patch involving agency-specific talkgroups/channels can be initiated on the local agency's console with approval by that agency's Watch Commander.

Any patch involving a common System resource should be initiated by Control One.

Protocol/Standard

Each agency must develop written console patch and/or gateway device patch procedures addressing their unique operation and resource capabilities. These procedures shall be consistent with this policy. All communications center personnel shall receive initial and continuing training on the use of this procedure.

Procedure

When an incident requires interagency coordination that is not available on a common talkgroup or channel, a request for a patch can be initiated. If the desired resource to be patched is a local agency resource and their agency-specific talkgroup/channel, the requesting agency can initiate the patch on their local console with their Watch Commander's approval and notification to Control One.

If the desired resource to be patched is a common System resource, the patch request must be directed to Control One after obtaining local agency Watch Commander approval. Control One will then initiate the patch from their console.

Before initiating a System patch, check to make sure the radio resource being patched is not already being used by another agency.

Radio console patches shall be used only if other suitable means for interagency communicating are unavailable or insufficient.

Any time a console patch has been established, someone in the requesting agency's communications center must continually monitor the patch to address and mitigate communications problems.

Management

The Lead Agency is responsible for managing this policy. All agencies electing to use console patching are responsible for establishing and managing internal patch procedures and complying with this policy.

6.3 Use of the Statewide and National Interoperability Channels

Purpose or Objective

Defines the procedures for the use of the conventional Statewide and National interoperable radio channels for communications between radio users of disparate radio systems and/or different frequency bands.

Technical Background

The FCC has designated certain VHF, UHF, 700 MHz & 800 MHz frequency pairs to be used exclusively for conventional interoperable communications between public safety radio users. Each frequency band includes a calling/hailing channel to be used in contacting the coordination center for the local operational area. Additionally, each frequency band includes channels for tactical operations in both repeater and direct “talkaround” modes. In the Orange County Operational Area, these channels are coordinated by the Control One.

All CCCS Partner Agency radios include many of the 700 MHz and 800 MHz interoperability channels in their standard radio programming template. Additional information on these channels, including channel names and general use, can be found in the discipline specific Orange County Official Communications Handbook (Radio Code Book) available to Partner Agencies through the Lead Agency.

The Lead Agency also maintains repeater systems with Interoperable channels in the VHF and UHF frequency bands which are available to CCCS Partner Agency users through a gateway patch on the Control One radio console. This allows CCCS radio users to be patched to a non-800 MHz radio system for interoperable communications with the users of that system.

Operational Context

These designated interoperable communications resources can be used for day-to-day interagency coordination, for urgent or emergency mutual aid situations, and/or for other purposes where coordination between radio users on separate 800 MHz radio systems or non-800 MHz radio systems must communicate to perform assigned duties.

These channels shall not be used for regular communications between radio users with full access to the CCCS, except when authorized and assigned by Incident Command.

Protocol/Standard

The 700 MHz and 800 MHz interoperability channels are programmed into the radio template of all CCCS subscriber radios. These channels may be used when traveling outside the coverage area of the CCCS System and are used to communicate with another 800 MHz radio system with base and/or mobile radios on those channels.

Control One shall monitor the interoperability hailing/calling channels at all times.

Procedure

When an incident requires the use of a Statewide or National 700 MHz or 800 MHz interoperability resource, the requesting unit or agency will contact Control One to request the assignment of an interoperable tactical channel. Control One will assign an appropriate channel and monitor for any issues.

When an incident requires the use of a Statewide or National VHF or UHF interoperability resource, the requesting unit or agency will contact Control One to request the assignment of a tactical radio channel in the appropriate frequency band. Control One will initiate a patch between the requested VHF or UHF resource and the 800 MHz talkgroup/channel used in the patch.

Control One shall monitor all interoperability hailing/calling channels 24/7 to provide immediate assistance when requested.

Management

The Lead Agency will manage this policy and the coordination and maintenance of interoperable radio resources in Orange County.

CCCS agencies are responsible for providing training to their personnel on the proper use of these Statewide and National Interoperable communications resources.

6.4 Control Station Usage on Interoperability Channels

Purpose or Objective

Establishes procedures for the use of control stations for gateway patching.

Technical Background

A control station is a radio that is set up like a portable or mobile radio, typically with a limited number of talkgroups or conventional radio channels. It can be connected to a radio console or used stand alone.

A control station can function on only one talkgroup or conventional channel at a time.

Use of a control station with a radio console to patch System resources can have a wide area impact. This type of patch can be easily accomplished, but may take up multiple trunked radio channels, causing the System to experience busies or possibly create radio interference. Control station usage must comply with parameters listed on the agency's FCC license.

Operational Context

There are a number of uses for control stations including:

- Installed at an agency that does not have a dispatch console to communicate with a conventional repeater or trunked radio system.
- Connected to a dispatch console at a communications center.

- Installed in a Mobile Communications Unit/Vehicle.
- Installed at an Incident Communications Center or Command Post.

Protocol/Standard

Radio control stations are permissible in the following circumstances:

- Connected to a radio console to be used to access the System by non-System user agencies for interoperability purposes.
- Installed in a MCU/MCV.
- Installed temporarily in an Incident Communications Center or Command Post.
- Connected to a radio console to be used to access the System by user agencies for interoperability purposes.
- Used with an audio logger to record transmitted or received audio.

All communications personnel performing the dispatch function shall be trained on the usage and constraints of the control station. They should receive continued training to maintain proficiency and understanding of the procedures.

A radio technician, COMT or other authorized person shall be involved in the configuration, installation and testing of control stations, whether a temporary or permanent installation.

Limitations

- Control stations should not be used to patch a System talkgroup to another System talkgroup except when approved by the Communications Center Supervisor and the Control One Supervisor.
- Control station antennas must not exceed 20' in height. If an antenna requires more height than 20' to access the System or mutual aid repeater, then a FCC license is required.
- No control station antenna may exceed 200' in height.
- Control stations should use Yagi (directional) antennas when possible.
- Antennas should use the lowest gain possible.
- Control station power should be kept as low as possible.

Procedure

Any agency wanting to use one or more control stations at the same location is only permitted to use that configuration if the design is compliant with this SOP. The process for obtaining permission is to submit a written request for control station usage to the Lead Agency Director.

- The request shall describe the location, desired talkgroups/channels, antenna height, power, antenna type, antenna gain and feed line type of each control station.
- The Lead Agency may approve, deny or request modifications to the request.

Management

The Lead Agency will manage this policy.

Each Dispatch Agency Manager will ensure their personnel are properly trained on the use of control stations for gateway patching.

6.5 Required Monitoring of Interoperability Channels

Purpose or Objective

Establishes procedures for monitoring mutual aid/interoperability channels at communications centers and command posts.

Operational Context

Monitoring of mutual aid channels is imperative for the benefit of users needing assistance. Many channels have been identified to use for interoperability but not all of them will be monitored when not in use. Due to the fact that these Statewide and National interoperable channels do not belong to any one agency, there is no channel 'owner' monitoring them. As a result, a designated monitoring center should be established in each Operational Area.

Protocol/Standard

Control One is the designated monitoring center in Orange County for all Statewide and National interoperability calling/hailing channels available. Control One will monitor and respond to any unit requesting assistance on the calling/hailing channel and assign an appropriate tactical channel as necessary.

Dispatch Centers are responsible for monitoring any Statewide or National Interoperable channel assigned to them for an incident. The local Dispatch Center will monitor and respond to any communications traffic on the assigned interoperable channel until the completion of the incident.

Once the incident has been terminated and the interoperable resource is no longer needed, the Dispatch Center will notify Control One and release their responsibility for monitoring the tactical channel.

Management

The Lead Agency will manage this policy. The Emergency Communications Coordinator will work with Control One to identify specific interoperable channels to be monitored 24/7 by Control One.

Each Dispatch Agency Manager will ensure their personnel are properly trained on the use of Statewide and National interoperability resources.

7.0 MAINTENANCE RESPONSIBILITIES

7.1 System Maintenance

Purpose or Objective

Defines the System maintenance responsibilities and roles. The maintenance levels for the 800 MHz Radio System and its subsystems shall be set to a standard to protect the overall functionality and integrity of the System for all users.

Operational Context

The 800 MHz CCCS System is a complex network of radio sites and equipment that require highly trained engineering and technical personnel to constantly monitor the System and intervene as required to prevent System failure and quickly restore the System should any equipment experience failure. The CCCS Governance Committee has designated the Lead Agency as the primary agency responsible for the maintenance of the System. Agreements between the Lead Agency and maintenance contractors are at the Lead Agency's discretion, but the Lead Agency is ultimately responsible for the System maintenance.

Recommended Procedure

Any maintenance issues affecting the System will be addressed and resolved by the Lead Agency. The Lead Agency may, at its discretion, involve contract vendors in the process as necessary

For emergency and urgent repairs, the Lead Agency may request and expect cooperation from support resources (e.g. – support staff and/or parts) from other agencies to restore equipment/systems to normal operation.

For day-to-day maintenance, the Lead Agency or its contract vendor shall maintain the equipment.

Repair of any equipment not normally maintained by the Lead Agency requires the notification and consent of the owning agency.

The Lead Agency and/or their contracted service providers are responsible for:

- FAA registrations, FCC ASR registrations and FCC licenses, ensuring that equipment is properly licensed and copies of the licenses are posted at the sites as required by regulations.
- Maintaining equipment within the limits of County of Orange FCC licenses.
- Notifying the responsible personnel of equipment and location issues that require attention.
- Managing the inventory of the radio subscriber and infrastructure equipment.
- Ensuring that equipment at the tower sites that is not part of the System inventory shall be clearly labeled to indicate agency ownership.
- Routine equipment maintenance logs are kept at the sites.
- Maintaining current copies of all as-built documentation at each site and at the Lead Agency office. Lead Agency is responsible for ensuring the accuracy of all as-built data related to the infrastructure equipment and any changes shall be immediately documented. Lead Agency shall distribute the updated information as required.
- Coordinating, implementing and/or overseeing configuration changes affecting the System infrastructure.

- Any work being scheduled affecting the System and/or subsystems performance and reasonable notification to the System's users of same.
- Ensuring all technicians assigned to work on System equipment have successfully completed appropriate training on the equipment. Training requirements are referenced in the training section of the SOP.
- Following a preventive maintenance plan as defined in the preventative maintenance section of the manufacturers' manuals.
- Maintaining a list of the qualifications and contact information of technical staff in the event of an emergency.
- Maintaining a list of the available spare parts/equipment pertaining to the System and subsystems.
- Ensuring any equipment upgrades or changes affecting normal operations of the System are discussed and approved by the Governance Committee.
- Determining how critical an equipment failure is operationally, determining the appropriate action, and escalating or de-escalating the repair process as needed.

Management

The Lead Agency is responsible for managing the maintenance of the System equipment and sites and managing the repair responsibilities in emergency situations.

7.3 Maintenance / Repair Notifications

Purpose or Objective

Defines the procedure for notifications of scheduled and unanticipated maintenance activities having an impact on normal System operations, System interruptions, and System outages.

It is the policy of the Lead Agency to provide guidelines for user notifications for any maintenance actions having a potential for System interruptions.

Technical Background

Typically, equipment functionality can change when hardware and software configuration alterations or other maintenance activities are performed. Advanced notification of planned maintenance activities that impact the normal operation of the System allows user agencies and subscribers to make preparations as needed. Notification will also be made to user agencies when a catastrophic failure happens.

If the notification process is difficult and lengthy, it can become a barrier to making notification to user agencies.

Failure to make proper notification to user agencies can result in unneeded confusion, disruption or loss of public safety communications, and possible compromise of any special operations communications.

Operational Context

Affected agencies shall be notified of maintenance activities that impact their subscribers on the System. Agency notification of radio maintenance activities to their individual subscribers is at the discretion of the user agency's designated representative.

Protocol / Standard

The Lead Agency is responsible for monitoring the System on a 24-hour basis, through various methods including on-site staff in the System Watch unit. Maintenance activities, planned or unplanned, that could impact the subscribers usage of the System requires notification to the affected agency's radio representatives.

In the event of planned maintenance, all efforts should be made to conduct this type of activity during off-peak hours where radio utilization is as low as possible. If an emergency or high priority incident is in progress at the time of scheduled maintenance, it may be necessary to reschedule or delay the maintenance until the situation has stabilized and can be safely moved to alternate talkgroups or channels.

Procedure

A reasonable advance notice shall precede planned maintenance activities that affect the agencies using the System. The notification methods shall be by phone, e-mail, radio, or any combination of the same. The notification will consist of:

- The type of planned maintenance activity.
- When the maintenance will be conducted.
- The amount of time anticipated to complete the activity.
- The anticipated impact to the System and subsystems.

If a known activity has a significant operational impact upon any specific agency, a confirmation of receipt of notification shall be obtained. It is the responsibility of the Lead Agency to ensure that all affected users are notified will in advance of any such operations. Whenever possible, these operations shall be scheduled when the normal radio traffic is slowest.

Prior to commencing the maintenance operation, personnel from the Lead Agency shall coordinate with Control One to contact each affected dispatch center's supervisor for a last minute situational briefing.

Once maintenance operations begin, if dispatch operations recognize a need to terminate the operation, or if unexpected problems occur, a communications supervisor must call Control One to have the technical staff notified of the situation.

Unanticipated maintenance or equipment failures affect the agencies on the System and require notification to the affected agency's radio representative.

Upon notification of an equipment outage, Lead Agency technical staff is expected to:

- Determine the impact of the impairment to the operation of the System. A minor failure is something that either does not affect or minimally affects user functionality. A major failure is something that seriously affects or risks user functionality of the System.

- Determine if there are internal or external factors that alter the priority of System impairment, such as weather, subscriber loading unique public safety activities or impending events, etc.
- Determine if manual intervention is required. A serious failure requires initiating repair processes regardless of the time of day. Minor failures can wait until normal business hours or other convenient time before repair. The determination is at the discretion of the Lead Agency, and shall be based on internal System functionality and external subscriber needs.
- Determine if additional external resources are required.

Once the operation or repairs are complete, Lead Agency personnel shall contact Control One for an update and user feedback.

When requested by the Governance Committee, the details of the recovery processes may be reviewed for improvements.

Management

The Lead Agency is responsible for maintaining this policy and ensuring representatives from all affected agencies are notified as appropriate. Each agency's radio representatives are responsible for notifications within their respective agencies.

7.4 System Coverage

Purpose or Objective

Establishes the requirements for regular outdoor testing and verification of System signal quality and coverage.

Technical Background

Signal coverage of the System fluctuates constantly and is influenced by many conditions including but not limited to:

- Terrain.
- Weather.
- Vegetation.
- Building Construction.
- Equipment Condition.
- Location.

Regular sampling of signal quality and strength at pre-designated locations will help to confirm adequate coverage, or if a problem might have developed in certain locations due to changes in one of the above conditions.

Operational Context

Periodic coverage testing is a critical component of System operation and maintenance, and will continue toward identifying and mitigating any signal coverage issues, including any potential effects of new building construction and development.

Protocol / Standard

Lead Agency staff performs comprehensive signal coverage test to evaluate the System's signal strength and quality across the service area. The locations and number of individual test points shall be based on the area's building density and known areas of poor coverage.

The results of each test will be compared to previous results and monitored for signal degradation. Test results will be stored on a shared data server for historical comparisons.

Management

The Lead Agency Director oversees the process, evaluates the results, develops remediation strategies, and reports significant findings to the Governance Committee.

7.5 Repair Parts Inventory

Purpose or Objective

Establishes an inventory control procedure for infrastructure and subscriber repair parts.

It is the policy of the Lead Agency to ensure that planning is in place and available resources identified to expedite the recovery of the System and related components in the case of disaster, catastrophic failure or other major incident that affects operations of the System.

Operational Context

Lead Agency will maintain an inventory of spare parts for regular repairs to the System and subscriber radios.

Protocol / Standard

The spare parts inventory for infrastructure and subscriber units shall be kept at Lead Agency facilities for ready access when needed.

Management

The Lead Agency maintains and manages the repair parts inventory.

7.6 Disaster Recovery

Purpose or Objective

Establishes the minimum requirements for a System disaster recovery plan.

It is the policy of the Governance Committee and Lead Agency to ensure that planning is in place and resources identified and available to expedite the recovery of the System and related components in the case of disaster, catastrophic failure or other major incident that affects operations of the System.

Operational Context

Lead Agency personnel will maintain a comprehensive plan for restoration of the System during times of disaster. If the Operational Area EOC is activated, the Emergency Communications

Coordinator (ECC) must be notified of any System problem so that it can be logged into WebEOC.

Management

The Lead Agency maintains and manages the Disaster Recovery Plan.

8.0 SITE AND SYSTEM SECURITY

8.1 Site Security

Purpose or Objective

Establishes the minimum requirement to provide site security and protect the integrity of the System's radio towers equipment shelters and equipment.

Technical Background

Security measures have the overall benefit of protecting the functionality, integrity and operation of the System. Details of specific security measures cannot be placed within a public document as this would compromise measures used in monitoring and maintaining security.

Operational Context

The physical security of equipment, facilities, and structures making up the core of the radio System infrastructure is paramount to the reliability and availability of communications carried on the System. Each site is within a fenced, gated and locked compound, with shelter entry monitored and reported to a central monitoring point. A remote controlled camera systems are installed and monitored for any unauthorized entry or security concerns.

Protocol / Standard

Access to the sites are tightly controlled and entry to those sites is granted only to those personnel with proper authorization from the Lead Agency. All personnel requiring site access must be accompanied by Lead Agency staff. Unaccompanied access to any System site is not authorized. Entry alarms for the remote sites are received at Systems Watch and sent immediately to Lead Agency technical support staff.

Procedure

Notification to Lead Agency Technical staff and Systems Watch is required of all agencies and vendors prior to gaining site access. Any person requiring access to the tower sites for any reason shall have full clearance from the Lead Agency and be accompanied and monitored by Lead Agency personnel while on site. Law enforcement personnel will be immediately notified and dispatched to any site with unexpected or unexplained alarms or unidentified personnel viewed remotely from the camera systems.

Any agency or vendor requiring access to any tower site or equipment location shall make immediate notification to the Lead Agency of urgent issues such as discharged employees or cancelled contracts.

When a site has been vandalized or broken into, the jurisdictional law enforcement agency should be notified. The person who discovers the event has the responsibility to preserve the crime scene and not contaminate it. He/she should have Systems Watch log the time when the event was discovered and any other pertinent information relating to the site/scene. Systems Watch should notify the appropriate local law enforcement agency as well as the Orange County Sheriff's Department Watch Commander and Control One. Other agencies may be notified if they own equipment at the site. Lead Agency will notify all affected agencies as soon as possible.

When the site is off the air due to a crime, the technician should refrain from making entry unless permission has been given by the Lead Agency Director due to extreme circumstances taking place that requires coverage from the site.

If a radio technician should arrive at a site and an unauthorized vehicle or person is on the property, they should back off, notify Systems Watch and call 911. The technician should give the 911 call taker the street address and advise them of the situation. If there is no cell service on site, the technician should radio the information to Systems Watch and request law enforcement response. Systems Watch personnel should immediately contact the appropriate law enforcement agency to request response. Systems Watch personnel will also notify Lead Agency supervisors and management. At no time should the technician put themselves at risk of harm.

If a technician has to respond to a vandalized remote site after normal business hours, it is recommended for safety reasons that a minimum of two persons respond to the site. Law enforcement may be requested to go to the site with the technician.

Management

The Lead Agency Director is responsible for managing this procedure.

8.2 Network Operational Security

Purpose or Objective

Establishes the specific security measures for System and subsystem equipment and to define site security policy.

Technical Background

Security measures have the overall benefit of protecting the functionality, integrity and operation of the System. Details of specific security measures cannot be placed within a public document as this would compromise measures used in monitoring and maintaining security.

Protocol / Standard

All items identified as 'Restricted Information' will be maintained in secure areas within the control of the Lead Agency and is not available outside of the Lead Agency except by formal written request.

Technical information that can compromise System security is considered 'Restricted Information'.

The System's network is protected from other data networks by isolation or by using System manufacturer specified and configured firewall with the approval of the Lead Agency.

All remote access points to the System are kept secure and are coordinated with the Lead Agency.

Passwords protect the System and subsystem equipment for the purpose of preventing unauthorized access to equipment. The Lead Agency issues and manages the passwords.

User login accounts are protected with passwords providing an appropriate level of protection. If a password is suspected of being compromised, it must be immediately updated or the user account will be disabled pending resolution.

External devices (computers, modems, routers, data storage, etc.) shall not be connected to the System network, computers, or consoles without the approval of the Lead Agency Director. Any such device must also be supplied, supported, and maintained by the user Agency's Information Technology department or service provider to ensure the most current device security software and virus protection is in place.

At no time will any personally owned device be connected to any port or connector on the System. Any such action may result in the immediate revocation of access privileges for the offender and/or agency.

It is recommended that computers used for programming or maintenance not be connected to the internet to help reduce possibility of virus infection.

A 'Group Policy' shall be implemented on the System to prevent the use of external USB ports on all dispatch consoles.

Procedure

All agencies, contractors, and personnel that require access to Lead Agency controlled sites, equipment or networks must pass a comprehensive background check before access is allowed and must be accompanied by Lead Agency staff while on site.

Violations of System security policy or procedures may jeopardize the System and result in the loss of a technician's, agency's or vendor's privileges to access the System.

System documentation is classified as 'Restricted Information'.

Management

The Lead Agency Director is responsible for the network, equipment, and site security of the System.

8.3 Software, Firmware and Document Security

Purpose or Objective

Establishes the minimum security measures and procedures to protect the integrity of the System software and programming.

Technical Background

The documentation, service and technical manuals, databases, spreadsheets and software of the System contain critical operational and technical information that could compromise the System if obtained by unauthorized personnel and is classified as 'Restricted Information'.

Operational Context

The documentation and software of the System changes as the System evolves. Those changes and revision must be documented and maintained in a central location for quick and easy access for the technical support staff.

Protocol Standard

In the best interest of public safety, all documentation, service and technical manuals, databases, spreadsheets and software of the System are considered 'Restricted Information'.

Software relating to the programming of any System component shall only be installed on authorized government owned computers or Lead Agency authorized contractors' computers.

Procedure

All items identified as 'Restricted Information' will be maintained in secure areas within the control of the Lead Agency Director. These items will only be shared with those who require knowledge of it for operational purposes. This information is not available to anyone outside of the Lead Agency. An exception may be made with a formal written request and approval from the Governance Committee. This information is not to be released to any personnel who do not have a legitimate and appropriate need for it.

Management

The Lead Agency Director is responsible for managing this procedure.

9.0 APPENDIX

9.1 Lead Agency Contact Information

Normal Working Hours – Monday-Friday 7:30AM – 4:30PM

Customer Service – 714-704-7999

- Radio repair request
- Radio programming request
- Radio/accessories purchase request
- Dispatch console repair request

Systems Watch – 714-628-7020

- Lost/Stolen radio notification
- Radio deactivation
- Radio transmission history/statistics

After Normal Working Hours

Systems Watch – 714-628-7020

- Lost/Stolen radio notification
- Radio System coverage issues
- Emergency radio repair requests
- Emergency dispatch console repair requests

Control One – 714-834-7008

- Operational issues
- Request restricted talkgroup assignment
- Interoperability assistance
- Emergency radio or console repair requests

Physical Address:

OCSD/Technology Division – Administration & Radio Repair

840 N. Eckhoff St.
Suite 104
Orange, CA 92868

9.2 Glossary – Definitions and Acronyms

Item / Acronym	Definition
700MHz	For Public Safety LMR, digital P25 voice radio channels between 769/775 MHz and 799/805 MHz. Channels have 30 MHz seperation between Tx & Rx when repeated. FCC designated low power channels can be used analog voice.
7CALL / 7TAC	Nationwide 700 MHz Calling and Tactical channels
800MHz	For Public Safety LMR, analog or digital voice or data radio channels between 806/816 and 851/860 MHz. Channels have 45 MHz seperation between Tx & Rx when repeated.
8CALL / 8TAC	Nationwide 800 MHz Calling and Tactical channels
ACU-1000	An audio gateway device capable of connecting disparate radio systems, channels, or talkgroups together during on-scene operations, similar to a console patch between talkgroups
AES	Advanced Encryption Standard
Alias	A common alphanumeric name used to identify a radio, talkgroup, site, etc. rather than referencing the assigned 6 digit ID number
ANSI	American National Standards Institute
APCO	Association of Public-Safety Communications Officials
APCO P25	A public-safety digital radio standard

Item / Acronym	Definition
ASK	Advanced System Key
BDA	Bi-Directional Amplifier, relays radio signals into and out of a building
BER	Bit Error Rate
CCCS	Countywide Coordinated Communications System
Channel	A pair of frequencies, transmit and receive, that are used for a single communications path
Channel Bank	A device that combines multiple data and/or audio inputs into TDMA format so that it can be transmitted over microwave or T1 circuit and shared between transmitter sites
Code plug	The file containing a specific radio's programming parameters
COMC	Communications Coordinator
COML	Communications Unit Leader
COMT	Incident Communications Technician
Console Patching	Ability to connect channels via dispatch consoles
Consolette	A mobile radio mounted into a case with power supply and converted for desk-top use
Control Station	An installed radio unit, sometimes a mobile radio, normally found at a desk or common work area indoors or directly connected to a console or other fixed transmitting location
DAS	Distributed Antenna System, relays radio signals into and out of a building
Digial radio	Digital radios turns sound (by signal processing) into patterns of digits (numbers) rather than the radio waves which are used for analog transmissions.
Dispatch Console	A fixed radio operator position with multiple radio resources and features that can access any subset of talkgroups and/or conventional channels
ECC	Emergency Communications Coordinator
EIA	Electronic Industry Alliance
EMS	Emergency Medical Services
EOC	Emergency Operations Center
FAA	Federal Aviation Administration
FCC	Federal Communication Commission
Fixed	Radio equipment that is installed at a radio site or dispatch center
Fleetmap	The master spreadsheet plan of the talkgroups, zones, Failsoft assignments, alias information and other pertinent System and radio programming
FM	Frequency Modulation
Gateway	A device that allows two or more radio or voice devices to be connected together
IAP	Incident Action Plan

Item / Acronym	Definition
IC	Incident Command
ICALL	Calling Channel for ITAC
ICC	Incident Communications Center
ICP	Incident Command Post
ICS	Incident Command System
ICS 205	Incident Radio Communications Plan
ICS 217	Communications Resource Availability Worksheet
ID	Identification
Infrastructure	All of the fixed electrical and mechanical equipment, towers and building structures, generators, transmitters, controllers, antennas, microwave and ancillary equipment that comprise the operational backbone of the radio System
Inter-agency	Located or occurring between two or more agencies
Interoperability	The ability of Public Safety responders to share information via voice and data communications systems on demand, in real time, when needed, and as authorized.
Interoperable	Ability of a system to use the parts or equipment of another system
ITAC	Conventional mutual aid channel 800 Mhz
ITS	Information Technology Services
IUID	Item Unit Identification number is a unique number assigned to each individual subscriber radio authorized to have access to the System.
Lead Agency	Agency primarily responsible for maintenance, management, operation and enhancement of the CCCS System. The CCCS Governance Committee has designated the Orange County Sheriff Department Technology Division as the Lead Agency.
LMR	Land Mobile Radio
Logging	The act of recording radio conversations for replay as required
MCC	Mobile Communicaiton Center
MCU	Mobile Communications Unit
MCV	Mobile Communications Vehicle
MHz	Abbreviation for megahertz. 5 MHz = 5,000,000 Hz or 5,000 kHz. A unit of measure for the number of times a frequency makes one complete cycle in one second
Mission Critical	For mission critical applications, users have an expectation of "immediate" communication with their dispatch or command center and little to no end-to-end audio delays.
Mobile Radio	A vehicular mounted radio with an power source and antenna
Mutual Aid	Personnel, equipment, or services provided to another jurisdiction

Item / Acronym	Definition
NECP	National Emergency Communications Plan
NGOs	Non-Governmental Organizations
NIMS	National Incident Management System
OCCOPSA	Orange County Chiefs of Police and Sheriff's Association
OTAP	Over the Air Programming
OTAR	Over the Air Rekeying
P25	A suite of standards for digital radio communications for use by federal, state and local public safety agencies in North America to enable them to communicate with different vendor radio systems using a common platform
Patch	Electrically connecting two or more radio channels or talkgroups so that those users of those separate resources are able to communicate with each other
POC	Point of Contact
Portable	A lightweight, completely self-contained radio unit usually worn on user's belt
Public Safety	An agency, department, or individual directly involved with the health, safety, and/or security of the public including, but not limited to police, fire, emergency management, and medical personnel and responders
Public Service	An agency, department, or individual involved with providing non-emergency type services to the public including, but not limited to utilities, transportation, education, and other governmental services, supporting public safety
Restricted Information	Documentation, service and technical manuals, databases, spreadsheets and software of the System containing critical operational and technical information that could compromise the System if obtained by unauthorized personnel. All items identified as 'Restricted Information' will be maintained in secure areas within the control of the Lead Agency and is not available outside of the Lead Agency except by formal written request.
RF	Radio Frequency
SCIP	Statewide Communications Interoperability Plan
SEOC	State Emergency Operations Center
Simplex	Radio to radio communications on one frequency. Also called Direct
Simulcast	A type of radio communications in which voice communications are transmitted from multiple radio sites and can be received simultaneously by field units to provide wide area coverage
Site	The physical location of an antenna tower, equipment shelter and radio System infrastructure equipment
SOP	Standard Operating Procedure
SOW	Site on Wheels
Subscriber Unit	A mobile, hand held or control station radio used on a trunked radio system
System User	An individual operating a radio authorized to access the System.

Item / Acronym	Definition
System Watch	Lead Agency unit responsible for 24/7 monitoring of CCCS and responding to any System issues. This includes notifications, troubleshooting, callouts, repair, etc., resulting in System restoration.
TAC	Tactical on scene operation
Talk Around	Radio to Radio communications on one frequency, usually the same frequency on which a repeater transmits. Simular to Direct or Simplex
Talkgroup	Term ususally used with trunked radio systems. A talkgroup is a predefined list of radios/users assigned a unique ID which allows them to communicate with each other over a trunked radio system.
Talkgroup Alias	Abbreviated naming of the talkgroup to fit within the 8 or 14 character radio display
Talkgroup Failsoft Channel	The system channel designated for a talkgroup when in the failsoft mode
Talkgroup ID	Numerical designation of the talkgroup in decimal and/or hexadecimal
Talkgroup Name	Name of the talkgroup as it is programmed into the system
TIA	Telecommunications Industry Association
Trunking/Trunked	The automatic and dynamic sharing of a number of communications channels between large numbers of radio users
UHF	Ultra High Frequency – Range of 300 to 3,000 MHz for public safety LMR usually refers to two bands. 380 to 460 MHz (low) and 460 to 512 MHz (high).
UPS	Uninterruptible Power Source – a battery back-up device that provides emergency power to connected equipment when utility power is not available.
User Agency	An agency authorized to operate a radio on the System.
VHF	Very High Frequency – For public safety LMR, usually refers to VHF High Band with a range of 136 to 164MHz. VHF Low Band has a frequency range below 100MHz.
Zone	An area in the radio / template containing positions for 16 individual talkgroups or conventional radio channels which is normally labeled by an acronym that closely represents the owner agency