

BayRICS Authority
STAFF REPORT

DATE: Thursday August 14, 2014
TO: BayRICS Board of Directors
FROM: Barry Fraser, General Manager
SUBJECT: Item 8 – Regional P25 System Key Exchange Guidelines

RECOMMENDATION:

Endorse the System Key Exchange Guidelines as a model for the Bay Area; direct staff to distribute the Guidelines to BayRICS Members and Bay Area public safety agencies; and encourage agencies to implement the Guidelines as part of their P25 radio programming procedures.

Purpose

BayRICS staff and Technical Advisory Committee recommend that the BayRICS Board of Directors endorse the attached *System Key Exchange Guidelines* (Guidelines) and encourage BayRICS Members to implement the Guidelines to enhance interoperable public safety communications in the Bay Area.

The Guidelines set forth uniform radio programming parameters and a process for exchanging secure system encryption data for each Bay Area P25 sub-system operating a 700/800 MHz P25 trunked radio network. These recommended programming procedures will facilitate rapid and seamless radio operation across P25 systems to enhance interoperable communications during mutual aid incidents.

By endorsing these model guidelines, the BayRICS Authority encourages its Members and Bay Area public safety agencies to adopt the Guidelines and incorporate them into each agency's radio programming procedures. Each agency's decision to implement the Guidelines remains purely voluntary at this time.

Staff wishes to acknowledge a working group of representatives of the following San Francisco Bay Area Project 25 (P25) system operators (collectively, the "Participating Agencies"), who were instrumental in the development of these Guidelines:

- Bay Area Rapid Transit (BART)
- East Bay Regional Communications System Authority (EBRCSA)
- Golden Gate Bridge, Highway and Transportation District (GG Bridge)
- Marin Emergency Radio Authority (MERA)

- City of Oakland (Oakland)
- City and County of San Francisco (San Francisco)
- San Mateo County Information Services Division (SMISD)
- Silicon Valley Regional Interoperability Authority (SVRIA)

Funding for the development of the Guidelines was provided through the cooperation of Counties of San Mateo, Alameda and Contra Costa, City of San Jose and City and County of San Francisco. Technical support and development of the key numbers, talkgroup IDs and individual ID ranges was provided by CDX Wireless, Inc. through a contract with San Mateo County.

Background

BayRICS was established in August 2011 to oversee advanced public safety communications projects in the San Francisco Bay Area. BayRICS provides technical assistance and tools (such as these model guidelines) to enhance operability and interoperability of its Members' wireless voice and data networks, which will be used by over 25,000 first responders to protect the life and property of 7.5 million Bay Area residents and 16 million visitors annually.

In September 2012, the BayRICS Authority endorsed the "Fleetmap" Interoperability Guide as the region's blueprint for allocating channels and assigning talkgroups among P25 systems operating on the 700/800 MHz spectrum ranges. These Guidelines build on that collaborative effort by developing model system key sharing parameters to facilitate programming systems and radios for more effective interoperability.

The Guidelines were developed between January and June 2014, through a series of collaborative meetings of an advisory group established by BayRICS General Manager and made up of representatives of the Participating Agencies. The advisory group, the BayRICS Technical Advisory Committee (TAC), and participating P25 System Operators recommend the adoption of these Guidelines by the region.

P25 Radio Systems and System Keys

Each of the Participating Agencies, except MERA, operates a standards-based P25 trunked radio system, which primarily provides voice radio service to public safety and service agencies within their geographic footprint. Although MERA does not currently operate a P25 trunked system at this point in time, it is in the planning stages to deploy a P25 system in the near future.

The Bay Area P25 systems assign a unique unit ID to each radio on the system to allow programming of individual operating parameters and permissions for each radio. The Guidelines establish the agency unit ID ranges, as well as parameters for system talkgroups that are intended to be used for interoperability purposes between multiple

agencies and disciplines. The talkgroup parameters should be programmed into Participating Agency radios to facilitate interoperable communications across P25 systems.

When operating across P25 systems (for example, during mutual aid support) many radio systems require a system key to “unlock” full programming capabilities. Without this key, the user can alter only minor parameters within the radio. With a system key in place, the user can program crucial parameters, such as entering and manipulating other system talkgroups to facilitate interoperability. However, these system keys contain sensitive security information that should not be shared or disclosed without proper protocols established.

Implementation of the Key Exchange Procedures

The Guidelines establish a process for the secure exchange of system keys among Participating Agencies. As subscriber radios are programmed for the field, each Participating Agency will provide one system key to all other Participating Agencies. Each system key will be configured with specified system ID, talkgroup ID ranges, and individual ID ranges.

In exchange for receiving system keys from other Participating Agencies, each agency agrees to various security protocols and best practices to ensure the integrity and security of each system. In addition, hardware-based, system keys shall be configured to expire six months from creation, to further minimize security concerns.

The Guidelines also propose a non-binding, issue resolution process to resolve questions and implement future change requests related to the key exchange process.

Recommendation

Staff recommends that the BayRICS Board of Directors endorse the System Key Exchange Guidelines as a model for the Bay Area, direct staff to distribute the Guidelines to BayRICS Members and Bay Area public safety agencies and encourage agencies to implement the Guidelines as part of their P25 radio programming procedures.

A copy of the Guidelines (with sensitive security information redacted) begins on the following page.

BAY AREA REGIONAL PROJECT 25 PUBLIC SAFETY RADIO SYSTEMS

MODEL PROGRAMMING GUIDELINES:

SYSTEM KEY EXCHANGE GUIDELINES

Version 1.5: July 21, 2014

Purpose

These interoperability guidelines (Guidelines) have been developed and endorsed by the Bay Area Regional Interoperable Communications System Joint Powers Authority (BayRICS) as model guidelines to enhance Project 25 (P25) system interoperability and coordination among the following San Francisco Bay Area public safety agencies: Bay Area Rapid Transit (BART), East Bay Regional Communications System Authority (EBRCSA), Golden Gate Bridge, Highway and Transportation District (GG Bridge), Marin Emergency Radio Authority (MERA), the City of Oakland (Oakland), City and County of San Francisco (San Francisco), San Mateo County Information Services Division (SM ISD), and the Silicon Valley Regional Interoperability Authority (SVRIA), collectively known as the “Participating Agencies.” The purpose of the Guidelines is to facilitate mutual aid response by ensuring that the programming of each Participating Agency’s 700/800 MHz P25 trunked radio systems allows rapid and seamless activation of interoperability talkgroups for mutual aid communications. BayRICS Authority strongly urges each Participating Agency to adopt these Guidelines and incorporate them into its Agency radio programming procedures.

Background

BayRICS was established in August 2011 to oversee public safety communications projects in the San Francisco Bay Area. Members of BayRICS include the State of California, City and County of San Francisco, City of Oakland, City of San Jose, Counties of Alameda, Contra Costa, Marin, San Mateo, Santa Clara, Sonoma, and “hub” cities in the East Bay and South Bay. BayRICS provides technical assistance and tools (such as these model guidelines) to enhance operability and interoperability of its Members’ wireless voice and data networks, which will serve over 25,000 first responders to protect the life and property of 7.5 million Bay Area residents and 16 million visitors annually.

In September 2012, the BayRICS Authority endorsed the “Fleetmap” Interoperability Guide as the region’s blueprint for allocating channels and assigning talkgroups among P25 systems operating on the 700/800 MHz spectrum ranges. These Key Exchange Guidelines build on that collaborative effort by developing model system key sharing guidelines to facilitate programming systems for more effective interoperability.

The Guidelines were developed through a series of collaborative meetings of an advisory group established by BayRICS General Manager and made up of representatives of the Participating Agencies. Funding for technical review and drafting support was provided through the cooperation of Counties of San Mateo, Alameda and Contra Costa, City of San Jose and City and County of San Francisco.

The advisory group and the BayRICS Technical Advisory Committee (TAC) recommend the adoption of these Guidelines by the region.

P25 Radio Systems

Each of the Participating Agencies, except BayRICS and MERA, operates a standards-based P25 trunked radio system, which primarily provides voice radio service to public safety and service agencies within their geographic footprint. Although MERA does not currently operate a P25 trunked system at this point in time, it is in the planning stages to deploy a P25 system in the near future.

Individual radios operating on these systems are assigned a unique unit ID to identify them as well as assign operating parameters and permissions on these systems. The Participating Agencies systems and their individual ID ranges are listed in Exhibit 1.

Each existing system maintains a series of talkgroups that are intended to be used for interoperability purposes between multiple agencies and disciplines. The interoperability talkgroup IDs for each existing system are listed in Exhibit 2. These interoperability talkgroups will be programmed into Participating Agency radios to facilitate interoperable communications and render mutual aid.

P25 System Keys

Radios are programmable via a software program and hardware interface. Many radio systems require a computer file or hardware “dongle” called a system key to “unlock” full programming capabilities. Without this key, the user can alter only minor parameters within the radio codeplug or programming. For example, without a system key, a user may be able to alter scan lists, enable backlight, or label existing talkgroups. With a system key in place, the user can program crucial parameters, such as entering and manipulating trunking talkgroups in the codeplug.

To provide a more secure solution for programming of radios region wide, the BayRICS Authority and Technical Advisory Committee recommend implementing hardware-based system keys, when available from the radio manufacturer.

Implementation

For subscriber unit programming, each Participating Agency will provide one system key to all other Participating Agencies. System keys will be developed corresponding with the Key Number denoted in Exhibit 3, seven from each Participating Agency. Each system key will be configured with the system operator’s system ID numbers, talkgroup ID ranges, and individual ID ranges as shown in Exhibit 3. Hardware-based system keys shall be configured to expire six months from creation.

In exchange for receiving system keys from other Participating Agencies, each agency agrees:

- To destroy all copies of previous software keys from other Participating Agencies in their possession.
- That the key will only be used by employees who are technically qualified to program, develop, modify and implement code plugs / templates for the local agency.
- That should a radio be lost or stolen, it is incumbent that the lost or stolen radio ID be reported to all other Participating Agencies.
- To take reasonable precautions to secure the key from theft and unauthorized use.

- To notify the owning agency in the event of loss or theft of a system key.
- That in the event of a dispute or technical issue, any participating agency can request a meeting of all participating agencies by sending notice to the BayRICS general manager. The BayRICS general manager will then set up and facilitate a meeting within 30 days to assist in resolving the dispute or technical issue.
- That before authorization of the individual radio IDs is allowed, each Participating Agency agrees to provide a complete list of subscriber units which includes Radio Unit ID, Serial Number, Radio Model, Radio Unit ID Alias, Electronic Serial Number (if requested), Asset Tag (if requested), and Assigned Agency or Department. This list is to be kept current by each Participating Agency as subscriber units are added, subtracted, and/or reassigned. Participating agencies agree to provide an updated list to all other Participating Agencies within 3 days of any change in subscriber units.
- To designate a Point of Contact (POC) for coordinating with other Participating Agencies, and to inform Participating Agencies of any changes to the designated POC. Points of contact for each agency for the purposes of key exchange and radio unit ID authorization are listed in Exhibit 4.

Participating Agencies acknowledge that any failure to provide system keys or comply with any implementation provision may negatively affect critical public safety operations within other Participating Agencies. Therefore, each Participating Agency will make all reasonable best efforts to comply with all implementation provisions specified in this Section to the best of their abilities.

Each Participating Agency reserves the right to recover their key hardware at any time.

Issue Resolution Process

The following process may be used to resolve issues related to the Key Exchange guidelines.

Step 1: Impacted Participating Agencies should first meet and attempt to resolve the issue amongst themselves.

Step 2: If the agencies cannot resolve the issue, a Participating Agency may bring the unresolved issue to the BayRICS General Manager, who will schedule a meeting of an advisory group to discuss solutions to the issue. The advisory group will consist of the Participating Agency POCs (or their designated representatives) identified in Exhibit 4.

Step 3: If the advisory group cannot resolve the issue, the BayRICS General Manager will place the issue on the agenda for the next BayRICS Technical Advisory Committee (TAC) meeting. The TAC may make recommendations for the resolution of the issue, but does not have the authority to compel any participating agency to follow or adhere to the recommendations. The BayRICS General Manager will inform the BayRICS Authority Board of Directors of the TAC recommendations at the following Board meeting.

EXHIBIT 1
PARTICIPATING AGENCY SYSTEM ID RANGES

[EXHIBIT 1 INCLUDES CONFIDENTIAL AND SECURE INFORMATION RELATED TO PUBLIC SAFETY RADIO SYSTEMS. THIS INFORMATION HAS BEEN REDACTED]

EXHIBIT 2
PARTICIPATING AGENCY SYSTEM INTEROPERABILITY TALKGROUP IDS

[EXHIBIT 2 INCLUDES CONFIDENTIAL AND SECURE INFORMATION RELATED TO PUBLIC SAFETY RADIO SYSTEMS. THIS INFORMATION HAS BEEN REDACTED]

EXHIBIT 3
PARTICIPATING AGENCY SYSTEM KEY NUMBERS, TALKGROUP ID AND INDIVIDUAL ID RANGES

[EXHIBIT 3 INCLUDES CONFIDENTIAL AND SECURE INFORMATION RELATED TO PUBLIC SAFETY RADIO SYSTEMS. THIS INFORMATION HAS BEEN REDACTED]

EXHIBIT 4
PARTICIPATING AGENCY SYSTEM ID POINTS OF CONTACT

System Operator	Contact Name	Email	Phone
BART	Doug Ellis	[Redacted]	[Redacted]
EBRCSA	Bill McCammon	[Redacted]	[Redacted]
GG Bridge District	Joe Perez	[Redacted]	[Redacted]
Oakland	David Cruise	[Redacted]	[Redacted]
MERA	Shelly Nelson	[Redacted]	[Redacted]
San Mateo ISD	Bill Dunbar	[Redacted]	[Redacted]
San Francisco	Michelle Geddes	[Redacted]	[Redacted]
SVRIA	Bill McCammon	[Redacted]	[Redacted]