



NPSTC Report

Best Practices for Public Safety Interoperable Communications

**January 2017
(Updated May 2018)**

The National Public Safety Telecommunications Council is a federation of organizations whose mission is to improve public safety communications and interoperability through collaborative leadership.

The member organizations of the National Public Safety Telecommunications Council are grateful to the Department of Homeland Security's Science and Technology Directorate, Office for Interoperability and Compatibility (OIC), and the National Protection and Programs Directorate, Office of Emergency Communications (OEC), for their support.

TABLE OF CONTENTS

1. EXECUTIVE SUMMARY.....	1
2. OVERVIEW.....	4
2.1 BEST PRACTICES RELATIONSHIP TO STANDARDS AND REQUIREMENTS	5
2.2 USING BEST PRACTICES TO ENHANCE AND PROMOTE STANDARDS	5
2.3 COMBINING MULTIPLE BEST PRACTICES.....	5
3. BEST PRACTICE ELEMENTS	6
3.1 BEST PRACTICE STATEMENT	6
3.2 SCOPE OF THIS BEST PRACTICE	6
3.3 STATEMENT OF IMPORTANCE.....	6
3.4 SUPPORTING ELEMENTS.....	6
3.5 RELATIONSHIP TO SAFECOM INTEROPERABILITY CONTINUUM	7
3.6 USE CASE EXAMPLES	9
3.7 MIGRATION PATH.....	9
3.8 REFERENCE MATERIALS AND LOCATION	9
3.9 CONTRIBUTORS LIST	9
4. BEST PRACTICE DEVELOPMENT PROCESS.....	10
4.1 DISCUSSION AND REVIEW IN WORKING GROUP.....	10
4.2 FINAL DRAFT DEVELOPMENT	10
4.3 PEER REVIEW.....	10
4.4 ADOPTION OF BEST PRACTICE BY NPSTC GOVERNING BOARD.....	11
5. MAINTAINING BEST PRACTICES AND DEVELOPING NEW PRACTICES.....	11
6. CONTRIBUTORS TO THIS REPORT.....	11
7. APPENDIX	2
7.1 BEST PRACTICE #1 - NATIONWIDE INTEROPERABILITY CHANNEL NAMING AND USAGE.....	3
7.2 BEST PRACTICE #2- INTEROPERABILITY SYSTEMS CHANGE MANAGEMENT PRACTICES.....	8
7.3 BEST PRACTICE #3 - TRAINING AND PROFICIENCY IN THE MANAGEMENT AND USAGE OF INTEROPERABILITY EQUIPMENT AND SYSTEMS.....	14
7.4 BEST PRACTICE #4 - INTEROPERABILITY RELATIONSHIPS.....	21
7.5 BEST PRACTICE #5 - INFRASTRUCTURE MANAGEMENT	27
7.6 BEST PRACTICE #6 - CHANNEL ASSIGNMENT BASED ON INFRASTRUCTURE COVERAGE	33
7.7 BEST PRACTICE #7 - INTEROPERABILITY RESOURCES—AFTER ACTION REVIEWS	38
7.8 BEST PRACTICE #8 - RADIO DEVICE MANAGEMENT	50
7.9 BEST PRACTICE #9 - DEPLOYMENT FOR INTEROPERABILITY RESOURCES	58
7.10 BEST PRACTICE #10 - COMMUNICATIONS SPAN OF CONTROL	67
7.11 BEST PRACTICE #11 - MANAGING ENCRYPTION FOR INTEROPERABILITY RESOURCES	74
7.12 BEST PRACTICE #12 - RADIO CHANNEL ASSIGNMENT AND USE WITHIN HIGH RISK INCIDENT ENVIRONMENTS.....	81
7.13 BEST PRACTICE #13 - INTEROPERABILITY RESOURCES INFORMATION – STORAGE AND ACCESS.....	89

1. Executive Summary

Several major incidents in the U.S., including the death of 19 wildland firefighters in the State of Arizona and the Washington D.C. area Navy Yard shooting, focused attention on the need to define essential radio interoperability best practices involving daily operational use, system support and device programming, interoperability system management, and access, and training. During the writing of this report, other incidents including mass shootings in Las Vegas and Florida, the Santa Rosa and Chimney Top 2 wildfires, and several natural disasters such as Hurricanes Harvey, Irma, and Maria have underscored that need.



Granite Mountain Interagency Hotshot Crew/AP Photo/City of Prescott, Arizona

The National Public Safety Telecommunications Council (NPSTC) was requested to develop a set of communications interoperability best practices. The Radio Interoperability Best Practices Working Group (RIOBP), operating under the guidance of the Interoperability Committee, has developed a set of best practice statements using a standard template. Each statement records the best practice statement, a statement of importance, supporting elements, use cases, a migration path to meet the best practice, and how each relates to the SAFECOM Interoperability Continuum with regard to Standard Operating Procedures, Governance, Technology, Training/Exercise, and Usage.



The group was formed on May 29, 2014. Close to 200 members participated in the group and were asked to participate and review information as it was submitted and approved. The Working Group was chaired by Mark Schroeder, Communications and Infrastructure Manager, City of Phoenix.

The Working Group utilized the recommendations and information contained in dozens of incident After Action Reports that noted specific areas for improvement. The group

also reviewed regional and agency specific operating procedures to determine if strategic level best practices could be defined and recommended for buildout into a Best Practice Statement.

In many of the reports reviewed, common issues were identified that could be mitigated beginning at a strategic level. The Best Practices are designed for adoption by individual agencies and organizations at a strategic level.

It is important to note that these are Best Practice recommendations and are not intended to be standards or requirements. It is acknowledged that not all agencies operate in the same way and some agencies will not be able to fully implement these recommendations. This document articulates the Working Group's goal of the highest achievable level of interoperability based upon their experience and research, with the understanding that any step forward in the migration path is an improvement.

Technology changes rapidly and is expected to continue to do so in the future. Because of this, the Best Practice Statements are written at a strategic and policy level and will avoid technical content whenever possible. To extend the longevity of the reference information used in developing these Best Practices, the report will direct the reader to the location where supporting references can be found rather than post them directly into the report.

The Working Group identified 13 major topics during the development of their original scope of work. The completed Best Practices and the Best Practice statement explaining their intent are listed below. The full report on each Best Practice is included at the end of this master report. Each Best Practice is also available as an individual document on the Best Practice Working Group page of the NPSTC website at www.NPSTC.org, along with supporting information and reference material.

Best Practice #1 – Nationwide Interoperability Channel Naming and Usage

Nationwide Radio Interoperability Channels should be compliant with the current American National Standards Institute (ANSI) Standard designated names, frequencies, and technical information; and in accordance with the Federal Communications Commission (FCC) and National Telecommunications and Information Administration (NTIA) designated usage for that channel.

Best Practice #2 - Interoperability Systems Change Management Practices

Change management practices and policies should always be used to ensure that any changes to operational policies, system modifications, additions, or deletions of interoperability system infrastructure are communicated to all affected agencies.

Best Practice #3 - Training and Proficiency in the Management and Usage of Interoperability Systems

Radio Interoperability (I/O) equipment and systems should be used and managed only by personnel who have been properly trained and who have demonstrated proficiency with the appropriate technical, operational, and procedural aspects. This Best Practice applies to technicians, responders, telecommunicators, and managers, and includes both operational and interoperability issues.

Best Practice #4 - Interoperability Relationships

Formal relationships should be created to govern and manage interoperability resources.

Best Practice #5 - Infrastructure Management

The management of interoperability infrastructure should ensure its readiness, reliability, and resiliency; and the provision of failure notification and availability status of frequencies and sites.

Best Practice #6 - Channel Assignment Based on Infrastructure Coverage

Interoperability channels should be assigned based on the documented and known infrastructure coverage between the radio networks and the radio communication devices that are being utilized.

Best Practice #7 - After Action Reviews

Any After Action Review (AAR) held following a significant emergency incident or preplanned event that involved interoperability resources should include both operational and technical components including those which focus on communications infrastructure.

Best Practice #8 - Radio Device Management

Management of interoperability resources and radio devices should include a formal plan that ensures accurate radio programming and confirms the readiness of the equipment. This includes mobile and portable devices, as well as radio cache resources.

Best Practice #9 - Deployment of Interoperability Resources

In any incident or event there must be an early awareness of the need for augmented communications support, at the scene and in the communications center, to include both interoperability resources, and supplemental technical and support staff.

Best Practice #10 - Communications Span of Control

There should be one and only one talk path utilized for communications between first responders and the immediate supervisor managing their function during activity involving

environments considered to be Immediately Dangerous to Life and Health¹ (IDLH), or during critical tactical law enforcement activities.

Best Practice #11 - Managing Encryption for Interoperability Resources

The use of voice encryption on designated interoperability and mutual aid channels can create obstacles to interoperability and is highly discouraged. In the event encryption is deemed necessary due to unique operational needs, it must follow existing FCC regulations and comply with an approved regional communications plan.

Best Practice #12 - Radio Channel Assignment and Use within High-Risk Incident Environments

Radio equipment used by first responders deployed into an Immediately Dangerous to Life or Health (IDLH) environment should be programmed with the same incident communication channels including identical use of channel name, zone and channel location within the zone, and technical parameters.²

Best Practice #13 - Interoperability Resource Information Storage and Access

Information on available interoperability resources and communications plans in any given area should be documented and maintained in a central location for immediate access by first responders and PSAP personnel.

2. Overview

NPSTC is a federation of public safety organizations whose mission is to improve public safety communications and interoperability through collaborative leadership. For many years, various organizations and agencies have recognized a need to develop reference points or measurements to duplicate success or avoid communication failure. NPSTC has been very active in creating recommendations, providing support for the development of public safety requirements, and advocating the use of standards that promote effective interoperability.

These NPSTC Radio Interoperability Best Practice Recommendations are designed to provide guidance to public safety agencies and organizations regarding safe and efficient use of interoperability resources. These best practices identify why technical standards and standardized requirements are needed to improve the operational activities of public safety organizations to obtain optimal interoperability.

¹ https://www.osha.gov/pls/oshaweb/owadisp.show_document?p_table=standards&p_id=12716

² For the purposes of this Best Practice, an IDLH environment is not limited to the OSHA definition, but includes all activities where the focus of the mission places responders or citizens on the scene of an incident in immediate danger.

Many public safety agencies and organizations have already established effective procedures for communications and interoperability. These best practices are intended to highlight and define the successful elements commonly found during public safety incidents. At the same time, common failures are reviewed to determine a migration path toward improvement. The finalized Best Practices are simply statements defining strategic goals. They are not intended to be measurable but to provide guidance to agencies wishing to improve their level of interoperability.

2.1 Best Practices Relationship to Standards and Requirements

Technical standards have been developed to identify specifications and associated procedures which are designed to ensure the reliability of the materials, products, methods, and/or services necessary for reliable public safety communications. Examples of these include the ANSI Common Channel Naming Standard, which sets forth specific unique names for each nationwide interoperability channel, National Fire Protection Association (NFPA) 1221, which covers the installation, performance, operation, and maintenance of public emergency services communications systems and facilities, and Project 25 which addresses the need for common digital public safety radio communications.

However, these standards are ineffective without the support of policies and procedures governing their use. Standards are extremely important because they allow the combination of devices from different manufacturers to be used together to enable interoperability.

2.2 Using Best Practices to Enhance and Promote Standards

Standards are always intended to be measurable. When a standard is created it is based on a measurable quantity of some type that describes a very specific configuration, action, or result. Standards are developed, tested, and documented based on a defined strategic goal. Standards are then adjusted over time as the technology and measurements advance. But, a strategic goal rarely changes. Strategic goals and technical standards are best communicated together in the form of a best practice.

The goal of a best practice is to show why and how a specific standard or a group of standards should be used to help improve public safety communications.

2.3 Combining Multiple Best Practices

A single best practice cannot address all issues that may arise during an emergency incident. Both incident and after action reports will often reveal multiple areas for improvement and may identify recommendations for correction. The Best Practices in this report are intended to address single common issues and, when used in combination, provide guidance into addressing many common interoperability issues.

3. Best Practice Elements

For consistency, a standard template was developed to aid in the creation of each individual best practice. These include a Best Practice Statement, Scope of the Best Practice, Statement of Importance, Supporting Elements, Relationship to the SAFECOM Interoperability Continuum, Use Case Examples, Migration Path, and a Reference section.

3.1 Best Practice Statement

This statement is specific, at a high level, and should not be directive (e.g., does not use the words “shall,” “must,” or other terms traditionally associated with a requirement). It is visionary in its construction and though not a measurable standard, it can reinforce the need to follow a specific standard or set of requirements.

3.2 Scope of this Best Practice

During the development phase, it became apparent that many of the best practices could potentially cover very broad topics and often overlap with each other. To focus the individual best practice on those areas it is intended to address, this section is included to define the scope of what is covered and identify those areas that were not included in the document.

3.3 Statement of Importance

The statement of importance makes a case as to why a best practice should be executed by an organization or an agency. The statement also provides a more detailed narrative that may identify common problems and to support how the best practice can mitigate problems. This statement can also reference a practice that is not well known or defined. This is normally accomplished through discussions following an incident or incidents that have a common recurring issue that can be resolved by defining a best practice.

3.4 Supporting Elements

Supporting elements may also be presented that point to established processes or existing standards to help construct policies and processes that support the best practice. For example, the ANSI interoperability channel naming standard would be referenced as a best practice when building policies and programming templates. In this section, specific roles are defined to assure that a best practice is implemented and managed. These roles may be specific to a typical agency structure or are roles that are to be assigned.

Often, best practices are created to help promote technical standard applications and guidance, and encourage agencies and organizations to establish detailed processes, policies, or operational requirements.

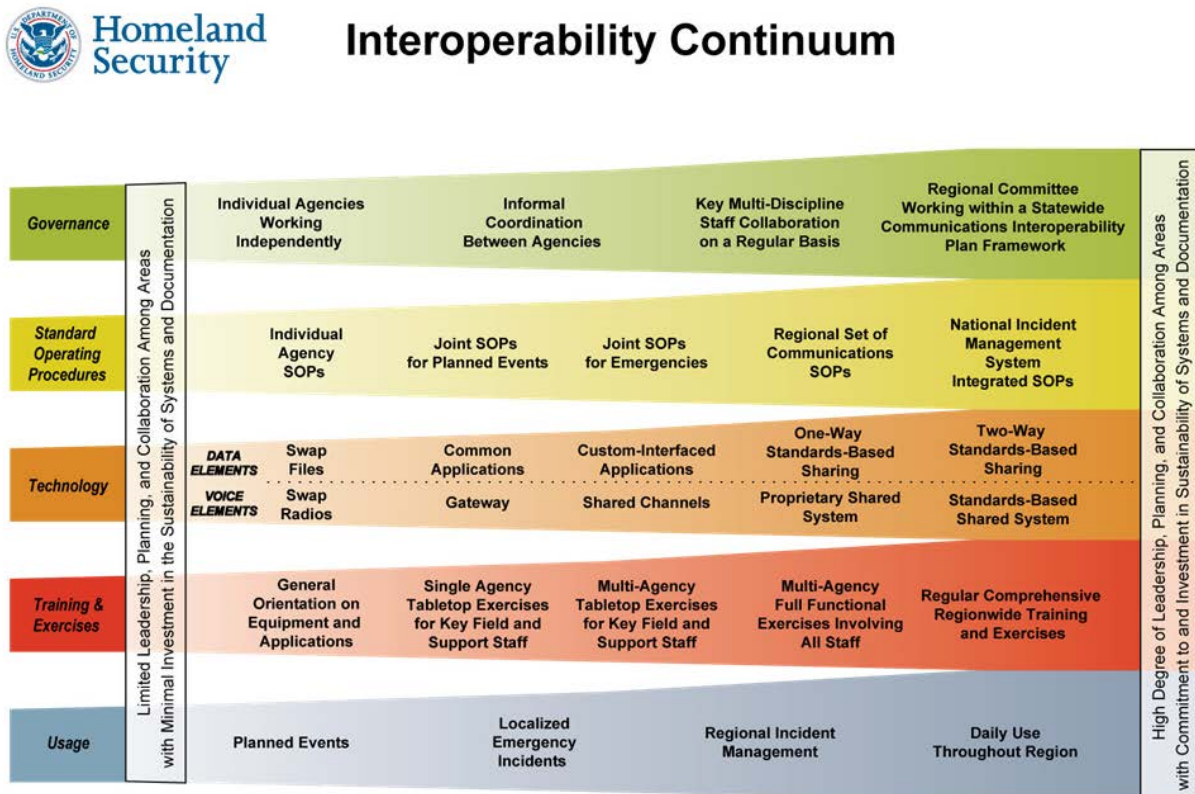
When possible, referenced documents and resources will be linked to an outside or responsible website or authority. If a reliable source is not available, relevant documents will be hosted on

the NPSTC website at www.NPSTC.org and links will be provided to their location within the Best Practice. Routine review of the website will confirm the referenced documents/links remain valid.

3.5 Relationship to SAFECOM Interoperability Continuum

Each best practice may involve many, if not all, lanes of the SAFECOM Interoperability Continuum. The best practices identify each lane, but do not go into detail in this section as the information is covered elsewhere in the statement.

Developed with practitioner input by the Department of Homeland Security’s SAFECOM program, the Interoperability Continuum is designed to assist emergency response agencies and policymakers to plan and implement interoperability solutions for data and voice communications. This tool identifies five critical success elements that must be addressed to achieve a complete interoperability solution: governance, standard operating procedures (SOPs), technology, training and exercises, and usage of interoperable communications.³



³ This chart and quoted content is found in the SAFECOM Interoperability Continuum brochure and can be downloaded at -https://www.dhs.gov/sites/default/files/publications/interoperability_continuum_brochure_2.pdf

Governance: “Establishing a common governing structure for solving interoperability issues will improve the policies, processes, and procedures of any major project by enhancing communication, coordination, and cooperation; establishing guidelines and principles; and reducing any internal jurisdictional conflicts. Governance structures provide the framework in which stakeholders can collaborate and make decisions that represent a common objective.”

Governance is noted whenever it is determined to be essential to the success of implementing a particular best practice.

Standard Operating Procedures: “Standard operating procedures—formal written guidelines or instructions for incident response—typically have both operational and technical components. Established SOPs enable emergency responders to successfully coordinate an incident response across disciplines and jurisdictions. Clear and effective SOPs are essential in the development and deployment of any interoperable communications solution.”

Developing and implementing national, regional, or agency specific Standard Operating Procedures (SOPs) are important steps in the successful support and implementation of each best practice.

Technology: “Technology is a critical tool for improving interoperability, but it is not the sole driver of an optimal solution.”

Technology plays a vital role in achieving interoperability; however, support from the other four lanes of the Continuum is essential. Technology references are used to describe any or all of the known technical settings or technologies that are typically used to meet the intent of the best practice.

Training / Exercises: “Implementing effective training and exercise programs to practice communications interoperability is essential for ensuring that the technology works and responders are able to effectively communicate during emergencies.”

Training/Exercises are noted in a best practice when the success of a best practice is achieved and/or enhanced through the development and implementation of training programs. It is important to recognize that training goes beyond initial training and should always include a plan for periodic remedial updates and exercises to practice the skills taught and to demonstrate proficiency.

Usage: “Usage refers to how often interoperable communications technologies are used. Success in this element is contingent upon progress and interplay among the other four elements on the Interoperability Continuum.”

While effective usage is often considered the goal of a best practice, it also plays an important supporting role to the other four lanes. Usage reveals the areas where governance is needed; it tests the standard operating procedures for efficiency, validates the technology and/or need for upgrading, and reduces the requirement for remedial training by keeping personnel familiar with the process.

3.6 Use Case Examples

Use cases are described in a narrative that demonstrates how the application of the best practice provides effective interoperability. The cases presented generally do not show a negative outcome when a best practice is not followed. There are a great many potential failure scenarios that could be described; however, it is more beneficial to show positive outcomes based on the application of the best practice.

The case or cases do not always show all supporting elements described above, but are written to demonstrate the most relevant.

For the purpose of these best practices, standard Incident Command System (ICS) roles and terminology have been used for consistency, recognizing that different agencies have often used their own nomenclature for those roles. The use case will focus on the functions performed by the role and not on the agency designated title.

3.7 Migration Path

This section shows how a best practice can be achieved by taking current operational processes and transitioning them to the best practice. A common tool that is used to assist with transition is the SAFECOM Interoperability Continuum. This shows how many processes and practices can be matured to reach the highest levels of interoperability.

Each best practice will describe a common method by which basic interoperability can be matured to the type of interoperability described in the best practice.

3.8 Reference Materials and Location

The reference area for each best practice identifies research materials used in their development and references for additional reading. Where possible, it will point to an Internet link to a site where information is maintained, or to a published agency policy. If an outside link is unavailable, the reference documents will be published on the Radio Interoperability Best Practices Working Group page of the NPSTC website at www.NPSTC.org.

3.9 Contributors List

The Radio Interoperability Best Practices Working Group consists of nearly 200 participants representing the public safety, government, academia, and industry communities. The overall report and each individual best practice was a collaborative effort spanning every phase of

development. As such, the overall report and statements do not identify individual contributors but instead recognizes the entire Working Group for their efforts in the creation and review of the report and best practice statements, with special thanks to the participants of the writing group who were instrumental in the development of the best practice documents.

4. Best Practice Development Process

A best practice is initiated by individuals who have made observations, read case studies about an incident, or otherwise become aware of a situation in which interoperable radio communications were less than optimal. Many times, the individual had encountered similar conditions and believed a better approach would help improve future outcomes.

Members of the Working Group solicited feedback and received nearly 200 suggestions for development into best practice statements. During a face-to-face meeting, that list was placed into categories which became the basis for the development of the first 12 Best Practices. An additional Best Practice was added to the original scope of work early in the development process. The initial work plan and format were revised as needed to create an effective vehicle which would work across the broad span of topics.

4.1 Discussion and Review in Working Group

Each Best Practice was discussed within the whole Working Group. The Working Group shared ideas, research, documents, and observations that were combined to create the initial best practice information. Individual group members volunteered to act as Best Practice Managers for individual Best Practice statements and worked either independently or within a small group to create the initial draft.

4.2 Final Draft Development

Following completion of the initial draft, a smaller writing group and the individual Best Practice Manager as available refined the draft for consistency of language and format. The resulting draft was then reviewed by the Best Practice Manager to ensure that the intent was still clear. When possible, the initial content was added to, not significantly changed. The final draft was returned to the whole Working Group for review and final editing based upon the submissions/comments received.

4.3 Peer Review

The Radio Interoperability Best Practices Working Group works under the guidance of the NPSTC Interoperability Committee. Following approval within the Working Group, the draft document was presented to the Interoperability Committee for review and comments. Submissions received from the Interoperability Committee were returned to the Working Group for consideration and consolidation prior to forwarding the final draft through the NPSTC editing process.

4.4 Adoption of Best Practice by NPSTC Governing Board

Upon final editing and approval by the Working Group and Committee, the document was submitted to the NPSTC Governing Board to approve, deny, or return with comments. Questions or changes requested by the Governing Board were addressed prior to approval. The final approved version was then distributed through the normal NPSTC outreach process.

5. Maintaining Best Practices and Developing New Practices

The Radio Interoperability Best Practices Working Group will define a review schedule as a part of the Best Practice document process. At this time, the Working Group will determine if each Best Practice is still valid or whether it should be revised or retired. Any and all changes will be addressed initially in the Interoperability Committee. If it is deemed necessary, the Working Group will convene to complete the edits. Once finalized, the updated version will be announced and posted on the NPSTC website at www.NPSTC.org.

6. Contributors to this Report

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would especially like to thank the participants of the writing group who were instrumental in the development of each individual best practice and the overall report.

Patti Broderick – Retired
Orange County Sheriff’s Office Florida

John Lenihan – Retired
Los Angeles County Fire Department

David Byrum
Pinellas County Sheriff’s Office

Denis Marin – Retired
Orange County Sheriff’s Department
California

Brent Finster
University of Hawaii
Department of Public Safety

Mark Schroeder
City of Phoenix Technology Services,
Arizona

John Johnson – Retired
State of Tennessee

Keith Victor
Town of West Hartford, Connecticut

Chris Kindelspire
Grundy County 911, Illinois

Everett Wittig
City of Bisbee Communications, Arizona

7. Appendix

The 13 completed individual Best Practice Reports are located in the appendix and available for download separately on the NPSTC website at www.NPSTC.org.

7.1 Best Practice #1 - Nationwide Interoperability Channel Naming and Usage

Best Practice # 1 - Nationwide Interoperability Channel Naming and Usage

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the Radio Interoperability [Best Practices Report](#)⁴ companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Nationwide Radio Interoperability Channels should be compliant with the current ANSI Standard designated names, frequencies, and technical information, and in accordance with the FCC and NTIA designated usage for that channel.

Statement of Importance

Communications interoperability refers to the ability of emergency response agencies to talk across disciplines and jurisdictions via radio communications systems, exchanging voice or data with one another on demand, in real time, when needed, and as authorized.

The effective use of interoperability frequencies has failed when agencies use these resources without following the standards that have been defined for these channels. The potential consequences of failed communications place lives, infrastructure, and property at risk.

It is not enough for agencies to simply program the interoperable channels in their equipment. Doing so without conforming to the ANSI Standard Channel Nomenclature for Public Safety Interoperability Channels naming practice or using the standardized tone squelch or network access codes creates a problem nearly as large as not having them at all.

Several communication plans that have been published by agencies around the country show the use of interoperability channels, but do not follow either the same technical specifications in the Standard, the same channel naming convention, or are not using them in the manner identified as a best practice use of that channel. Though this Best Practice does not aim to identify specific incidents or agencies, even the most cursory review of after action reports will often point to instances where mission critical voice operations have been hindered when first responders from different agencies are unable find a common channel in their radios. This

⁴http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_IO_Best_Practice_Overall_Report_Final.pdf

occurs often when different channel names are used to identify the same interoperable frequency. Mutual aid personnel have also not been able to find the designated interoperability channel listed in the Incident Action Plan because their local radios are programmed with nonstandard channel names. Not following the standards that have been identified for these channels will result in either a delay in effective interoperable communications or no communications capabilities on these channels at all.

Furthermore, it is important to understand that technology is only a piece of the interoperability solution. For a technical solution to be successful, areas of governance (often the most difficult challenge of all), standard operating procedures (SOPs), training and exercises, and the promotion of routine usage must also be addressed.

Supporting Elements

Interoperability channels can be local, regional, and statewide, in addition to nationwide. These channels will only work when every agency makes it a priority to program them in their radios and consoles, using the ANSI channel names when applicable. It's equally important to train members on these channels, as well as when to utilize them, and to have agreements with neighboring departments or mutual aid organizations.

Today's public safety radios are capable of over 1,000 channels. Many agencies try to put every radio frequency used in their city, county, surrounding counties, region, state, etc. into their radios so they can monitor or talk to other agencies. The major problems are:

- Keeping the information current
- Ensuring notification of a change has been sent and received
- The cost and time to reprogram
- Making sure the information is programmed correctly

If one agency changes something, then all radios need to be reprogrammed. More often today, the use of interoperability/mutual aid channels are the new norm. The use of the nationwide, state, regional, or local mutual aid/interoperability channels has proved itself to be very successful and reduces the need for reprogramming.

Interoperability channels should be programmed based on ANSI standards and should never be edited or abbreviated for local variation. Additionally, channels that are not designated nationwide interoperability channels should never be programmed using a naming convention that is so similar to the designated channel name as to become misleading to the first responders. This has occurred where local agencies use VTAC names for their local channels for

example. The NPSTC Intrastate Channel Naming Recommendations report provides recommendations for state and local interoperability channels.

Radio purchasing decisions should include the radio's capacity to meet the ANSI Standard and the needs of the agency's mutual aid or interoperability communications plan.

SAFECOM Continuum

Nationwide Interoperability Channel Naming and Usage touches every lane of the Continuum, which effectively demonstrates its importance in creating an interoperability solution.

Use Case Example

Castle County Fire Rescue and Beach County Fire Rescue share a major highway between the two counties. Castle County Fire Rescue and Beach County Fire Rescue both respond to a multi-vehicle crash on the shared highway. Each agency owns and operates a proprietary radio system. The systems are not compatible and interoperability is accomplished via use of the conventional 800 MHz channels. Castle County, the incident owner, requests Beach County responding units switch to 8TAC91 to coordinate the response. Due to regional planning, training, and coordination, both agencies communicated successfully and within moments. The regional approach provides technical and operational preparedness for any interoperable need. In accordance with policy, proper dispatch coordination, and repeater responsibility, along with the channel announcement and radio location to end users, seamless communication will occur.

Migration Path

Step 1: Provide user training on the channel names and educate users how the agency will "bridge" from current non-standard names to the ANSI-approved name. Channel naming policies should be recorded in official agency SOPs.

- Personnel should receive training on channel names and interoperability procedures at the same time they receive training on radio operability and on a recurring basis.

Step 2: Any radio using an interoperability channel should have that channel programmed exactly as identified in the standard. Communication plans maintained by the agency owning those radios shall identify these channels using the standard channel names. Agencies should only use these channels under the best practice guidelines use of that channel.

- During the transition, until all agencies have programmed their radios with the ANSI Standard, an agency may choose to program radios with both the ANSI Standard channel name in a separate interoperability zone in the radio and leave the current non-

standard channel name in a local channel zone. This is identified as a tool to use during the migration process only and these alternate names should be removed from those agencies' communications plan as soon as all of the pertinent agencies have programmed their radios and consoles to meet the standard.

- Ensure radio consoles are programmed with the same ANSI channel names as the mobile and portable radios. In an emergency, any responder should be able to grab any other responder's radio and find the correct frequency/channel to call for help.
- For preplanned events or extended operational incidents, radio channels should be programmed into the same positions on all radios assigned as per the ICS 205, to reduce confusion between personnel at the scene who are searching for a common channel.

Step 3: Channels should be tested on a regular basis to maintain user awareness of proper usage. Suggested uses to accomplish this include:

- Use the channel during a daily or weekly roll call.
- Use the channel in planned events several times a year.

Step 4: Communication plans developed by agencies that includes or anticipates the use of these interoperability channels should meet the standard for these channels, and identify any supporting infrastructure that will provide appropriate coverage.

- The use of these channels by any agency internally or with other agencies shall use the ANSI Standard and the channel shall be identified on each mutual aid agency's communication plans using the Standard.
- Work with all public safety agencies in the region to adopt the same process to ensure interoperability on day-to-day responses as well as major incidents.
- All agencies that have agreed, through governance or formal mutual aid response plans, shall have all selected interoperability channels programmed into the same locations on each radio, to enable quick effective access of these channels and reliable communications.

Related Documents

The following links point to reference materials that were used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practices Working Group page on the NPSTC website at www.NPSTC.org or by joining

NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.⁵

[ANSI Standard 2017](#)⁶

[NPSTC Intrastate Channel Naming Recommendations Report](#)

[Establishing Governance to Achieve Statewide Communications Interoperability Report](#)

[State of Alabama SCIP](#)

Date Approved

January 24, 2017

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

⁵ Select Interoperability Committee -> Best Practices -> Shared Documents

⁶ http://npstc.org/download.jsp?tableId=37&column=217&id=3836&file=11042-2017_CommonChannelNamingDocument.pdf

7.2 Best Practice #2- Interoperability Systems Change Management Practices

Best Practice #2: Interoperability Systems Change Management Practices

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the [Radio Interoperability Best Practices Report](#)⁷ companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Change management practices and policies should always be used to ensure that any changes to operational policies, system modifications, additions, or deletions of interoperability system infrastructure are communicated to all affected agencies.

Statement of Importance

An interoperability system is comprised of infrastructure, people, policies, and processes, and is dependent on all of these working together in order to be successful. Each individual item within this system can always change for any reason at any time requiring system adjustments. When this happens, it is critical that the change is communicated in appropriate detail to each person involved.

Change management processes are frequently not developed or memorialized in policies when it relates to technical systems or their support. This is generally very different from the majority of operational management processes for others within a public safety organization.

Radio system or system use changes should always be submitted through an established organizational change management process in order to be successful when implemented. As an example, this can ensure that when a radio site or channel is inoperable that everyone who should be informed is informed and ensures they are also notified when the site or channel is back in operation.

Following an agreed upon change management process will ensure that anyone granted the use of an interoperability system is aware of any changes, is communicating these changes

⁷http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_IO_Best_Practice_Overall_Report_Final.pdf

across their organization as required, and is also reviewing a change before it takes place, if it could in anyway impact how they operate, as proactively as possible.

Common examples of interoperability system change are:

- When the operational hours an interoperability channel is monitored or supported by an agency changes or a channel is reserved for an operational period for a pre-planned event.
- When a radio site or entire channel is placed out of operation for testing or improvements.
- When a radio site or channel is found to be out of service.
- When a technical system change may need to be made that could affect the existing programming of radios.
- When technical or informational documentation changes are made necessitating the replacement of previously issued versions.
- When a change in the approved or intended use of a channel is changed.

Supporting Elements

Successful change management depends on identifying, generally before a system or process is employed, who will be assigned the four key roles of a change management process. These are:

- **Responsible**: This is the role assigned to someone or the group that will be implementing a change and has likely proposed the change that is being made. This role has recommended that the change is made for whatever reason and has performed due diligence as to the impact of the change. The role also has developed a back-out / back-up plan in case the change has any negative impact. This role also initiates the change management procedures established and ensures that all roles (persons) that have been identified are informed or have accepted the changes before they are employed.
- **Accountable**: This is the highest level of involvement within a change management process. This role is assigned to the person or group that owns the responsibility for the system. Any change to a system or process that has identified a person or a group assigned this role always requires their review and approval before a change is made.
- **Consulted**: This role is assigned to someone or the group who may be involved with helping to implement a change or will need to be a key adviser or tester of a change, before it is escalated to the Accountable level.
- **Informed**: This role is assigned to anyone and everyone who may need to know that a change is taking place and that it may or may not impact normal operations in any way. A practice to report any discoveries that occur during the change should be in place prior to the change being implemented.

SAFECOM Continuum

Change management touches the Governance, Standard Operating Procedures, Training and Exercise, and Usage lanes of the Continuum.

Use Case Example

A base station radio supporting multiple agencies on a regional interoperability channel has failed. This has been discovered during a weekly routine test conducted by dispatchers and field personnel. As soon as this has been found to be inoperable, and per established change management policies:

- The dispatch center responsible for the control and oversight of this channel logs this operational status change and ensures that this channel or radio site will not be assigned. In this case, the dispatch center's agency holds the *Accountable* role.
- The dispatch center notifies any other agencies that depend on this channel and station as an available resource that it is not available. The other agencies hold the *Informed* role in this case.
- The dispatch center then contacts the appropriate support personnel that will begin the repair process to restore this base station to normal operational use. The support personnel hold the *Responsible* role to manage and resolve this issue.
- When support personnel have restored this station to operational status, the dispatch center will retest the station with field personnel for proper operation. In this case, the dispatch center holds the *Consulted* role as they provide information about the issue and also participate in accepting and reviewing or testing the solution.
- After successful testing is completed, the dispatch center will accept the base station from the support personnel and broadcast to all affected agencies and other relevant personnel that the channel / base station is now back in normal operation. The dispatch center holds the *Responsible* role in this case.

Migration Path

One effective way of building and managing a change of any type is by developing and maturing a process using the Information Technology Infrastructure Library version 3 (ITIL v3) frameworks for RACI.⁸ This is simply illustrated as follows:

⁸ <http://itsm.fwtk.org/index.htm>

Responsible	The person who actually carries out the process or task assignment.
	Responsible to get the job done.
Accountable	The person who is ultimately accountable for process or task being completed appropriately.
	Responsible person(s) are accountable to this person.
Consulted	People who are not directly involved with carrying out the task, but who are consulted.
	May be stakeholder or subject matter expert.
Informed	Those who receive output from the process or task, or who have a need to stay informed.

Devising a process and identifying internal individuals, roles, or position within an organization ensures that when any type of change presents itself or a change is needed, following a pre-determined process safeguards that everyone who needs to be involved or informed, will be.

The first step in a successful change management process is to list possible scenarios and build up a list of those individuals and agencies that must be informed. This is very common. What is not very common is to strengthen some of these contacts by giving them a key position in the change management process. Also, by developing a defined process and backing it with internal policies, it provides technical support staff with “go” and “no-go” steps when making changes.

Technology issues frequently have a mystique of being unique and different from the business of public safety. In well-managed environments, change management is identical to most incident management practices. An example of what IT Incident Management can look like within the RACI Matrix is shown in the following table:

RACI MATRIX PROCESS USING INCIDENT MANAGEMENT AS AN EXAMPLE										
Activity	CIO	Executive Director's	Senior Management	IT Service Management Office	Unit SM Coordinator	Business Office	Change Manager	Staff	Service Desk	Customers
Incident Management Program		I	I	C	R, C, I	I	I	R, I	R, A	I
Incident Detection and Recording				C	I			I	R, A	
Classification and Tier 1 Support				C	I			C, I	R, A	C

Incident Matching				C	I			I	R, A	
Investigation and Diagnosis				C	I, C			R, I	R, A	C, I
Resolution and Recovery			R	C	R			R, I	R, A	C, I
Incident Closure			R	C	I			R, I	R, A	I
Monitoring			R	C	R, C			I	R, A	
Tracking		I	R	C, I	R, C			I	R, A	
Communication	I	I	R	C, I	R, C		I	I	R, A	I

By changing the titles in the vertical columns and the activity steps, it can be seen that incidents are pretty much managed the same way. Technology change management processes should be developed and managed in the same way within an agency as other incidents are. And, the accountability for following these should also be assigned to ensure that changes have minimal impact and are understood.

RACI MATRIX PROCESS USING BASIC INTEROP SYSTEM FAILURE AS AN EXAMPLE						
Activity	Regional Center Manager	Dispatch Center Supervisor	Regional Dispatch Centers (users of the system)	Authorized Radio Users	Technical System Manager	Technical Support Staff
System failure identified	A	R	I	I	I	I
Dispatch Center advises of unavailability		R	I	I		
Support request created		R			R	
Technical Staff engaged		I			A	R
System failure resolved		I				R
Dispatch Center and Technical Staff verify proper operation		C		C	A	R
Dispatch Center puts system back into service	A	R	I	I		

NOTE THAT ROLES/RESPONSIBILITIES WILL VARY BETWEEN AGENCIES

Related Documents

The following links point to reference materials were used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practices Working Group page on the NPSTC website - www.NPSTC.org or by joining NPSTC

Committees Community on the National Interoperability Information eXchange at www.NIIX.org.⁹

[Information Technology Infrastructure Library \(ITIL\) v3](#)

[ISO/IEC 20000](#)

[RACI Roles Chart](#)

Date Approved

January 24, 2017

Contributors List

Numerous members of the Ratio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

⁹ Select Interoperability Committee -> Best Practices -> Shared Documents

7.3 Best Practice #3 - Training and Proficiency in the Management and Usage of Interoperability Equipment and Systems

Best Practice #3: Training and Proficiency in the Management and Usage of Interoperability Equipment and Systems

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the [Radio Interoperability Best Practices Report](#) companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Radio Interoperability (I/O) equipment and systems should be used and managed only by personnel who have been properly trained and who have demonstrated proficiency with the appropriate technical, operational, and procedural aspects. This Best Practice applies to technicians, responders, telecommunicators, and managers, and includes both operational and interoperability issues.

Statement of Importance

Insufficiently trained personnel have incorrectly activated radio gateways/patches, programmed radios incorrectly, and failed to identify readily available interoperability solutions, all of which have led to major communications failures.

Successfully managing the communications aspect of a critical incident involves significant investment by each participating agency – weeks, months, or even years prior to an incident occurring. This investment is not just a budget line item, but rather an investment in human resources and management priority. Personnel with responsibility for interoperability components include:

- The radio and IT technicians (who design, implement, and maintain the solution).
- Users (including communications center dispatchers/telecommunicators, emergency responders, and incident Communications Unit personnel).
- Their supervisors (in their role as instructors, mentors, schedulers, and evaluators), and of course management (overall responsibility for policy and budget).

The common thread is each of those personnel receiving targeted, adequate training for their specific aspect of the interoperability puzzle. The term "adequate" may mean watching a 20-

minute awareness video by first responders as part of their training program. It may mean a Communications Center staff member receiving a 4-hour introduction to the region's Tactical Interoperable Communications Plan (TICP). Or it may mean the considerable investment in attending an Incident Communications Technician (COMT) or All-Hazard Communications Unit Leader (COML) course, including the requirement for demonstrated proficiency at exercises or real incidents before becoming fully qualified.

Training on interoperability is multi-faceted. Prior to procurement, the initial and ongoing training and staffing to support interoperable solutions (such as fixed/infrastructure, mobile, or portable equipment) must be addressed. Every department member should receive at least a minimum baseline of awareness training, including terminology and an overview of available resources and assets.

This should include the following:

- A basic understanding of portable and mobile radio features by field personnel including how to change groups/zones/channels, expectations of performance coverage for each channel (especially as it relates to tactical, simplex, or interoperability channels), and troubleshooting.
- Communications center personnel need information on interoperable channel assets and options available during major or multi-jurisdictional incidents and system failures.
- Individuals with basic or intermediate understanding who show a willingness or desire to become more involved should be given opportunities for advanced training regarding interoperability including COMT and COML.
- Personnel who have received incident communications training and those who supervise them should be intimately familiar with their agency and regional Tactical Interoperability Communications Plan (TICP) and Statewide Communications Interoperability Plan (SCIP), and actively participate in their maintenance and revision.

An engineered solution to an interoperability problem is worthless without the proper training of and demonstrated competence by those who use that option in the midst of a critical incident.

Supporting Elements

Successful management of mission critical communications interoperability requires time sensitive action by personnel with very little margin for error. Employees with responsibility for interoperability include agency, contract, and vendor personnel as described below:

- Radio and IT technicians, who develop, implement, deploy, and maintain interoperability equipment/systems.
- Users of the interoperability equipment/system, including emergency responders, incident commanders, communications center telecommunicators, and ICS Communications Unit personnel.
- Supervisors in their operational role and as instructors, mentors, schedulers, and evaluators.
- Executive level management staff that provide overall responsibility for policy and budget.

All personnel should receive both orientation and focused training which is appropriate for their specific role. All training provided should result in demonstrated proficiency to the level documented by agency policy.

- Technicians, users, and supervisory personnel need generalized training which provides an overarching view of the interoperability system. This should include:
 - Knowledge of all subscriber unit radios, consoles, gateways, features, and accessories, including recovery (back up) from system failure.
 - Knowledge of radio network infrastructure and capabilities, including specialized interoperability resources managed by the PSAP, dispatch center, and field users.
 - A variety of delivery systems should be developed to supplement formal classroom instruction, including the use of multi-media components to engage the student and maintain their attention. The use of systems that simulate the live environment (or the use of the live environment when appropriate) is recommended.
- Technical personnel, who program, maintain, or repair interoperability equipment and systems need training on existing and/or new systems and system enhancements. This should include:
 - The ability to maintain the systems, troubleshoot problems, program subscriber devices, deploy the equipment, and knowledge of console operations.
 - The ability to demonstrate proficiency in the operation and maintenance of those networks.
 - Training on all relevant RF and network systems and software applications.
- Users need initial **and recurring** training on the proper use of interoperability resources and have demonstrated proficiency in effective decisionmaking and operational use of equipment and systems. This shall include:
 - Knowledge of how and when to contact appropriate support personnel when systems do not operate as expected.

- Communications center personnel need specific training and readily accessible information (such as TICPs, Operations Guides, contact information both internal and external to their agency, etc.) on interoperable channel options. This should include:
 - Knowledge of resources, proper usage, coverage area limitations, and console capabilities and functions.
 - Identifying and securing available options or resources during major or multi-jurisdictional incidents or system failures.

SAFECOM Continuum

Training touches every lane of the Continuum, which proves its importance in the overall success of any interoperability challenge.

Use Case Example

A police officer is in pursuit of a bank robbery suspect and is approaching the county line where he will lose coverage from his home agency radio system. The home agency dispatcher broadcasts and coordinates with the agencies that may be affected by the pursuit to identify an available interoperability channel, which is available in the officer's radio. The channel name and location in the radio is broadcast by the respective dispatcher to their units. The officer accesses the channel and follows appropriate protocol for calling the adjacent county. The dispatch facility in the adjacent county is prepared to take over at the appropriate time.

Agency-wide training in interoperability policies and procedures enabled a seamless and successful outcome.

- Corrections, law enforcement, EMS, and fire all have this issue.
- Implementation of this Best Practice also supports incidents in which a first responder is outside of his/her jurisdictional area.
 - First responder selects a preprogrammed interoperability calling channel, which shall be dispatch monitored 24x7x365.
 - Dispatch may need to activate, and, in some cases, disable, repeaters to provide radio coverage for multiple responders as they travel in and out of coverage.
- During a planned event, an incident occurs and additional communications resources are needed.
 - The Communications Unit Leader (COML) is trained to contact the Communications Coordinator (COMC) at the dispatch center to coordinate for available interoperability resources.

- Communication Centers are trained to patch an operational channel to an interoperability resource if needed.
- ICS205 form should be prepared in advance and list the available channels.

Migration Path

This Training Best Practice can be both the easiest and most important of all of the Best Practices to implement. Most agencies already have a training program in place into which this Best Practice can be incorporated.

Agencies may adopt this Best Practice statement by taking incremental steps:

- Establish policies for supporting the best practice.
 - Management with the overall responsibility for interoperability, meets with colleagues and established groups and organizations (such as the SIEC) to determine any existing plans or programs.
- Develop a training plan which ensures that all department personnel receive baseline training, with some persons identified for advanced training, as relevant to their position.
 - Involve supervisory personnel in the development process to ensure consistency regarding participation and evaluation.
 - Existing DHS/FEMA/NWCG training courses and materials should be used which support a national/international standard.
 - FCC rules and regulations for use of communication resources should be followed.
 - In addition to necessary changes as situations develop, established training plans should be reviewed and revised annually.
 - Communications Center personnel are a critical component of a successful interoperability solution.
- Provide initial training to agency personnel.
 - Documentation of this training should be retained by the agency and the employee.
- Establish performance objectives and evaluation criteria to document each employee's proficiency in using interoperability systems.
 - Employees who have been trained on the use of interoperability systems are then individually assessed to demonstrate proficiency.
 - Documentation of their proficiency level should be retained by the agency and the employee.

- Implement a schedule for recurring training for all personnel.¹⁰
 - Operability and interoperability training can be incorporated into other existing training programs.
- Develop a regional approach to interoperability training to ensure consistency.
 - Regional approach to training should be reviewed on a recurring basis.
 - Agencies which may become involved in an interoperability incident should be encouraged to participate in initial and recurring training and exercises.
 - Effective communications between agencies is critical during incidents and should be stressed during training exercises

Related Documents

The following links point to reference materials were used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practices Working Group page on the NPSTC website - www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.¹¹

[Radio Interoperability Best Practices Report](#)

[Navy Yard Shooting - DC Police After Action Report](#)

[NIFOG](#)

[Colorado Interoperability Web Training Module 1](#)

[Colorado Interoperability Training Program - Module 2 Interoperability Basics](#)

[Yarnell Hill Fire After Action Report](#)

[Tactical Interoperable Communications Plan \(TICP\) Template](#)

[ICS Form 205](#)

[Florida Region 9 Plan](#)

¹⁰ Executive level management staff, Users of the interoperability equipment/system, Supervisors, and Radio and IT technicians should all receive recurring training consistent with the level of initial training received.

¹¹ Select Interoperability Committee -> Best Practices -> Shared Documents

State Interoperability Statewide Communications Interoperability Plans¹²

[ANSI Common Channel Naming Standard](#)

[NPSTC Intrastate Channel Naming Recommendations](#)

Date Approved

January 24, 2017

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the following participants of the writing group who were instrumental in the development of this individual Best Practice document.

¹² www.npstc.org -> Resources -> Broadband Directory -> Organizations -> National Council of Statewide Interoperability Coordinators (NCSWIC) -> SCIPs

7.4 Best Practice #4 - Interoperability Relationships

Best Practice #4 - Interoperability Relationships

This Best Practice is part of a larger, ongoing effort by NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the [Radio Interoperability Best Practices Report](#)¹³ companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Formal relationships among all involved stakeholders should be created to manage and govern interoperability resources.

Statement of Importance

First responders need to know the interoperable channels and resources¹⁴ that are available to them for day-to-day coordination, automatic aid, and mutual aid responses. That knowledge includes channel names, where they are located in their respective radio equipment, how they operate, and the *policies regarding channel use and authorization*.

Supporting Elements

Interoperability is defined in Section 90.7 of the Federal Communications Commission's (FCC) rules as, "An essential communications link within public safety and public service wireless communications systems which permits units from two or more different entities to interact with one another and to exchange information according to a prescribed method in order to achieve predictable results."¹⁵ The success of radio interoperability must start with planning. Systems that include shared interoperability channels are a simple solution. The rules of when to use these resources, who controls and maintains them, the knowledge of where they work (coverage), and who has access should be codified by all stakeholders leveraging these formal relationships. Participants in these formal agreements must include technical, operational (field and communications center), and management personnel.

¹³http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_IO_Best_Practice_Overall_Report_Final.pdf

¹⁴ Interoperability resources include console patches, IP Gateways, designated talk groups on trunking systems, as well as conventional channels.

¹⁵ http://www.ecfr.gov/cgi-bin/text-idx?SID=ba5840d92638b2a5365a528ddb8004ad&mc=true&node=pt47.5.90&rgn=div5#se47.5.90_17

The importance of developing and maintaining a local and/or regional Tactical Interoperable Communications Plan (TICP), with input and consensus approval by all stakeholders, cannot be overstated.

One way of developing successful interoperability relationships is by identifying common shared channels, agreeing to their intended use, defining their name and CTCSS/DPL or NAC code (if not already defined by a national standard), agreeing to common placement within the radio, and identifying if they should be installed on dispatch center consoles and supported by communications center personnel. The goal should be to have the groups/zones/banks programmed in the same position, using the standardized channel name¹⁶ in the radios. This arrangement will help operational personnel find the assigned channel during an emergency. These channels should also appear with the same name on the dispatch consoles. Channel groupings could be defined by common geographical boundaries or common operational areas, or by functionally defined operations. These groupings should be adopted by formal agreement and assigned when incidents occur in the designated areas. *See Use Case #3.*

Challenges to successful interoperability occur when agencies build interoperable communications infrastructure and announce it as "available for use" without accompanying policy and procedure guidelines. In other cases, changes were made which affected the use of interoperability resources and information was not distributed in advance of the change. Impediments to successful interoperability can be minimized and awareness and use heightened through the adoption of written policies and procedures; establishment of a formal change management process,¹⁷ and adoption of a recurring training program.

Incident Use Case Examples

Use Case # 1: Adams County operates on an 800 MHz radio system while Baker County operates on a UHF system. A vehicle pursuit initiates in Baker County near the border of Adams County. As the pursuit heads towards Adams County, dispatchers from Adams County and Baker County agree on a patch that will provide seamless radio communication. Only one agency needs to create the patch and this action is coordinated between the dispatch centers. Dispatchers from both counties then announce to their field units that the patch has been enabled and provide instructions on how to access the frequency. In this case, the Adams County PSAP patches their 800 MHz talkgroup to the UTAC repeater located in the eastern portion of Adams County (which is also available in Adams County's console). As the pursuit moves away from the Baker County UHF coverage area, Baker County's deputies switch to the

¹⁶ ANSI Standard 2017 - http://npstc.org/download.jsp?tableId=37&column=217&id=17&file=11042-2017_CommonChannelNamingDocument.pdf

¹⁷ BP #2 – Interoperability Systems Change Management Practices - <http://npstc.org/radioInteropBP.jsp>

selected UTAC channel allowing units to remain in communication with Adams County deputies who continue the pursuit. This is made possible due to preplanning efforts and ongoing coordination between the public safety agencies in the region. Technicians, first responders, and communications center personnel all participate in these planning efforts. The use of the UTAC channel and the patching solutions used in this pursuit had been developed and vetted through the regional communications coordinators (COMC), formalized in a written document, and then adopted by the regional agencies.

Use Case #2: A statewide VHF repeater system has been implemented and serves as a travel channel when large wildland fires occur and mutual aid resources respond up and down the state. The channel is monitored by designated dispatch centers in order to assist strike teams with logistical needs or to redirect units if conditions change. The repeater output frequency is available for simplex intra-strike team communications. The policy for this channel's use was developed through the Statewide Interoperability Executive Committee (SIEC) and executed through the State's Emergency Management Agency via written mutual aid agreements. Fire agencies throughout the state sign the agreements and distribute the travel communications plan. Fire agencies are responsible to confirm that all VHF equipment in their possession is programmed properly and that responders are trained to use the channel.

Use Case #3: The City of Quincy runs an International airport whose departures fly over Quincy Bay. Adams County Lifeguards patrol the inner waters of Quincy Bay and the Coast Guard patrols the outer waters. The city, county, and United States Coast Guard (USCG) established a Communications Working Group (CWG) and created a Marine Disaster Communications Plan to address any incident that that may occur on the bay or beach area. The Communications Plan includes 16 channels to support interoperability and emergency response. Each agency has agreed to program these channels into a Bank or Zone as specified in the Plan. The Bank or Zone will be referred to as the "Marine Zone." The 16 channels in the Marine Zone are USCG channels, County Fire and Lifeguard channels, City Fire channels, interoperable channels, and shared air-to-ground channels. This agreement was formalized and compliance with the communications elements of the plan are mandatory for all agencies responding to incidents in the covered area. The annual Marine disaster drill utilizes this set of channels to validate and familiarize responders to the purpose and usage of these channels.

SAFECOM Continuum Lanes

This Best Practice touches the Governance, Standard Operating Procedures, and Training and Usage lanes of the SAFECOM Interoperability Continuum.

Migration Path

Agreements between two or more agencies involving the sharing of channels should always be formalized in advance. The nationwide interoperability/mutual aid channels are a standardized set of channels that could serve as a basis for initial on-the-scene coordination and resolution of local interoperability issues. These nationwide interoperability/mutual aid channels will also be of benefit for deployments outside of the normal response area. While these channels should be preprogrammed in radios, perhaps the most difficult part is the management or governance piece of the solution. The rules that govern mutual operation must be considered prior to any actual use.

There are several steps to consider when establishing a formal interoperable communications agreement, be it statewide, regional, or an agreement between two agencies.

- Do not limit the list of shared channels to only include the nationwide interoperability channels.
- Be aware that the FCC and NTIA have each published regulations governing the use of the Nationwide Interoperability channels by both federal and non-federal entities. These rules provide specific guidelines for the coordination and use of the frequencies and need to be considered in any plan.¹⁸
- Establish formal communications working groups that include operational, technical, and management personnel from each agency involved in the planning. The inclusion of communications center personnel is an integral part of this planning process.
- Associate working groups are helpful to the planning process, including those with established authorities such as Fire Chiefs, Police Chiefs, Joint Power Authorities, SIECs, etc.
- The communications plan should define the channel lineup, the geographical boundaries for usage, and responsibility of 24 hour monitoring, enabling and disabling of repeaters and patches.
- Written policies and procedures should be created.
- Final versions of these documents shall be adopted by the respective authorities and shared among all stakeholders.
- Recurring training and the use of exercises and drills, both intra and interagency, will encourage the utilization of these established resources resulting in familiarity and accomplishing the interoperable goals.
- Daily use these channels (as appropriate) should be encouraged to maintain awareness and to sustain technical and operational proficiency.

¹⁸ See <http://www.ntia.doc.gov/osmhome/redbook/redbook.html> section 4.3.16 for Federal frequency use under the rules of the NTIA. See http://wireless.fcc.gov/index.htm?job=rules_and_regulations Part 90 for Non-Federal frequency use under the rules of the FCC.

- A review process addressing the policy, procedures, and communications plan, including provisions for change management, should be developed.

Related Documents

The following links point to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practice Working Group page on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.¹⁹

[Writing Guide for a Memorandum of Understanding \(MOU\) – SAFECOM/DHS -
http://www.safecomprogram.gov/NR/rdonlyres/2D396F0E-CE19-4DCB-A30A-
35982721F5AA/0/SOP.pdf](http://www.safecomprogram.gov/NR/rdonlyres/2D396F0E-CE19-4DCB-A30A-35982721F5AA/0/SOP.pdf)

[Emergency Communications Governance Guide for State, Local, Tribal, and Territorial Officials,
September 2015 – SAFECOM/NCSWIC -
https://www.dhs.gov/sites/default/files/publications/2015%20Governance%20Guide_Master_508c%20Final.pdf](https://www.dhs.gov/sites/default/files/publications/2015%20Governance%20Guide_Master_508c%20Final.pdf)

[Communications-Specific Tabletop Exercise Methodology
http://www.safecomprogram.gov/NR/rdonlyres/C67306E9-3C28-4654-91A5-
0CDFD6D3DE55/0/CommunicationsSpecificTabletopExerciseMethodology.pdf](http://www.safecomprogram.gov/NR/rdonlyres/C67306E9-3C28-4654-91A5-0CDFD6D3DE55/0/CommunicationsSpecificTabletopExerciseMethodology.pdf)

[DHA/SAFECOM Webpage on Governance Resources - https://www.dhs.gov/safecom/governance](https://www.dhs.gov/safecom/governance)
[Best Practice #1 – Nationwide Interoperability Channel Naming and Usage](#)

[Best Practice #3 – Training and Proficiency in the Management and Usage of Interoperability Equipment and Systems](#)

Date Approved

March 31, 2017

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

¹⁹ Select Interoperability Committee -> Best Practices -> Shared Documents

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

7.5 Best Practice #5 - Infrastructure Management

Best Practice #5 - Infrastructure Management

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the Radio Interoperability Best Practices Report companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

The management of interoperability infrastructure should ensure its readiness, reliability, and resiliency, provision of failure notification, and availability status of frequencies and sites.

Scope of this Best Practice

This Best Practice limits its scope to the awareness and vigilance required of stakeholders who rely on interoperable communications systems in order to assure availability of these critical resources.

This Best Practice does not discuss areas involving design, installation, or maintenance of interoperability infrastructure,²⁰ operational and training requirements, deployable resources, or subscriber systems.

For this Best Practice, interoperability system knowledge includes RF site location and coverage, basic knowledge of system design including base stations, repeaters, relays, switches, interconnecting systems, consoles, gateway devices, and a general understanding of the networks and software that provide the interoperability functionality.

Statement of Importance

Infrastructure management best practices may also apply to agency specific communications infrastructure, as well as interoperability infrastructure. All agencies should ensure that each telecommunicator, first responder field user, and technician is aware of the operational and functional parameters required to successfully use the interoperability system.

Telecommunicators need to know which interoperability infrastructure solution will work best for any given incident. This requires that they be aware when a particular interoperability

²⁰ Refer to the NPSTC Defining Public Safety Grade Systems and Facilities Report, May 2014.
http://www.npstc.org/download.jsp?tableId=37&column=217&id=3066&file=Public_Safety_Grade_Report_140522.pdf

system is off line for maintenance or is in use by another agency. First responders need to understand the various interoperability infrastructure solutions that may be available, so they may request activation of a particular asset. Technicians need to understand how various interoperability infrastructure systems are interdependent to fully assess the impact of taking a system offline for maintenance.

This Best Practice recommends active monitoring of interoperability infrastructure in order to make critical decisions on the selection of an interoperability solution in real time. The sophistication of the real-time monitoring depends on the complexity of the interoperability systems. In some agencies, notes placed on a grease board are sufficient to track interoperability system status. Other agencies who share regional interoperability infrastructure may use a software application to display the availability of a range of frequencies and systems.

Successful use of interoperability infrastructure leads to well-coordinated public safety response through the cooperative agreements upon which agencies rely.

Supporting Elements

The elements of infrastructure management include coverage, frequencies, availability, control, testing, maintenance, and change management.

Coverage Knowledge

For planned or unplanned events, knowledge of the coverage footprint of the interoperability resource is critical in order to ensure that communications can be maintained throughout the incident. Incidents covering a wide geographic area require more planning and coordination and typically involve more interoperability assets.

Frequencies and Availability of Resources

Each public safety agency should be aware of the cooperative agreements that are in place with other agencies which govern the shared use of interoperability systems.²¹ The interoperability system capabilities need to be known in the event gateway devices or other supplemental technology is required. All individuals, including telecommunicators, who are responsible for activating or deactivating interoperability system components, should have readily available reference documents. (e.g., NIFOG, procedure manuals, wall charts, talkgroup matrix lists, etc.). Availability of assets should be managed in such a way that all agencies have immediate visibility into each interoperability system's availability. This can be accomplished in a variety of

²¹ See BP #4 – Interoperability Relationships - <http://npstc.org/radioInteropBP.jsp>

ways, including the use of software or through the identification of a single agency or entity that functions as an interoperability gatekeeper.

Control

Each public safety agency needs to know which agency is responsible for the operation and maintenance of each component of interoperability infrastructure. This is essential in order to report a system failure to the correct agency having jurisdiction for the equipment. In many cases, the owner agency must authorize use of the interoperability system and activate it based on the unique needs of the incident. This process, for accessing and activating the interoperability system, should be established through cooperative agreements and documented in written agency policy.

Practice/Testing

Agencies should use the interoperability infrastructure on a recurring basis to maintain proficiency and to verify that the systems are fully functional. These practice sessions should include both dispatch and field personnel. Both announced and unannounced drills are important to ensure that all personnel on all shifts are familiar with the operation of the technology.²²

Failures/Maintenance/Alarm

Faults and failures involving interoperability system infrastructure should result in an immediate notification to the public safety agency responsible for the technology. This notification should be automatic if at all possible. The scope of the failure should be evaluated immediately and communicated to all agencies having access to the system.²³

Changes

Any changes which impact the availability, coverage, and/or operation of an interoperability system must be communicated to all agencies which rely on that technology. A formal process should be used to ensure that all agencies are notified. Each agency receiving a notification should ensure that all personnel within their agency who may be impacted are also informed

²² See Best Practice #3 - Training and Proficiency in the Management and Usage of Interoperability Equipment and Systems - <http://npstc.org/radioInteropBP.jsp>

²³ Preventative maintenance of interoperability systems should be performed based on the manufacturer's recommendations. Agencies may elect to enhance this schedule depending on local needs.

(e.g., the notification should extend beyond the PSAP). This includes field users, telecommunicators, command staff, and appropriate technicians.²⁴

SAFECOM Continuum

Infrastructure Management touches every lane of the Continuum, which effectively demonstrates the importance of creating an effective infrastructure management plan.

Incident Use Case Example

Use Case #1: Two neighboring communities utilize the same fixed 8TAC repeater channels. Community 1 is currently using the 8TAC91 repeater for a planned event involving a parade. Community 2 needs to use the 8TAC91 repeater to provide targeted geographic coverage for a multi-jurisdictional incident. Both communities have additional fixed 8TAC resources. Advance planning and use of established policy allowed both communities to quickly resolve this issue. A decision was made to move the preplanned incident to an alternate 8TAC channel and resulted in both incidents having an available, non-interfering resource.

Use Case #2: Scheduled testing ensures the readiness of any interoperability system. The controlling agency announces that a roll call is being conducted with the participating agencies. The controlling agency calls each agency by name. The responding agency will check all the interoperability system parameters including audio and visual indicators ensuring expected performance of the interoperability resource. If an agency does not respond, the controlling agency should contact them by alternate method to verify their participation or to verify that a system failure has occurred. This testing can be accomplished using local, regional, and state partners. Testing should also include field personnel using their assigned radios to promote familiarity and confidence in the interoperability systems.

Migration Path

Develop the Plan

Agencies with access to interoperability systems are encouraged to plan and coordinate with adjacent agencies, Statewide Interoperability Executive Committees (SIEC), and Regional Planning Committees (RPCs). Involvement in these groups, training programs, and exercises will aid in the planning and development of cooperative and effective agreements. The relationships developed in the process are an important component and will aid when execution of the plan is required. It is important to determine what interoperability resources

²⁴ See BP #2 Interoperability Systems Change Management Practices - <http://npstc.org/radioInteropBP.jsp>

are available, where they work (coverage), who operates and maintains them, and the process necessary to access and use them.

Develop Training and Job Aids

Once an agreement is developed, documents should be created which are tailored to a specific public safety audience, (e.g., telecommunicator, first responder, and trainer). This may include flip charts, visual coverage maps, and other resource information for PSAP personnel.

Alternatively, it may include a Field Operations Guide, radio matrix quick reference card, or smart phone app to support field users and COMLs. It is also recommended that checklists and quick reference flow charts be created to guide the response to an interoperability system failure. These tools will help assure the proper steps are taken when interoperability systems are utilized or when problems occur. Training on the use of these job aids is a critical component to successful interoperability utilization.

Practice and Use

Familiarity with the process to request, access, and recurrent use of the various interoperability systems and components leads to proficiency and validates the SOP, the infrastructure, the training, and the job aids. Frequent use also reveals gaps or other previously undiscovered issues and concerns that may need correction.

Periodic tests of the system through planned and unplanned stakeholder roll calls and drills will help keep the users aware of its presence.

Roll calls and drills will:

- Identify failures prior to an incident, including connectivity concerns, latency, and poor performance.
- Enhance the proficiency of communications center personnel with repeater and system activation/deactivation and knowledge of additional console resources available for assignment.
- Assist in identifying any unauthorized use or use of the interoperability resource that is contrary to written agency SOPs.
- Familiarize field users with capabilities and features of the various interoperability systems.

Related Documents

The following list points to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practice Working Group page²⁵ on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.²⁶

[NPSTC Public Safety Grade Report](#)

[Oklahoma State Emergency Operations Center Radio Network Test Log](#)²⁷

[Tennessee Homeland Security District 5 Rollcall Script](#)²⁸

[Arizona Interagency Radio System \(AIRS\) State Plan](#)²⁹

[Interoperability Channel Roll Call Log Example](#)³⁰

Date Approved

May 25, 2017

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

²⁵ <http://npstc.org/radioInteropBP.jsp>

²⁶ Select Interoperability Committee -> Best Practices -> Shared Documents

²⁷ http://npstc.org/download.jsp?tableId=37&column=217&id=3873&file=800_MHz_Radio_Test_Log.pdf

²⁸ http://npstc.org/download.jsp?tableId=37&column=217&id=3874&file=Homeland_Security_District_5_Roll_Call_Procedures_Script_Appendix_C.pdf

²⁹ <http://npstc.org/radioInteropBP.jsp> -> Best Practice Reference Documents

³⁰ http://npstc.org/download.jsp?tableId=37&column=217&id=3875&file=Interoperability_Channel_Roll_Call_Log_Example.pdf

7.6 Best Practice #6 - Channel Assignment Based on Infrastructure Coverage

Best Practice #6: Channel Assignment Based on Infrastructure Coverage

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the [Radio Interoperability Best Practices Report](#)³¹ companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Interoperability channels should be assigned based on the documented and known infrastructure coverage between the radio networks and the radio communication devices that are being utilized.

Scope of this Best Practice

This Best Practice is intended for channel assignment of any channel recognized as a mutual aid or interoperability channel, whether it is local, regional, state, federal, or tribal. For the purpose of this Best Practice, the term “interoperability channels” is not limited to the channels listed in the NIFOG.

Statement of Importance

Interoperability channels and resources used to support an incident should be selected based on documentation that verifies the system’s capabilities, including geographic coverage and availability in first responder radios. Interoperability channels and resources should be tested to ensure their capabilities are verified and the results should be documented and distributed to all potential users.³²

Infrastructure coverage is defined as the radio system’s current coverage and reliability in a geographically bounded area with subscriber radios (mobile, portable, etc.) that will be used during an incident. As the subscriber radio types deployed may vary from agency to agency, interoperability channels should be tested prior to assignment to confirm that the radio communications coverage for a given area will be successful. This includes the ability to communicate both in building and over a wide geographical area using mobile and portable radios

³¹http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_IO_Best_Practice_Overall_Report_Final.pdf

³² This includes PSAP supervisors, operators; radio system technicians and to field level first responders.

Maintaining radio contact between first responders and the supporting communications center is important, but should not necessarily be the primary reason for channel and resource selection. There may be specific tasks within an incident where limited communications are needed which may be provided using simplex radio channels that are not available to the communications center.

Channel selection should always be based on the operational requirements of the incident and those requirements should be documented or communicated in advance. This allows for selection of the most appropriate resource and prevents over or under utilization of interoperability systems. The use of an interoperability channel should always be in conformance with the documented capabilities and limitations of the channel resource that has been selected. First responders and telecommunicators should always be aware of system limitations that may impact operations if the selected interoperability resource is less than optimal.

Insufficient planning prior to assignment of an interoperability resource to support an incident or event often results in poor, unreliable, or even non-existent communications between assigned operational teams and/or the communications center.

The initial assignment of an interoperability channel or resource starts with an established or suggested assignment practice. It may also be based on a request to the on-duty dispatchers responsible for the area in which the incident is occurring. As the incident expands, immediate interoperable decisions are critical, and knowledge of the local, regional, and statewide assets that can be brought into the incident is paramount.

Interoperability channel assignments and the ability of the systems to support them is an ever changing dynamic. Documented or known infrastructure coverage, the use of this knowledge prior to channel assignment to an incident, along with pre-established governance³³ and change management³⁴ comprise the decision making process when a selection is made.³⁵

Supporting Elements

Ideally, the decision of which channels or talkgroups to assign to an incident would be transparent to the telecommunicator and should be based on established policy. The policy

³³ See Best Practice #4 – Interoperability Relationships -

http://npstc.org/download.jsp?tableId=37&column=217&id=3902&file=BP_4_IO_Relationships_Final_170403.pdf

³⁴ See Best Practice #2 - Change Management Practices -

http://npstc.org/download.jsp?tableId=37&column=217&id=3856&file=BP_2_IO_Sys_Change_Mgt_Practices_Final.pdf

³⁵ The NPSTC Best Practice report and other Best Practice Statements can be found on the NPSTC website at <http://npstc.org/radioInteropBP.jsp>.

may be based on the incident's location and the most appropriate and available channel to support the operations. Some agencies use wall charts and maps to display this information while others use automated dispatch software that provides recommendations for channels or talk groups that have been determined to have the highest reliability for the incident area and type. Maps are commonly used and are typically developed internally to provide visual guidance on what channels or talkgroups are the most appropriate for an incident. Other common methods to determine resource assignment are based on historical experience and system status knowledge. All of these are highly reliable methods and all support this best practice by avoiding the assignment of resources without sufficient information on their capabilities.

Telecommunicators should receive initial and recurring training on how resource assignments are made. This training should include familiarization with, or use of, local, regional, and statewide interoperable assets and their associated coverage capabilities. These assets can typically provide wider area coverage and should be preprogrammed into agencies subscriber units. It should be noted that regional and statewide systems may operate in a different manner than the local radio systems used on a daily basis.

SAFECOM Continuum

Channel Assignment Based on Infrastructure Coverage touches every lane of the Continuum, which effectively demonstrates its importance.

Incident Use Case Examples

Use Case #1. Multiple agencies are responding to an incident that requires the assignment of an interoperability channel in a remote section of the home agency's jurisdiction. Previous testing has shown that the incident location has little to no communication infrastructure support on all channels available to the communications center, but all channels and their coverage abilities have been well documented in advance (direct only, repeated local, or linked to the communications center). The computer aided dispatch (CAD) system has been preprogrammed to recommend primary and alternate interoperability channels that best meet the coverage needs for the incident location and type. The responsible telecommunicator instructs responding units to select the appropriate channel. Initial units arrive on the scene and advise the communications center that the channel assigned does not provide the support needed. An alternate channel is selected based on the CAD recommendation and both on scene and responding units are advised of the change. The communications center announces the channel

that has not provided the expected level of support as unavailable for assignment and follows the predefined policy to initiate the repair.³⁶

Use Case #2. A Search and Rescue Mission for a missing hiker in a rugged mountainous region requires interoperable communications between Search and Rescue (SAR) personnel, the local EMS provider, and the County Sheriff's Office. Due to the box canyon nature of the search area, there is no infrastructure solution that provides uniform coverage and the terrain is not conducive to long-range simplex operations, thus requiring a deployable solution. Deployment of a portable repeater with battery and solar cell charging systems to a nearby elevated area is determined to be the best solution, based on prior planning which identified all available interoperability resource in the region and their technical capabilities. The deployable asset provides reliable radio communications to all team members at the incident and also allows access, including satellite Internet capability, to the Sheriff's Office dispatch center.

Migration Path

One of the first steps involves identification of all interoperability resources available to an agency or region. Planning, training, and testing are all based on the available infrastructure. Relationships and the use of a Memorandum of Understanding (MOU) or similar instrument are important to document ownership, maintenance and repair responsibilities.³⁷

Interoperable radio channels assigned to an incident should be chosen based on the availability of the communications infrastructure, frequency band operations, and console access in and around the affected area. The following steps articulate the sequential actions to improve interoperability based on the discussion in this Best Practice:

- Step 1. Determine which local and regional infrastructure is available for use during an event or incident.
- Step 2. Ensure MOUs/MOAs are in place with most logical responders who will use the interoperable channels.
- Step 3. Ensure interoperable channels/talkgroups are programmed into all appropriate subscriber units.
- Step 4. Develop coverage maps for existing infrastructure for both portable and mobile subscriber units. In the short-term, this step can be used to train dispatchers about the

³⁶ See Best Practice #5 – Infrastructure Management - http://npstc.org/download.jsp?tableId=37&column=217&id=3936&file=BP_5_Infrastructure_Management_Final_170517.pdf

³⁷ See Best Practice #4 – Interoperability Relationships - http://npstc.org/download.jsp?tableId=37&column=217&id=3902&file=BP_4_IO_Relationships_Final_170403.pdf

system, provide a Communications Unit Leader (COML) with information should it be required, and, in the longer-term, be used to develop automation in channel/talkgroup assignment for event/incident support.

- Step 5. As system upgrades and changes are made, ensure that proper training is conducted for dispatch center staff and associated personnel as it relates to system coverage and performance.
- Step 6. Practice or simulate multiple scenarios in different areas to provide real-world experience with system performance across its mapped coverage area.

Related Documents

The following links point to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Radio Interoperability Best Practice Working Group page on the NPSTC website at www.NPSTC.org or by joining the NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.³⁸

[Allied Radio Matrix for Emergency Response \(ARMER\) Standards, Protocols, Procedures](#)
[Phoenix Regional Interoperability Guide](#)
[Arizona Interoperability Radio System \(AIRS\)](#)³⁹

Date Approved

July 2017

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

³⁸ Select Interoperability Committee -> Best Practices -> Shared Documents

³⁹ AIRS SOP -

http://www.npstc.org/download.jsp?tableId=37&column=217&id=3928&file=Arizona_AIRS_SOP_10192010.pdf

7.7 Best Practice #7 - Interoperability Resources—After Action Reviews

Best Practice #7: Interoperability Resources—After Action Reviews

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the Radio Interoperability Best Practices Report companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Any After Action Review (AAR) held following a significant emergency incident or preplanned event that involved interoperability resources should include both operational and technical components including those which focus on communications infrastructure.

Scope of this Best Practice

The general perception of an AAR involves a formal, detailed report following a large scale or highly complex incident and centers around the operational intent and outcomes of the event. In reality, many AAR sessions involve an EMS crew sitting on the back of the ambulance or a small group of law enforcement officers at a briefing room table discussing the call they just returned from. AARs may also generate a thorough and detailed account of the incident and be hundreds of pages in length following group discussions, individual interviews, and detailed incident review.

Though the interoperability and operational aspects of an AAR may intersect, the scope of this best practice is limited to the need to add a technical component and include any interoperability resource issues as a formal component of each AAR.

This Best Practice is not intended as a guideline for the creation of an AAR.

Statement of Importance

An AAR should document incident or exercise findings, bringing operational, technical, and policy issues to the forefront with the intent to improve overall emergency response while also addressing communications interoperability for the safety of first responders.

AARs are normally conducted at the end of an incident or training exercise though many agencies are taking the time to incorporate AARs during the planning stage. This approach provides review of potential failures before they happen, ranging from radio programming opportunities to specialized equipment needs. On extended incidents, such as a wildland fire, it may be necessary to conduct a brief version of an AAR at the end of each operational period to

capture lessons learned for incorporation into the next day's planning process. Most agencies do a debriefing on the day's operations, but an AAR is distinct in that it begins with a clear comparison of intended vs. actual results achieved and identifies the successes and areas of improvement.

Proactive agencies conduct critical examinations of their operations and look for ways to enhance their operable and interoperable communications. Agencies which do not include communications specific discussions during their AARs miss an opportunity to examine and resolve familiar failures, including channel/talkgroup assignment errors, first responder equipment knowledge gaps, and underutilization of console and gateway resources. Public safety agencies benefit by becoming engaged with established local and regional communications working groups and by becoming involved in the AAR processes that provide a safe and more positive outcome for future events.

Supporting Elements

An AAR is a simple process used by public safety agencies to capture the lessons learned following a recent incident, to include both the successful and challenging components of the response. The goal of an AAR is to improve future performance. It is an opportunity to reflect on an incident, training exercise, or planned event so the agency may perform better the next time. It is recommended that both technical and operational⁴⁰ personnel be involved in the entire AAR review process. Many radio systems today provide a large amount of performance data that can be leveraged to better understand the root cause of operational successes and failures. Likewise, CAD systems also provide an abundance of documentation on minute-by-minute actions at the scene. This information can significantly enhance the quality of the AAR discussions and resulting recommendations.

The components of the interoperability section of an AAR are identical to the overall report itself, but should provide information on communications specific issues:

- What was supposed to happen?
- What actually happened?
- What caused the differences?
- What went well and why?
- What could be done differently the next time?
- Who needs to know?

⁴⁰ Operational personnel include both responders and dispatchers.

The goals of the AAR Interoperability section are also identical to the overall goals of the review:

- Capture observations of the incident/exercise.
- Identify best practices and lessons learned.
- Highlight strengths/acknowledge successes.
- Ascertain specific improvement actions if needed.
- Assign those actions to the responsible parties.
- Establish target date for action completion.
- Test, document, and train upon the improvements.

While there are many ways to conduct an AAR the process should be kept as simple and as easy as possible for stakeholders, with the intent to address any concerns discovered during the review. Challenges and concerns documented during the AAR should be turned over to appropriate subject matter experts who will focus on the desired outcome and make necessary changes or suggestions. Any changes arising from an AAR need to be formally documented. This includes the need to update SOP manuals and written policy.⁴¹ These updates should reach all affected parties and training should occur to ensure knowledge of the operational and technical changes.

SAFECOM Continuum

This Best Practice touches the Governance, Standard Operating Procedures, Training, and Usage lanes of the SAFECOM Interoperability Continuum.

Incident Use Case Examples

Oceans County Sheriff's Office (OCSO) owns and operates a countywide 800 MHz radio system. Dade City Police Department (DCPD) is an agency within Oceans County, which operates as a partner on the county's 800 MHz system. The DCPD is responding to a disturbance call and shots are fired upon the arrival of the first officer. An area-wide alert is broadcast by DCPD dispatch for mutual aid. An OCSO unit is in the vicinity and responds to the DCPD call. The telecommunicator coordinates activation of an interoperability solution, announces control of the patch, and directs responders to select the agreed upon interoperability talkgroup. DCPD made the console patch providing the necessary interoperability and OCSO responders selected the assigned talkgroup in their radio equipment. This successful process was based on changes

⁴¹ See Best Practice #2 – Interoperability Systems Change Management Practices - http://npstc.org/download.jsp?tableId=37&column=217&id=3856&file=BP_2_IO_Sys_Change_Mgt_Practices_Final.pdf

which were approved following recent challenges highlighted in another AAR report. Lessons learned in a prior incident resulted in updated policy and training. A prior AAR had revealed that once a talkgroup has been patched by an agency console, it cannot be patched with other resources by another console.

Migration Path

The inclusion of an interoperability component to an agency's AAR process can be easily accomplished, especially if the agency/region has an AAR or other review policy already in place.

Interoperable resources are typically shared on a regional, state, or nationwide basis; and the interoperability components of an AAR are common to the larger AAR format. Therefore, adding an interoperability component to a local, regional, or statewide AAR policy can be done with minimal effort. Likewise, if an individual agency does not have an AAR policy in place, it is recommended they develop a policy of their own or modify one from another agency within the region. Areas with a high occurrence of mutual aid incidents may consider developing a regional approach to the AAR process including both operational and interoperability components.⁴²

Recommended steps to create the Interoperable Section of an AAR should include:

- Review the policy and procedures manual with a combined group of operational, communications, and technical personnel.
- Identify areas related to interoperability resources that are not addressed in the overall AAR.
- Modify the policy as needed.
- Plan an exercise to confirm the recommendations are valid.
- Distribute revised information to all stakeholders.
- Define a process for addressing future AAR recommendations.

When reviewing interoperability policy and procedure, the following issues should be examined as they directly impact future AAR recommendations:

- Which agency is responsible for each piece of interoperability equipment?

⁴² See BP #5 – Infrastructure Management - http://npstc.org/download.jsp?tableId=37&column=217&id=3936&file=BP_5_Infrastructure_Management_Final_170517.pdf

- What are the operational parameters of each interoperability resource? (console patching, gateway devices, conventional repeater coverage, etc.)
- Who is responsible for completing the AAR report? (Logistics Chief, Communications Officer ,⁴³ etc.), and what is the process to distribute the findings and recommendations?
- What is the testing process to ensure interoperability equipment is in a ready state?
- What is the SOP update process, to include telecommunicator and first responder training?

The situations faced by public safety vary significantly depending on location, resources, and incident type. And the intricacies of a multi-agency event make it difficult to create an AAR that covers all of the possibilities. Appendix A provides an extensive list of topics that may need to be addressed in the communications section of an AAR. This document is not an AAR template, but intended as a checklist to assist in identifying items to be considered, including operational, interoperability, and technical components. This list is not all inclusive and not every topic listed will be relevant on every incident or event.

Related Documents

The following links point to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Radio Interoperability Best Practice Working Group page on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.⁴⁴

The [Homeland Security Exercise and Evaluation Program \(HSEEP\)](https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf) provides a set of guiding principles for exercise programs, as well as a common approach to exercise program management, design and development, conduct, evaluation, and improvement planning. HSEEP exercise and evaluation doctrine is flexible, adaptable, and is for use by stakeholders across the whole community and is applicable for exercises across all mission areas – prevention, protection, mitigation, response, and recovery. - https://www.fema.gov/media-library-data/20130726-1914-25045-8890/hseep_apr13_.pdf

The **NPSTC Best Practice Report and other Best Practice Statements** can be found on the NPSTC website at <http://npstc.org/radioInteropBP.jsp>.

[NPSTC Communications Unit AAR – Example Checklist for Event Incident/Exercise Report](#)

⁴³ The COML may not be with the same agency as incident command.

⁴⁴ Select Interoperability Committee -> Best Practices -> Shared Documents

Date Approved

September 7, 2017

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

Appendix A

Example Checklist for Event Incident/Exercise Report

National Public Safety Telecommunications Council
Radio Interoperability Best Practices
Communications Unit AAR –
Example Checklist for Event/Incident/Exercise Report

The following is an extensive list of topics that may need to be addressed in the communications section of an After-Action Report (AAR). This document is not an AAR template, but intended as a checklist to assist in identifying items to be considered, including operational, interoperability, and technical components. It is understood that this list is not all inclusive and that not all incident or events will touch every topic.

Incident	Does the report contain the following incident information?	
		Incident/Event/Exercise Name
		Incident/Event Location
		Incident/Event Date(s)
		Brief description of the incident/event
		A complete list of units on the scene
		Response Agencies Involved: Local /State/ Federal /Tribal/Non-Government Organizations
		Commercial Vendors Involved
		Agencies Providing Communications Equipment or Assistance
		Commercial Vendor(s) Providing Assistance
		Is the Comm Plan, ICS205, and 217A included in the AAR?
	Is there a copy of the CAD event entry information available for reference?	
Overview	Overall Communications and Technical Review	
		Things that went well
		Areas for improvement
		Recommended steps for correction ⁴⁵
Communications Unit:	Include list of positions filled, including name, agency, and ham call sign	
		Communications Unit Leader (COML)
		Communication Technician (COMT)
		Radio Operator (RADO)
		Telecommunications Specialist (THSP)
		Incident Communications Manager (INCM)
		Auxiliary Communications Personnel (AuxComm)
		Incident/Tactical Dispatcher (INTD)
		Messenger or Runner
	Were personnel evaluations performed?	

⁴⁵ Areas flagged for correction should be forwarded to the responsible party in accordance with the agency policy and change management process.

Communication System Types	What communications system types were used? ⁴⁶
	Trunked
	Conventional
	Analog
	P25
	Other digital formats
	Cellular/Satellite
	Amateur Radio
	FirstNet/Broadband
Other	
Interoperability Continuum	SAFECOM Continuum
	Were there any Governance/Policy Issues?
	Were there any SOP / TIC-P / FOG issues?
	Were there any technology issues?
	Were there any planning or training issues?
Were there any usage issues?	
Mobilization and Demobilization	Mobilization and Demobilization
	Were there any notification issues with mobilization?
	Were there any response issues with mobilization?
	Were there any technical issues with mobilization?
	Were there any credentialing issues with mobilization?
	Were there any notification issues with demobilization?
	Were there any response issues with demobilization?
	Were there any technical issues with demobilization?
	Were there any documentation or check out issues with demobilization?
	Were there any safety issues?
Were there any accountability issues?	
PSAP Operations	
PSAP/ Communications Center/ EOC	E9-1-1/Emergency Number/NG9-1-1
	Were there any issues with the public calling in to E9-1-1?
	Were there any issues with the PSAP receiving incoming E9-1-1 calls?
	Were there any issues with the non-E9-1-1 emergency phone lines?
	Were there any issues with the non-emergency phone lines?
	Were there any issues with dedicated phone lines or ring down lines?
	Did the roll over process perform as expected?
	Were there any issues with text to 9-1-1?
	Were there any issues or usage of video to 9-1-1?
	Notifications in the PSAP/EOC
	Were there any issues with the outgoing notification system?
Was a dispatch network notification used to broadcast situational awareness to	

⁴⁶ Include both first line and support personnel in each position

		affected agencies, i.e., announcement of 911 overflow, announcement of channels in use, etc.?
		Was Reverse 911 (Community Emergency Notification Service) used?
	Communications Center	
		Were there any operational issues with the dispatch console?
		Were there any issues with resource availability in the communications center?
		Was emergency power needed, and, if so, was the transition seamless?
		Were all communication channels managed through PSAP and PSAP telecommunicator or were additional channels managed by field positions or onsite tactical telecommunicators (tactical, air, etc.)?
		Was the telecommunicator familiar with the interoperability resources?
		If needed, were back up positions available and operating correctly?
		Was the communications center staffing level sufficient to meet the needs of the incident?
		Did CAD withstand the influx of data entry and query requests?
Resource Requests		
	Deployable and Fixed Resource Requests	
		Were there any requests for deployable resources?
		What resources were requested?
		Who were requested resources through/from?
		Who (agency) provided resources?
		Who made the request and how was it transmitted?
		Were there any notification issues with deployment of requested resources?
		Were there any technical issues with deployable resources?
		Were there any response issues with mobilization?
		Did sufficient staffing and instructional support arrive with the deployable resource?
		Did a resource briefing take place ensuring resource awareness? E.g., operational knowledge, reference materials, supplies etc.
		Was the equipment returned in the same condition as it was when assigned? (e.g. missing antenna, knob, cracked display).
		Were there any concerns with the return equipment process? Flowed effectively? Was this accomplished in a reasonable amount of time?
Handheld Subscriber Devices		
	Portable Radios	
		Were any cache radios utilized and, if so, how many were deployed?
		How many of the cache radios deployed were actually utilized?
		What channels were used?
		Any radio maintenance issues?
		Any lost radios or accessories?
		Any issues with radio programming?
	Was the battery management plan effective?	
		Multi-unit chargers
		Disposable batteries
		Clam Shells
		Any battery issues identified?
		Was there ample staffing to prepare and deliver the supplies in a timely manner?

Gateway	Was a gateway or console patch utilized?
	Were there any issues with the gateway and/or patch?
	What channels were used in the gateway and/or patch?
	What agency initiated the gateway and/or patch?
	How was the patch created? (ACU/ICRI/RIOS/Other/Console Patch)
	Was the gateway/patch initiated in a timely manner?
Portable Repeater or Base Station	What Channels were used in the repeater/base station?
	VHF (Lo/Hi)
	UHF
	700 MHz
	800 MHz
	Local system
Interoperability Channels	Nationwide / Regional / State / Local Mutual Aid or Interoperability Channels Utilized:
	V/U/7/8 CALL or V/U/7/8 TAC
	Interop Talk Groups
	Direct or TA
	Any other frequency resource used? HAM, Marine, AIR, etc.
Deployable Infrastructure Support Resources	Were any of the following resources used?
	Radio Tower Trailer(s)
	Conventional / Trunked Sites on Wheels
	Generator(s) on Wheels
	Agency Leased Satellite Services (PTT, Voice, Data)
	Tactical Bi-directional Amplifier (BDA)
	Tactical Digital Vehicular Repeater System (DVRS)
	Mobile Communication Unit (MCU) or Mobile Communications Vehicle (MCV)
	WIFI/ Internet Access
	Microwave, Fiber, Inter-Connect System
	Airborne repeaters (Maned or Unmanned)
	Airborne Video
Radio Communication Sites	Were there any issues regarding the following?
	Site Access
	Shelter
	Site Security
	Commercial Power
	Wind or Solar Power
	UPS
	Battery Back Up
	Generator and/or Fuel
	Grounding system
Tower	

		Tower antenna
		Tower lights
		Feedline
Voice and Data Resources	If used, were there any issues of the following resources?	
	Commercial Wireless:	
		Voice
		Data
		Cellular on Wheels (COW)
		Cellular on Light Truck (COLT)
		Aerial Communications ⁴⁷
	Mobile Data:	
		Commercial – Air Card
		FirstNet - Fixed Site and/or Deployable
		Agency Owned
	PSTN/VOIP	
		DSL, T1, T3, etc.
		Voice
		Landlines
		Fax
		Voice Over Internet (VOIP)
	Satellite	
		Voice
	Data	
	Push to Talk (PTT)	
Emergency Telecommunications Services		
	Wireless Priority Services (WPS)	
	Government Emergency Telecommunications Services (GETS)	
	Telecommunications Services Priority (TSP)	
Notification System	Where any of the following notification systems used?	
		Emergency Alert System - EAS
		Integrated Public Alert Warning System - IPAWS
		National Oceanic and Atmospheric Administration - NOAA
		WEA – Wireless Emergency Alerts
		Any Local, Regional or Statewide Systems
		Pager
		Smart Phone App
		Text Messages
		Prompt Notification System (Sirens)
		Reverse 9-1-1

⁴⁷ Cellular on Wings (Flying COWS), Tethered Balloons, etc.

Additional Concerns	Where any of the following an issue and was follow up needed/completed?	
	Was there any lack of radio coverage; i.e., "dead spots" observed during the event.	
	If yes, what was the underlying cause?	
		Coverage issue
		System maintenance issue
		Channel assignment
	Were there any "blocked" or excessively busy resources such as radio or telephone channels that were overloaded with traffic, thus preventing or delaying messages from being received?	
	Were there any unexplained communication failures that occurred during the event?	

7.8 Best Practice #8 - Radio Device Management

Best Practice #8: Radio Device Management

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the [Radio Interoperability Best Practices Report](#)⁴⁸ companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Management of interoperability resources and radio devices should include a formal plan that ensures accurate radio programming and confirms the readiness of the equipment. This includes mobile and portable devices, as well as radio cache resources.

Scope of this Best Practice

This Best Practice is intended to address the need to maintain all radio devices which may be used to support interoperable communications. This includes agency-owned devices being used to support interoperability, radio caches,⁴⁹ and vehicular radios, all of which require a ready state.

This Best Practice is not intended to address Infrastructure⁵⁰ or the deployment of interoperable resources.⁵¹ Nor is it intended to develop an agency's operational plan for a local radio system.

Though this Best Practice will not specifically address portable repeaters, it is understood that they should be maintained in accordance with the same recommendations stated for radio devices included within the scope.

Statement of Importance

The goal of interoperability is to facilitate effective communication among various agencies in an emergency situation. In the event of a large multiagency incident or event, it is often

⁴⁸ http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_IO_Best_Practice_Overall_Report_Final.pdf

⁴⁹ For the purpose of this document, a radio cache is not limited to handheld radios but includes all other wireless assets (e.g., mobile radios, cell phones, wireless internet, satellite (SAT) phones, and other ancillary support equipment such as batteries and chargers.

⁵⁰ For more information see Best Practice #5 Infrastructure Management

⁵¹ For more information see Best Practice #9 – Deployment for Interoperability Resources

necessary to utilize additional assets to achieve that goal. To ensure that interoperability resources are operational and prepared for deployment, it is important for agencies operating independently or within an approved Memorandum of Understanding (MOU) to establish a robust maintenance and inventory policy. When followed, a well-conceived policy will ensure the accuracy of radio programming; verify the readiness of the equipment; include training recommendations on the operation of and interoperability aspects of the resource; define governance and responsibility; and confirm compatibility with other deployable resources. This includes mobile and portable devices, as well as radio cache resources.

It is important that any resources identified for interoperability communications are maintained appropriately and are confirmed to be programmed and operational under a defined communications plan. When a communications plan, whether it is local, regional, or state, is adopted or updated, a campaign to update radio devices must occur. Important considerations to the campaign include effective date, time to program, method of training, and validation of the device.

When a request is made for additional resources, they should be ready for assignment and procured easily with fully prepared accessories and accurately documented inventory. Knowledge of what resource may be needed, as well as the request procedures and the availability and programming capability of the device is vital to a successful communication outcome.

Supporting Elements

A radio cache is the basic level of interoperability between multiple agencies and responders. When developing a plan for interoperability, whether it is local, regional, or statewide, it is important to include policy and procedure provisions for the management of available radio caches and vehicular radios that are designated as an interoperability resource. The chances of communication failures increase when these fundamentals are not identified, agreed upon, implemented, and practiced regularly.

There are many components to the management of interoperable radio devices including programming, charging, ownership, identification and inventory, accessories, maintenance, mobilization and demobilization, technical support, and training recommendations.

Programming: All cache radios in the region should be programmed in accordance with regional programming guidance appropriate to their make, model, type, and frequency band.⁵²

⁵² SAFECOM Template page 22

It is critically important that radio programming is accurate and that a quality assurance cross check is performed to ensure the various parameters are entered correctly. Programming the radio incorrectly can result in failure of the radio to perform as needed, even when it appears to be working correctly. Personnel tasked with programming cache radios should be fully trained and properly equipped. The PAM Tool⁵³ is a valuable resource when programming large quantities of radios for many different makes and models.

Charging: Cache radios must be fully charged and ready for immediate deployment when requested. Deployed equipment includes extra batteries and battery chargers to support extended deployments.

Ownership: The owner is the person or agency responsible for the device. Although the device may be operated by multiple users and programmed by several technicians, it is important to define ownership for the purposes of inventory and responsibility. Ownership and inventory may be one and the same for many agencies, but this is not always the case.

Identification and inventory: Each radio in a radio cache should have a unique identification number (e.g., serial number, etc.) for inventory tracking. Devices should be labeled by engraving or a secured tag on the body of the device. Agencies may also consider affixing a bar code sticker on each radio and including a barcode reader and computer software that allows the deployment team to quickly scan and enter basic information for first responders using the radios.⁵⁴ A local, regional, or state agreed-upon numbering system will help when a device is missing or recovered. Though agencies may use their own inventory to support a scene rather than a shared radio cache, it is important those agency-owned radios be maintained following the same protocols. There should be an inventory control system which logs the assignment and return of cache radios. Proper documentation aids in the recovery of missing or misplaced equipment.

Assignment: Each device programmed will have an internal ID which is associated with a user, a location (i.e., in a Command vehicle), or radio cache. When the device transmits, the ID in most cases will display on the system ID tracking program and/or over a console. Once radios have

⁵³ [NPSTC PAM Tool](#) -

https://www.google.com/url?q=http://npstc.org/download.jsp%3FtableId%3D37%26column%3D217%26id%3D3010%26file%3DNPSTC_PAM_Tool_A&sa=U&ved=0ahUKewixkuXao_jXAhXn4IMKHYUnBZsQFggEMAA&client=internal-uds-cse&cx=016962067942227185377:lfD0n8m4vhm&usg=AOvVaw3uJdY8cPMeMnKxL3HmJiVL

⁵⁴ Communication Interoperability, "So You Want to Start Off With a Portable Radio Cache", www.policeone.com
<https://www.policeone.com/police-products/communications/articles/137350-So-you-want-to-start-off-with-a-portable-radio-cache/>

been distributed, the assignment information should be relayed to the communications center to assist with identification in the event a cache radio's emergency button is activated and the internal ID is displayed on the console.

Accessories: A radio cache that contains only radios is only functional until the batteries die. It is equally important to confirm that each radio in a cache is fully charged and that needed accessories are available. Spare batteries and battery chargers equal to the number of radios in the cache should be included. Agencies should consider a variety of batteries including rechargeable, single use for emergencies, and those that can be powered with alkaline batteries such as AA. This third type is especially important when the cache is being deployed into a situation, such as post hurricane, in which power is an issue and it may be easier to have commonly available disposable batteries delivered. Additional accessories include microphones and replacement antennas. Other very important accessories that can easily be overlooked are transport vehicles, to include trailers, hard weather-proof storage cases, portable repeaters, and interconnect switches complete with a large assortment of cloning and programming cables for every model of portable radio in the region. Broken and poorly maintained equipment must be removed from service and not issued to personnel being assigned into an operational environment.

Maintenance: Routine and seasonal maintenance is imperative to keep interoperability equipment regularly available for deployment and ensures the device is ready to perform at its best when needed the most. Cracked and worn cable covers, batteries that will not charge properly, broken radio display windows, missing knobs, and wrong antennas can result in less than optimal communications and potential injury to the user. Scheduled maintenance should be performed regularly as well as seasonally depending upon anticipated usage (i.e., prior to wildfire or hurricane season) and following any deployment. The use of interoperable resources and radio cache equipment should also be used during any planned interoperability exercise. This will allow an additional opportunity to confirm the readiness of the equipment as well as providing training and familiarity of the equipment to the first responders. The replacement of faulty equipment should be fully documented and forwarded to the appropriate party.

Mobilization and Demobilization: When cached resources are requested, the responsible point of contact (POC) or technical specialist (THSP) should be notified to retrieve the requested equipment and deliver it to the scene. Upon arrival, they should sign the cache over to the requesting agency for incident use or, if assigned to, remain on the scene, to coordinate radio cache deployment procedures with the Communications Unit.

To ensure inventory management, the distribution of cached resources on the scene must be fully documented. The COML or their designee should maintain a record of each user and

agency to which a radio and associated accessories have been distributed, document the identification number of each radio deployed, and the channels in use. A brief overview/introduction of the radio and the relevant portions of the communications plan (e.g., short list of channel assignments, concise set of notes for quick reference, etc.) should be provided to those receiving the cache radios. Each user and/or agency that receives a radio from the cache will be responsible for returning that radio and all associated accessories to the cache at the end of the incident.

When cache radios and accessories or equipment are no longer required to support the incident, they should be returned to the radio cache POC location in the same condition and configuration as they were issued. Prior to return, the incident COML should confirm the contents of the cache and determine if any radios or accessories are missing or damaged. If applicable they should also note the user and agency to which the missing or damaged equipment was distributed and provide that information to the POC for resolution. Responsibility for lost or damaged equipment should be defined and dictated by existing policies and procedures.



Technical support: Qualified radio cache THSPs or COMTs familiar with the necessary documentation and device operation and capabilities should be available for on-scene support during the deployment if the requesting agency cannot act in this capacity.

Documentation: Documentation should be present in all radio caches as part of the inventory. This includes a list of the complete inventory with radio ID noted, a copy of the originally programmed communications plan, a list or photo of the contents in place in the case to assist with repackaging for return, POC information, and any other documents deemed necessary by policy. Additional documents may include quick reference guides or device tutorials or other “cheat sheet” reference materials.

A radio cache requires constant maintenance and therefore should be maintained by an agency that has the personnel, space, and dedication. In order for a device to operate in accordance with written guidelines or policy, there are multiple aspects to consider, from local agency inventory to shared asset inventory, and from the type of asset available up to its operational condition. Use of common forms and practices, saves time and aids in the management of devices and resources

SAFECOM Continuum

This Best Practice touches the Governance, Standard Operating Procedures, Training and Usage lanes of the SAFECOM Interoperability Continuum.

Incident Use Case Examples

Liberty County Fire Department is on the scene of a multiple acre brush fire that is threatening nearby housing, business, and schools. The scene needs are changing and assistance from local and out of area regional partners is being requested. There are concerns with traffic, road blocks, evacuation, and communications. The local responders are directed to the common interoperability channels or talkgroups previously identified and trained upon for mutual aid incidents. When necessary, the radio is re-programmed by the Communications Unit on scene. Fire ground units require additional batteries and some are requesting second radios to interoperate with the incident agency. Due to the established local and regional partnerships, the request was handled in accordance with the written policies. Items that were prepared in advance include extra accessories, serial and internal ID tracking sheets, template and radio operation tip sheets, and a dispatch contact number. All of which saved time, money, staffing resources, and communication errors, and which is building a common ground for knowledge of interoperability for the future.

Migration Path

The successful management of interoperability radio devices must begin with a comprehensive policy which has been endorsed under an approved MOU. The final policy must be a collaborative effort involving all public safety stakeholders within a region and include communications and technical support representation from all the various disciplines affected by the plan.

The final policy should include a number of components that identifies:

- List of all radio devices covered by the plan
- Process and responsibility for inventory and maintenance of the devices
- Process and responsibility for mobilization and demobilization of the resources
- Process and responsibility for replacement of missing or broken equipment
- Maintenance program that ensures the resource is operational when requested
- Process to ensure the device internal ID is activated at the time of deployment
- Complete list of documentation to be included in the deployed resource
 - Inventory of the devices and accessories contained within the cache, including serial numbers
 - Currently programmed communications plan
 - Brief description of device operation
 - Copies of common documents i.e., IC 205, etc.
- Training and/or proficiency requirement for personnel responsible for or authorized to program the devices

- Written policy for deployment and demobilization⁵⁵

Agencies within the region should include the provision to request the use of these interoperable resources for all planned interoperability exercises or events to promote familiarity. This also results in an additional opportunity to confirm the accuracy of the inventory and the operational readiness of the devices and accessories.

The completed and approved policy should be reviewed routinely to identify any missing information or areas that require revision.

Related Documents

The following links point to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practice Working Group page on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.⁵⁶

Best Practice #5 - [Infrastructure Management](#)

Best Practice #9 – [Deployment for Interoperability Resources](#)

[SAFECOM Template page 22](#)

[PAM Tool](#) -

Communication Interoperability, "[So You Want to Start Off With a Portable Radio Cache](#)", - <https://www.policeone.com/police-products/communications/articles/137350-So-you-want-to-start-off-with-a-portable-radio-cache/>

Date Approved

December 6, 2017

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

⁵⁵See Best Practice #9 – Deployment for Interoperability Resources

⁵⁶Select Interoperability Committee -> Best Practices -> Shared Documents

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document

7.9 Best Practice #9 - Deployment for Interoperability Resources

Best Practice #9: Deployment for Interoperability Resources

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the [Radio Interoperability Best Practices Report](#)⁵⁷ companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

In any incident or event there must be an early awareness of the need for augmented communications support, at the scene and in the communications center, to include both interoperability resources, and supplemental technical and support staff.

Scope of this Best Practice

This Best Practice is intended to address the importance of identifying the potential need for supplemental interoperability resources in a timely manner thus allowing sufficient time to process the request, respond to the location, and complete set up and activation. These resources needs include both equipment and personnel.

This Best Practice does not address the multitude of other supplies and equipment which traditionally fall under the logistics area of responsibility.

Statement of Importance

Continuity of communications is central to the success of any incident or event. When managed properly, the use of interoperability resources such as radio caches, mobile command units, and deployable communications infrastructure has proven to be an effective tool in reaching that goal. However, failure to plan for and identify the need in a timely manner and allowing sufficient notice for response and set up, greatly reduces the impact a deployable resource will have on the outcome.

Additionally, successful deployment of interoperable resources does not begin with the request for assistance, but is instead the result of an established policy, and well-documented resources information including commonly defined types and capabilities.

⁵⁷http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_IO_Best_Practice_Overall_Report_Final.pdf

Training of both operational and communications personnel is an essential component. Promoting current knowledge of resources and the procedures that have been developed to deploy and utilize resources will greatly reduce the amount of time it will take to respond to the scene and be activated. Equally important is the need to maintain a current list of interoperable resources that are available at any given time, not just housed within the agencies included in the agreement

Public safety radio systems are configured for reliable, effective, and secure communications. Poorly implemented connections to other systems can impair or disable critical resources and increase risks to people and property in an emergency. Knowledgeable, skilled support personnel are needed to conduct the necessary planning to reliably and effectively plan for and deploy interoperable resources.⁵⁸

Planning, coordination, and training are key to having successful communications between first responders in any multi-agency/multi-jurisdictional incident. It is essential for agencies and regions to develop a deployment plan for interoperable resources that will incorporate and coordinate policy, training, and outreach activities for all personnel, at all levels.

Supporting Elements

“Incidents typically begin and end locally and are managed on a daily basis at the lowest possible geographical, organizational, and jurisdictional level. However, there are instances in which successful incident management operations depend on the involvement of multiple jurisdictions, levels of government, functional agencies, and/or emergency responder disciplines.”⁵⁹

For successful incident management, Incident Command must look towards what the incident is going to look like an hour or even a day ahead of time and coordinate the need for deployable resources during each operational period. The plan for the use of interoperability resources needs to be in place prior to the incident occurring. Preparedness planning should address the equipment, protocols, and support needed to achieve effective communications. Ideally, the plan should address multi-disciplinary concerns and should, at a minimum, be addressed on a regional level.

Established [Interoperability Relationships](#)⁶⁰ should include a plan for the responsibility, maintenance, programming, and usage of interoperability resources. The plan should also

⁵⁸ National Emergency Communications Plan: Urban Area Communications Key Findings and Recommendations, 2011, DHS

⁵⁹ NIMS – Introduction and Overview

⁶⁰ See Best Practice #4 – Interoperability Resources

provide verified documentation on existing resources, including amount, type, capabilities, and any additional personnel/services/policy needed to support each resource. This information needs to be updated for availability and accessible to both the communications center and command as needed.

Any policy addressing deployable interoperability resources should include direction for the following:

Timeliness of request: Within an incident, trigger points should be identified that will automatically escalate or cause the use of certain interoperability systems or resources. Considerations should be given for immediate needs vs. planned needs when requesting resources, noting that response time has to also include set up, activation, and the arrival of qualified staff. Specialty resources may require an extended response and set-up time and should be requested early in the incident. For instance, requesting the response of a mobile communications unit (MCU) would also entail the need for qualified personnel to be available to deploy and operate the unit.

Type of deployable: The speed with which a deployable resource can be expected to be operational greatly depends upon the type of resource being requested and can range from simple delivery and distribution of a radio cache; arrival and activation of a portable repeater; or the extended response time necessary to set up of the larger resources such as a MCU, System on Wheels (SOW), and Cell on Wheels (COW). It could also be as quick as identifying a channel or flipping a switch to activate additional frequencies for tasks within the incident such as Air to Ground (AG) for a wildland fire. Attention must be given to establishing an estimated response time when identifying potential resources during the planning process. Resource typing should be defined and used for all resources, regardless of the proprietary or responsible agency.

Additional resources to support the requested item: Not every deployable resource is self-contained. For instance, ordering a communications trailer may also require a microwave truck or a satellite truck and some may require additional trained personnel (such as a COMT) to be available for deployment. Additional communications personnel may be needed to support ancillary channels, both at the command post and in the Communications Center. Any plan for the deployment of interoperable resources should articulate both the resource and the support needed for a successful deployment. When planning for support staff, it is important to also consider the duty cycle and anticipated duration of the event.

Source of deployable resources: Most deployable resources within an interagency agreement will come from local, regional, state, or federal partners. Deployment plans should indicate the location of those resources to help determine the fastest response time, as well as contact

information, including the responsible agency or person. For the sake of expediency, it is important to have a phone number and a backup number in addition to an email. Some resources may come via vendors or other private sources with which the agency/agencies have a previously defined relationship. Contact and proximity information for those sources should mirror those of the public agency or mutual aid resources.

Training: All personnel, including technical, operations, and communications, need initial and ongoing training on the capabilities, limitations, location, and policy surrounding the use of interoperability resources. Training should include components on situational awareness, field training, and safety. While many agencies emphasis ICS training for operational personnel only, it is necessary that this training is extended into the communications center as well. Dispatchers are an excellent investment for training as they are in a safe environment, have access to resource materials, see the big operational picture, and, when properly trained, can assist in providing direction if needed. This is especially true for personnel assigned to a mobile communications unit team.

As with any agency policy or interoperability relationship, a robust change management process⁶¹ is required to keep the resource availability and capability list current and to ensure all stakeholders are included in the distribution of the updated information.

SAFECOM Continuum

This Best Practice touches the Governance, Standard Operating Procedures, Training and Usage lanes of the SAFECOM Interoperability Continuum.

Incident Use Case Examples

It is 10:00 a.m. and a fire has broken out in the foothills of the Misty Mountain range. The fire is spreading quickly towards the National Forest boundary and the County Fire Department has dispatched a second alarm. It is the policy of the County Fire Department to notify a Communications Unit Leader (COML) on all second alarm fires.

The Incident Commander has forecasted that the fire will crest a ridge and cross into the National Forest in about 6 hours, leaving the coverage footprint of the County Fire Command Channel. The COML has been trained in the deployment of County Fire's Mobile Communications Vehicle (MCV) and is aware of the 4-hour deployment and setup timeframe. The COML immediately initiates a call for a qualified Communications Technician (COMT) to bring the MCV to the check-in location for assignment. The MCV is housed at Fire Headquarters where it can be serviced by the fleet mechanics and the inventory can be maintained by

⁶¹ See Best Practice #2 – Interoperability Change Management Practices

qualified COMTs. It contains portable repeater kits, portable radio caches, extra radio batteries, radio programming equipment/software, and has the built-in ability to accommodate two radio operators to operate independent of the County Fire Communications Center. Proactively, a common radio interoperability communications plan for all staged or deployable equipment within this region is also pre-programmed into each piece of equipment to facilitate rapid deployment and use. The COML is aware that the MCV is equipped with a generator and submits a request for additional fuel to the Logistics section.

As the MCV is activated, Communications Center personnel place it unavailable in the Regional Shared Resource database so no other agency will request it. They also establish a Request Number in the Federal Resource Order and Status System (ROSS) to assure proper tracking for cost-sharing purposes.

The COML determines the best location at the Incident Command Post (ICP) for the MCV, relays that to the COMT, and begins to identify sites suitable for portable repeaters. The portable repeaters carried in the MCV will be used to extend the current command channel coverage footprint. The MCV will be used to handle Incident Communications, relieving the Fire Communications Center of Incident radio traffic.

The COML orders three qualified Radio Operators (RADO) and two additional COMTs to support the needs of the Incident and drafts an initial ICS-205 based on the regional communications plan used in pre-programming the communication resource being used or provided.

Migration Path

Developing a complete and usable deployment plan begins with a robust planning process involving collaborative efforts and input from all public safety stakeholders in the region, regardless of service discipline. The plan should include provisions for policy, procedure, common resource typing and documentation, and a tracking process, all of which should all be codified under an approved MOU.

Often, agencies will have a Tactical Interoperable Communications Plan (TICP) in place. TICPs are designed to document a state/territory, tribe, region, county, or urban area's interoperable communications assets, and usage policies and procedures. First responders can use a TICP to clearly define the breadth and scope of interoperable assets available in the area, how these assets are shared and their usage prioritized, and the steps individual agencies should follow to request, activate, use, and deactivate each asset. If a TICP is in place, it should be reviewed to confirm comprehensiveness and accuracy. If an agency is not part of an approved TICP, they should review existing plans from other locations for guidance in developing their own.

Development: The development of a deployment plan for interoperability resources should include representatives from all stakeholders in the area regardless of service discipline, and including tribal, and any non-government, volunteer or private party entities if affected by the plan. Suggested participants include but are not limited to:

- Fire, law enforcement, and EMS communications personnel
- Fire, law enforcement, and EMS operational incident management personnel
- Communications Unit Leaders
- Technical personnel including radio, data, telco, etc. as needed

The agenda for this meeting should include plans to discuss and document the area's existing plans, MOUs, technology assets, and policies relating to interoperable communications for incidents ranging from day-to-day operations to large-scale incidents, and to develop a common plan⁶² throughout the region. Additional topics include the need to identify any areas where the current resources are insufficient to meet the needs of the stakeholders involved and create recommendations for improvement over time. The discussion should include a review of the activation time necessary for each resource.

Prior to the meeting, individual agencies should identify any interoperable resources for which they are responsible to expedite the planning process.

Policy and procedure: Policy that governs regional mutual aid communications plans should be familiar, consistent, clearly defined, and include instruction on standard operating procedures. The final document should cover roles and responsibilities, asset management, long-term goals, and address prioritization of requests. The plan must also include instruction on how and when to request resources dependent upon incident needs and time needed for complete deployment including set up and support. It should also define an inventory process which provides for a regional control point and resource availability information which is accessible to all authorized stakeholders.

One potential method for building this roadmap is the creation of a regional strategy that aligns with the State's SCIP and National Emergency Communications Plan.⁶³ A number of excellent templates exist to help in developing governance and procedure policy for interoperable communications including the Regional Interoperability Communications Plan (RICP)⁶⁴ guidance

⁶² Regional Interoperability Communications Plan, DHS OEC - https://www.dhs.gov/sites/default/files/publications/OEC_RICP_Guidance%20Final%2009%202011_0.pdf

⁶³ National Emergency Communications Plan - https://www.dhs.gov/sites/default/files/publications/2014%20National%20Emergency%20Communications%20Plan_October%2029%202014.pdf

⁶⁴ Regional Intrastate Governance Guide for Interoperable Emergency Communications Efforts - https://www.dhs.gov/sites/default/files/publications/OEC_RICP_Guidance%20Final%2009%202011_0.pdf

document published by DHS. Conforming to the RICP format is reflective of the bottom-up philosophy which emphasizes that statewide requirements should be driven by stakeholders at the local and regional levels and has the potential to improve grant funding and the application process.

Common resource typing and documentation: The use of common naming for equipment types is important to ensure that requests are effectively managed and the requesting agency receives the intended resources. Resource typing is the categorization and description of resources that are commonly exchanged in disasters via mutual aid, by capacity and/or capability. During an incident, this allows the incident commander to efficiently and effectively order the appropriate assets.⁶⁵ Resource typing should be done on a regional level, using FEMA resource typing definitions. Information on deployable interoperable resources should include, but not be limited to the following:

- What is available – type and quantity
- What are the capabilities
- Is additional support needed
- How long to deploy
 - Estimated time to process request
 - Estimated time to respond
 - Estimated time to set up
 - Estimated time for support personnel to arrive
- What is the resource lifetime
- Location requirements – power, size, etc.
- Are there any associated costs involved

Availability: A complete policy needs to include a process for determining availability of any particular resource at the time it is needed. At a minimum, there should be one identified entity, or resource ordering point, that has responsibility for maintaining this status for all resources within the plan. While any plan should require a single control point, with current technology and resources the ability to make accurate and updated resource capability, location, and readiness information available to other authorized stakeholders should be an option. A shared secure website or the use of a smart phone app accessible to incident command, COMLs, and communications centers are two of many options and stakeholders should identify which best meets their needs. In addition to a regularly updated Tactical

⁶⁵ Typed Resource Definitions, FEMA - https://www.fema.gov/pdf/emergency/nims/508-8_search_and_rescue_resources.pdf

Interoperable Communications Plan (TICP), some agencies compile and distribute a daily list of available communications resources.

Review Process: Once developed and approved, the plan should be distributed to all stakeholder agencies ensuring that communications users are knowledgeable about the plan and trained to implement its components immediately. This increases the area's ability to maintain appropriate and effective interoperable communications during any event or incident. These documents should be scheduled for an annual review to confirm information and ensure accuracy.

Related Documents

The following list points to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the [Best Practice Working Group page](#) on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.⁶⁶

[Oklahoma State Communications Resources website:](#)

https://www.ok.gov/homeland/Interoperable_Communications/Statewide_Communications_Resources/index.html

[Alaska Division of Homeland Security and Emergency Management Resource Catalog:](#)

<https://www.ready.alaska.gov/SEOC/Documents/DHSEM%20Resource%20Catalog%20minus%20DHSS.pdf>

alaskalandmobileradio.org/pdf/DHS%20OEC%20ECF%20Volume%2018.pdf

[National Interagency Fire Center Website: https://www.nifc.gov/NIICD/hotsheet/hotsheet.html](https://www.nifc.gov/NIICD/hotsheet/hotsheet.html)

Date Approved

December 6, 2017

Acknowledgements

⁶⁶ Select Interoperability Committee -> Best Practices -> Shared Documents

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

7.10 Best Practice #10 - Communications Span of Control

Best Practice #10: Communications Span of Control

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the Radio Interoperability Best Practices Report companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

There should be one and only one talk path utilized for communications between first responders and the immediate supervisor managing their function during activity involving environments considered to be Immediately Dangerous to Life and Health (IDLH), or during critical tactical law enforcement activities.

Scope of this Best Practice

This Best Practice is not limited to only Interoperability resources but is applicable to all operational communications. It is intended to address:

- The unique communication between those in IDLH environments and the person responsible for the direct communication required by OSHA law.⁶⁷
- The unique communication requirements during operationally intense circumstances such as tactical law enforcement operations or helicopter hoist operations.
- The recommended span of control for supervisors/dispatchers who must balance multiple channels.

Statement of Importance

There are many talk paths deployed during complex incidents. Command, Tactical, Logistics, Air-to-ground, and other channels are typically monitored at the Command Post and/or Communications Center and, when combined, can present an auditory array that may overwhelm responders and dispatchers. Limiting communications to only the channels pertinent to their assignment increases responder safety. Listening to several conversations simultaneously exposes the listener to competing audio that can easily bury important terms. Transmissions such as “Suspect does have a gun” and “Suspect does not have a gun” risk

⁶⁷ <https://www.osha.gov/SLTC/etools/ics/safety.html#Standards>

missing the key word because the word “gun” grabs their attention after key information is provided. Also, critical time-sensitive messages can be blocked by the priority scanned channel or lost while the listener concentrates on another conversation.

When supervisors are required to monitor more than one channel, it is a best practice to avoid scanning and utilize multiple radios. Additionally, it is best to separate the radio speakers away from front-center as much as practical.

Supporting Elements

Responders focused on critical life-threatening tasks should not be expected to listen to multiple channels in order to receive and provide information necessary to safely complete their assignments.

Under Incident Command, supervisory positions from the Division/Group Supervisor level and above are often responsible for monitoring more than one channel. Some agencies advocate scanning the channels as the method to accomplish this. When scanning, the radio is not “listening” to the other channels when the priority channel is active. The responder is not truly monitoring all the channels and risks missing an important message. Additional monitoring is lost when the radio and/or system is set to provide “hang time” in order to allow follow up communication on the active channel.

Responders need to train how to transmit on the scanned channel. Though some radios can be set to transmit on the scanned channel, responders would have to have a complete understanding of the process and the time limits required to accomplish such an action. The automation of this talk-back feature introduces a complexity rarely understood by most users. Additionally, humans have a long history of being challenged in managing automation in high stress environments.⁶⁸

The use of scanning has created enough operational concern that the National Fire Protection Association (NFPA) adopted the following excerpt in NFPA 1221.⁶⁹

A.9.3.4.1.5. While it is possible to find units that will scan both trunked talkgroups and conventional channels simultaneously, there are operational issues that must be understood in such operations. Any time a mobile or portable unit scans off its home trunked talkgroup to other conventional channels or other trunking talkgroups, the radio runs the risk of missing some or all of new transmissions on the home talkgroup during the time that the radio is off the

⁶⁸ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4221095/>

⁶⁹ <http://weblink.roanokecountyva.gov/WebLinkPurchPublic/0/doc/119517/Page21.aspx>

home trunked talkgroup. For that reason, if user radios cannot afford to miss transmissions on the home trunked talkgroup, either scanning should not be used or a separate radio should be provided to allow one radio to scan and the other radio to remain on the home trunked talkgroup.”⁷⁰

Whether or not the radio is scanning talkgroups or conventional frequencies, the fact remains that if a responder is responsible for monitoring a channel, for incident transmissions or to communicate with dispatch, the responder should never be off that channel.

This also applies to a busy communications center where telecommunicators deal with primary assigned agency channels with the potential of monitoring regional and national interoperability channel responsibilities. This is especially applicable during the early phases of a large incident when additional channels such as command, Tactical, Medical Communications, and Hazardous Material Entry Team have been assigned prior to additional communications support arriving on the scene to assume the necessary roles.

When a command post is established and there are multiple channels to monitor, studies⁷¹ have shown that the target voice (the one you should hear) is “masked” by competing audio that is similar in tone, cadence (urgency), and source location (speaker placement).⁷² The one solution that is workable for a command post is to separate the radios or speakers to a left-center-right configuration..

Though Incident Command principles speak to an ideal span of control being three to seven resources, studies have shown a sharp drop off in targeted perception as simultaneous voices reach three. Depending on the volume of traffic, when an incident requires four channels, Incident Commanders should consider command post assistance in order to monitor all the channels. *Example of channel overload (R.)*



However, there are a number of variables which further impact the decision to consider command post assistance. Studies on the brain’s ability to process auditory input show that there is no single

⁷⁰ NFPA 1221

⁷¹ <https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4469089/>

⁷² <https://www.ncbi.nlm.nih.gov/pubmed/22594135>

answer to the question of how many is too much. It is impossible to actually listen to multiple voices at once as the brain does not multitask, but instead rapidly moves from one task to another. Some recent studies indicate the ability to listen and comprehend multiple voices at once is hereditary. Others show that comprehension is largely based on pitch or tone of the competing voices. In this study, a higher pitched, excited voice relaying less important information may supersede a lower, steadier voice with critical information to impart. Studies which center on the effect of hearing loss show a marked decline in the ability to monitor multiple auditory stimuli in the event the listener has any degree of hearing loss or in a loud environment such as is common on the scene of an emergency incident. As the exposure to noises of 115 decibels (dB) or greater for more than 15 minutes per day can cause long-term hearing loss, examples of which include air horns and emergency sirens, this may be a contributing factor.

It has, however, been shown that it is possible to improve cognitive listening skills through training and experience. Agencies should include listening skills modules in their training program⁷³ to increase proficiency, aid individuals in determining their own abilities, and direct agency policy concerning the communications span of control.

SAFECOM Continuum

This Best Practice touches the Standard Operation Procedures, Frequency of Use, and Training and Exercises lanes of the continuum. The span of control needs to become adopted as procedural, trained on and practiced, and used often.

Incident Use Case Examples

Use Case #1. A hazardous material (HazMat) incident is occurring in the City of Quincy. The West End Hazardous Materials Squad is a composite of HazMat Technicians and Specialists from multiple agencies assembled to bring HazMat entry capability to each of the small cities on the west end of the county.

The incident involves a liquid that continues to leak and has exposed 25 people who need to be triaged, treated, and possibly transported. The Incident Commander has requested an entry channel for the HazMat team in addition to the Command, Tactical, and MedCom channels already allocated.

⁷³ See Best Practice #3 - Training and Proficiency in the Management and Usage of Interoperability Equipment and Systems

The entry channel is selected in the radios of the HazMat Entrants, stand-by Entrants, Entry Attendant, and Assistant Safety Officer and locked to avoid an accidental change of channel.⁷⁴ The radios are also set to SCAN OFF. This ensures that each of the key members is communicating on the dedicated channel and not distracted by the other channels active on the incident. The Entry Group Supervisor has two radios. One radio is selected to the entry channel and locked. The other radio is locked on the Command channel to assure incident objectives are monitored and situational awareness is maintained. The Entry Group Supervisor is able to keep track of each conversation by separating the speaker microphones to a left/right position.

Use Case #2. Abbott County Fire department is battling a brush fire at the border with Costello County. The Command Post is established in the regional park near the incident. The command vehicles from both agencies are collocated and positioned so that the backs of each vehicle establish a common work area. The incident has been allocated the following channels:

- Command – AcoFD C-12
- Tactical – VFIRE 22 (Left flank)
- Tactical – VTAC 11 (Right Flank)
- Crew/Dozer – AcoFD T-6
- Air-Ground – AcoFD A/G

With five channels in use, the Incident Commander assigns personnel to staff the radios at the command post. Each channel is selected on mobile or portable radios and arrayed to provide audio separation. None of the radios are set to scan so that each channel can be immediately heard by the assigned personnel. This allows the Incident Commander to focus on the strategic planning and tactical deployment decisions during initial attack.

Migration Path

Agencies should recognize the potential impact of scanning and include relevant training in the agency training program. This training module should teach personnel to operate in environments commensurate with the conditions responders might find themselves.

An example would be to start with simulations of simple events in which responders are given an additional talkpath to monitor. The complexity of the simulation is then increased with progressively more urgent messages being sent. The responders should attempt these simulations using both one radio while scanning and multiple radios with simultaneous audio occurring. This gives the responder an idea of their personal limitations of tracking multiple

⁷⁴ If the feature is available in the user device, programmable keys, safety feature (FD)

conversations while under stress and of the risk of missing important information while scanning.

Whether using virtual incident technology or the equipment carried daily, simulations should start at an entry level and gradually increase in complexity to allow progressive learning. By using the radios carried daily, responders become more proficient in their use.

Though most best practices recommend that policy be established prior to training, in this case the training may also lead to the creation of agency policy as it demonstrates and documents the limitations of dichotic listening and the associated risk management concerns. The limitation of scanning and the separation of voice when multiple channels are monitored should be adopted within agencies and encouraged throughout mutual aid partners.

Related Documents

The following links point to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practice Working Group page on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.⁷⁵

<https://www.osha.gov/SLTC/etools/ics/safety.html#Standards>

Divided Listening in Noise in a Mock-up of a Military Command Post -

http://npstc.org/download.jsp?tableId=37&column=217&id=3937&file=Military_Audio_Test_1_20324.pdf

Humans and Automation: Use, Misuse, Disuse, Abuse -

http://npstc.org/download.jsp?tableId=37&column=217&id=3938&file=Parasuraman_Humans_Automation_199706.pdf

<https://www.nih.gov/news-events/nih-research-matters/ability-listen-two-things-once-largely-inherited>

<http://american-hearing.org/disorders/noise-induced-hearing-loss/#whatis>

Date Approved

December 6, 2017

Contributors List

⁷⁵ Select Interoperability Committee -> Best Practices -> Shared Documents

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document

7.11 Best Practice #11 - Managing Encryption for Interoperability Resources

Best Practice #11 - Managing Encryption for Interoperability Resources

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the Radio Interoperability Best Practices Report companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

The use of voice encryption on designated interoperability and mutual aid channels can create obstacles to interoperability and is highly discouraged. In the event encryption is deemed necessary due to unique operational needs, it must follow existing FCC regulations and comply with an approved regional communications plan.

Scope of this Best Practice

For the purposes of this Best Practice, “interoperability Resources” is not limited to the FCC-designated public safety interoperability channels, but includes any channel intended to be shared in the context of multi-agency or multi-jurisdictional responses.

This Best Practice does not intend to instruct an agency how to manage encryption, nor provide a technical description of how it works. The Related Documents section of this Best Practice contains links to several of the numerous publications available for referencing encryption technologies and management.

Statement of Importance

Interoperable communications are critical to the success of any response when multiple jurisdictions or disciplines are involved. There are standards for the public safety interoperability channels⁷⁶ that include channel naming and CTCSS tones and NAC settings. Adding encryption to interoperability channels can create additional challenges and confusion. There are reported cases in After Action Reports where encryption was a factor in the inability to communicate.

⁷⁶ APCO/NPSTC 1.104.2-2017 Standard Channel Nomenclature for Public Safety Interoperability Channels - http://www.npstc.org/download.jsp?tableId=37&column=217&id=17&file=CommonChannelNamingDocument_11042_2017_180221.pdf

The decision to use encrypted interoperable communications must be made with the understanding that encryption can add a significant level of complexity and should be considered only when the operational requirements of the incident outweigh the additional complications.

There are various encryption technologies in Land Mobile Radio (LMR). AES 256 is the current standard for all Federal LMR devices and is recommended as the standards based, highly secure, encryption protocol. The Department of Homeland Security also issued rules in March 2017 that requires Project 25 (P25) radio equipment, which incorporates encryption, to include AES 256. If other non-standard encryption protocols are being used by interoperable agencies, the resultant barrier to communications must be addressed.

Access to the keys is an important element in encryption management. The Federal Partnership for Interoperable Communications (FPIC) Security Working Group has recommended all agencies that employ DES-OFB or AES encryption utilize keys generated by the National Law Enforcement Communications Center (NLECC) and the adoption of the SLN Database for national use. In addition, FPIC also recommends that a common Key ID database be developed and utilized to minimize the possibility of duplication of these keys.

Supporting Elements

The use of encryption has increased as technologies for monitoring public safety become more accessible. The options include scanners both digital and trunked, web based scanner services and smart phone apps and the use of those options can be detrimental to operations. Law enforcement needs secure communications and what was initially limited to SRT and SWAT operations have become options for daily use.⁷⁷ Fire and EMS agencies are also becoming interested in encryption as a means of protecting patient privacy and sensitive information in emergency incidents.

Encryption on some of the nationwide interoperability channels is governed by regulation. In 2016, the FCC issued Report and Order, PS Docket No. 13-209⁷⁸ and Report and Order, PS Docket No. 15-199 revising Section 90.20(l).⁷⁹ In the first, the FCC confirmed that analog FM is required for interoperability and modified its rules to require the use of analog FM as the common modulation scheme for mobiles and portables operating on the designated public safety nationwide interoperability channels in the VHF, UHF, and 800 MHz bands. The FCC

⁷⁷ https://wiki.radioreference.com/index.php/Encrypted_Agencies

⁷⁸ Analog Voice Operations

⁷⁹ Railroad Police Eligibility

decision is specific to the designated nationwide public safety interoperability Calling and Tactical channels. This FCC order does not mention encryption; however, the mandate for analog operations prevents the use of digital encryption. As the 700 MHz band is digital only, it was not addressed in this order.

The second Report and Order issued later that year authorizes railroad police departments to access nationwide interoperability channels. This order included an appendix of those channels and prohibits encryption on the nationwide interoperability calling channels in the VHF, UHF, 800 MHz and 700MHz bands. However, it does not supersede the requirement for analog FM modulation noted above on the calling and tactical VHF, UHF and 800 MHz band nationwide interoperability channels.

As a combined result of these two releases :

- Encryption may not be used on the nationwide interoperability calling channels in the VHF, UHF, 800 MHz, and 700 MHz bands.
 - VCALL10
 - UCALL40
 - 8CALL90
 - 7CALL50, 7CALL70
- Encryption may not be used on designated tactical channels in VHF, UHF and 800.
 - VTAC (VTAC11-14) & (VTAC33-38)
 - UTAC (UTAC41-43)
 - 8TAC (8TAC91-94)

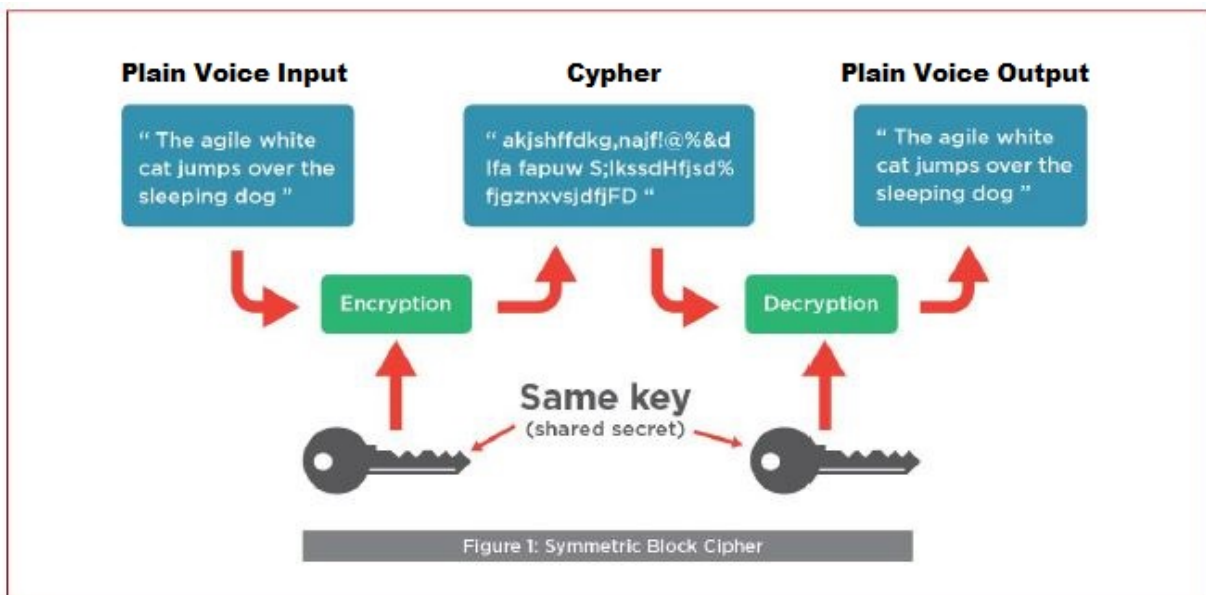
The FCC Orders do not apply to certain channels, where encryption is not prohibited by regulations such as :

- Mutual Aid channels
 - VFIRE, VMED, VLAW
 - UHF MED frequencies –
- 700 MHz Tactical channels
 - 7LAW, 7FIRE, 7TAC, 7MED,
 - 700 MHz Air to Ground channels
- NTIA designated channels
 - IR and LE
- State, regional, and local interoperability channels and talkgroups if allowed by SIEC/Local Authority

Though the use of encryption is not prohibited on these channels, it is discouraged except when it is determined to be the only solution and requires a concerted commitment and effort to

ensure interoperability. Even with prior planning and protocols that support encryption for first responders within a region, it is important to recognize that mutual aid units from outside the region may arrive without encryption capabilities. Encryption is basically a very complex alphanumeric password referred to as a “key” This key is very difficult to hack without tremendous supercomputer capabilities. Even though the numbers of combinations are astronomical, keys must be updated periodically to avoid the possibility of key compromise.

When a voice (or text) transmission occurs, the key is used to encrypt the information so it cannot be captured in transmission. The receiving device or console has the same key that is able to decrypt the message and reassemble it exactly as before encryption. (See Figure 1)



When the operational requirements outweigh the additional complexity of encryption, such as scene security, privacy, or other life safety issues, then encryption may be necessary, where authorized by FCC rules. The decision to encrypt interoperability channels must include all agencies that would have the channels in their devices and consoles.

The decisions that need consensus include:

- Which channels will be encrypted?
- Do all agencies operate with the same encryption technologies and algorithms?
- Do all agencies have the staffing and budget to support the planned key management profile?
- Who will control the keys?
- How and how often will the keys be updated?
- When will the keys be updated and what validation protocol will be employed?

- Are there channels “in the clear” available in the event interoperability is lost?
- Agreement and notification to all impacted agencies on the timeline and transition plan for implementing encryption
- Agreement on field user and PSAP training regarding the proper use of encryption, covering both governing policy and the technology involved.

SAFECOM Continuum

Managing Encryption for Interoperability Resources touches every lane of the Continuum, which effectively demonstrates its importance in creating an interoperability solution.

Incident Use Case

The Stanford County Department of Health, Emergency Medical Services (EMS) division recently switched all paramedic-hospital contact to a P25, AES 256-bit encrypted, trunked radio system operated by the County. The decision to do so was based on incidents where celebrity residents were identified by address and patient information was at risk of public release.

The EMS Agency licenses 47 emergency medical Advanced Life Support (ALS) providers and 16 base hospitals for ALS radio contact. The providers include fire departments, private ambulance companies, Sheriff SWAT Teams, and aero-medical services. Adding to those user devices are the 16 base hospitals that interface with the field units.

The need to coordinate encryption keys was recognized early and key management was assigned to the Sheriff’s Department. The Department determines which keys will be utilized, what month the re-keying will occur, and shares the information at the monthly EMS Agency/Stakeholder meetings. The date and time of Over-the-Air Re-keying (OTAR) is shared at least 2 months prior to give each stakeholder time to plan for updating. Those agencies that do not have radios capable of OTAR are in particular need to plan ahead. The time of day is chosen to maximize stakeholder’s ability to assure OTAR is successful. This would likely be in the early morning hours and would be completed before the daily paramedic-hospital radio check.

Migration Path

Public safety agencies wishing to deploy encryption on their interoperability channels need to become educated on the regulations controlling encryption. They need to understand what other entities are likely to operate on those channels and what encryption technology they utilize. Disparate technologies must be reconciled before entering any agreement.

Agencies should understand the staffing and other budgetary elements that encryption might introduce.

Next, an agreement on encryption policy needs to be formalized between all stakeholders. They must agree to all the key management parameters, including who controls the keys, how do agencies access the keys, when are keys updated, and how are the keys updated. There should be a process for immediate troubleshooting should encryption hamper response efforts.

Responders and dispatchers need to be trained on the major points of encryption. They must know which channels are encrypted, how and when to disable encryption (if capable), and what events might cause inadvertent “in-the-clear” transmissions, such as patching.

Related Documents

FCC PS Docket 15-100 – Amendment of Part 90 of the Commission’s Rules to Enable Railroad Police Officers to Access Public Safety Interoperability and Mutual Aid Channels

https://apps.fcc.gov/edocs_public/attachmatch/FCC-16-113A1.pdf

Report on the Use of Encryption on the Interoperability Channels

[https://www.google.com/url?q=http://www.npstc.org/download.jsp%3FtableId%3D37%26column%3D217%26id%3D3854%26file%3DEncryption on Interoperability Channels FINAL 20170131.pdf&sa=U&ved=0ahUKEwiDuovTx8nWAhVKw2MKHSBKA2QQFggFMAA&client=internal-uds-cse&usg=AFQjCNH9vIXOCnitJnmINw7cHdSxG_uSVg](https://www.google.com/url?q=http://www.npstc.org/download.jsp%3FtableId%3D37%26column%3D217%26id%3D3854%26file%3DEncryption%20on%20Interoperability%20Channels%20FINAL%2020170131.pdf&sa=U&ved=0ahUKEwiDuovTx8nWAhVKw2MKHSBKA2QQFggFMAA&client=internal-uds-cse&usg=AFQjCNH9vIXOCnitJnmINw7cHdSxG_uSVg)

Guidelines for Encryption in Land Mobile Radio Systems

https://www.dhs.gov/sites/default/files/publications/20160204_Guidelines%20for%20Encryption%20in%20Land%20Mobile%20Radio%20Systems_Final508c_0_0.pdf

Best Practices for Encryption in P25 Public Safety Land Mobile Radio Systems

https://www.dhs.gov/sites/default/files/publications/20160830%20Best%20Practices%20for%20Encryption_Final%20Draft508_0.pdf

Developing Methods to Improve Encrypted Interoperability in Public Safety Communications (Fact Sheet)

https://www.dhs.gov/sites/default/files/publications/20160830%20Fact%20Sheet%20Best%20Practices_Final%20Draft508_1.pdf

Considerations for Encryption in Public Safety Radio Systems

https://www.dhs.gov/sites/default/files/publications/20160830%20Considerations%20for%20Encryption_Final%20Draft508_0.pdf

Project 25 Compliance Assessment Program Encryption Requirements

http://www.npstc.org/download.jsp?tableId=37&column=217&id=3891&file=P25_CAP_Encryption_Requirements_March_2017.pdf

NPSTC Outreach Article, March 27, 2017 <http://www.npstc.org/article.jsp?id=1722>

LMR Encryption – Navigating Recent FCC Rule Changes (slide deck) – NPSTC Presentation at the APCO Western Regional Conference

[http://www.npstc.org/download.jsp?tableId=37&column=217&id=3910&file=APCO WR 2017 Encryption Final 20170413.pdf](http://www.npstc.org/download.jsp?tableId=37&column=217&id=3910&file=APCO_WR_2017_Encryption_Final_20170413.pdf)

Encryption on P25 CAP approved <https://www.dhs.gov/science-and-technology/news/2017/03/27/news-release-encryption-requirements-change-p25-cap-approved>

APCO/NPSTC 1.104.2-2017 Standard Channel Nomenclature for Public Safety Interoperability Channels -

http://www.npstc.org/download.jsp?tableId=37&column=217&id=17&file=CommonChannelNamingDocument_11042_2017_180221.pdf

Date Approved

January 9, 2018

Acknowledgements

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

7.12 Best Practice #12 - Radio Channel Assignment and Use Within High Risk Incident Environments

Best Practice Statement #12 - Radio Channel Assignment and Use Within High-Risk Incident Environments

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the [Radio Interoperability Best Practices Report](#)⁸⁰ companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Radio equipment used by first responders deployed into an Immediately Dangerous to Life or Health (IDLH) environment⁸¹ should be programmed with the same incident communication channels including identical use of channel name, zone⁸² and channel⁸³ location within the zone, and technical operational parameters.

Scope of this Best Practice

This Best Practice speaks to the need for devices to be programmed to an approved communications plan for interoperability channels which includes common channel names, zone, positions within that zone, and technical parameters. It will also speak to the need to confirm compliance prior to a first responder entering an IDLH environment, and to include the use of the plan in any large incident or event as well as in regular training exercises to increase familiarity.

This Best Practice does not make recommendations or promote any specific communications plan, but instead focuses on the need for stakeholders to develop both plan and policy on a local, regional, or state level.

⁸⁰http://npstc.org/download.jsp?tableId=37&column=217&id=3853&file=NPSTC_Radio_IO_Best_Practice_Overall_Report_Final.pdf

⁸¹For the purposes of this best practice, an IDLH environment is not limited to the OSHA definition, but includes all activities where the focus of the mission places responders or citizens on the scene of an incident in immediate danger.

⁸²Agencies may use different terminology such as zone, bank or fleet. For the purpose of brevity in this document the use of Zone will refer to any of those terms.

⁸³Agencies may refer to this as channel, position, frequency or slot. For the purpose of this statement it refers to the location of the channel within the device.

Statement of Importance

The provision of reliable and safe radio communications should not cause a distraction to a first responder at the scene of an incident. There are certain actions that can be taken in advance of the incident to help manage communications and interoperability. The disparity of radio device features and capabilities among first responder radios can create unintended challenges and potentially delay mission critical communications. The use of different radio programming templates and assignment of unique features within a single agency may also add to these challenges.

Interoperability risks increase during larger scale incidents involving multiple agencies. The development of a formal communication plan⁸⁴ includes identification of common interoperable channels, their specific channel names, channel locations, and zones in the radios. This assures that the interoperability channels assigned to an incident will be located in the same place and identified the same way in each first responder's radio. First responders from agencies that are not part of the agreement should have their communications equipment reviewed to verify it meets the minimum requirements of the communications plan. This should occur prior to the assignment of those first responders to incident activities if at all possible.⁸⁵

The communication center responsible for the incident should assign only those channels that are known to meet the communications plan and are available in the radio of each responding agency. When these mutual aid communications agreements are in place, there is a reasonable expectation that the channels assigned to the incident will be present in each radio and programmed according to the approved plan.

Supporting Elements

Public safety agencies rarely experience problems when using their communication devices for day-to-day emergency incidents. However, interoperability communications on a large-scale or complex emergency event involving the response of multiple agencies may have a different outcome.

⁸⁴ See Best Practice #4 – Interoperability Relationships

⁸⁵ We acknowledge this may be challenging in time sensitive situations which emphasized the need for all agencies in the region to participate in the planning process.

After Action Reports (AAR) for the Yarnell Hill Fire,⁸⁶ the D.C. Navy Yard Shooting, the Waldo Canyon Fire,⁸⁷ the Theatre Shooting⁸⁸ in Aurora,⁸⁹ and the Chimney Tops 2 Fire⁹⁰ in Gatlinburg all contain recommendations calling for improvements with interoperability communication devices, planning, and systems. Implementation of these recommendations can be difficult and should be made in a way that ensures regional acceptance and establishes a normal operating practice. Historically, these “Lessons Learned” often remain within the original agency and do not expand to the public safety community as a whole.

First responders should not be allowed to enter an IDLH type environment until their means of communications is confirmed. This is a critical step in minimizing risk to themselves and/or others. First responders would not enter a hazardous environment without required safety equipment (personal protective equipment, firearm, bullet proof vest, etc.). Radio equipment should also be considered a critical piece of safety equipment and should be required to meet appropriate specifications of the communications plan.

An agency specific Standard Operating Procedure (SOP) implementing the requirements of the regional communications plan should be developed which governs their responders in an IDLH type environment. Standardizing communication plans, radio channels, channel names, and their locations in the radio, enable an easily communicated method of selecting the interoperability resources assigned to the incident. Failing to follow the regional communications plan, using different channel locations, names, or other attributes that identify an assignable channel can create critical delays and lead to failed communications.

⁸⁶ “Radio Communications were challenging throughout the incident. Some radios were not programmed with the appropriate tone guards. Crews identified the problem, engaged in trouble shooting, and developed workarounds so they could communicate using their radios” – Yarnell Hill conclusions

⁸⁷ “A primary concern was the interoperability between the federal communication system and the county/city 800 MHz system. Not having the ability to directly communicate between agencies via radio created some issues and the ability to track the resources in this complex environment.” – Waldo Canyon

⁸⁸ “Attempting to use interoperability talk groups (channels) or scanning capability is too complicated during an emergency and may result in missing critical transmissions. Consider re-programming radios to simplify communications. Place specialized talkgroups in separate and distinct fleets and do not comingle them with standard (universal or department-wide) programming. Consider reducing the number of radio fleets (series of talkgroups) to avoid operational confusion. Use identical basic radio profiles (channel configurations).” - Aurora Recommendations

⁸⁹ “The complexity of communications hardware and software hindered communications. Too many things go on during a major emergency to remember which button to press when the choices are multiple and confusing.” – Aurora Key Findings

⁹⁰ “In addition, communication on this incident proved problematic with the interagency coordination because (Agency 1) operates on a UHF radio system and (Agency 2) operates on a VHF system. Neither (Agency 1) nor (Agency 2) fire staff have the ability to operate on the other’s radio system.” – Chimney Tops 2 Fire Review

The SOP should state that radio systems and equipment utilized must meet the communications plan and be available to all responders. Periodic review and update of the communications plan, policy, and SOP is critical to confirm the plan continues to meet the needs of all stakeholders covered by the plan. Other considerations when writing the SOP should include:

- Radio channel names should be based on ANSI standards and not abbreviated or edited for local variation.
- Communications plans should be detailed and followed as written. This includes identification of channel zone/channel position, channel name, and required programming of technical parameters.
- In an emergency, first responder radios should be interchangeable due to the common method of programming radio channels that may be assigned during an incident.
- The use of established communication plans and channel assignments should be incorporated into all agency and regional training⁹¹ and/or planned events.
- An additional component of the AAR to review the interoperability resources used during the incident and to identify recommended improvements.⁹²
- A provision for dispatch consoles to be configured with the approved channel name to be displayed in the same manner as on the first responder's radios. Communication center personnel are encouraged to regularly test these channels with responders to ensure reliable communications capabilities.

For devices with limitations to channel capacity, channel name, and/or channel position (which cannot be programmed to meet the communications plan), the following actions are recommended to meet the best practice:

- Limit assignment of those radios to users who will not be responding into an IDLH type environment.
- Provide cache radios at the staging location to replace any radios that are not compatible with the incident communications plan or the environment in which the responder will be working. These radios should be checked to verify they meet the incident communications plan, and reprogrammed or replaced as needed.
- First responders arriving with radio equipment that is not programmed to meet the communications plan should have their radios reprogrammed upon arrival or be issued a cache radio.

⁹¹ See Best Practice #3 – Training and Proficiency

⁹² See Best Practice #7 – After Action Review

- Communication plans and channel assignments cannot be changed during an incident unless the capabilities of all radio equipment in use have been reviewed and can meet the revised communications plan.

SAFECOM Continuum

This Best Practice touches all lanes of the SAFECOM Continuum, which demonstrates its importance to successful interoperability.

Incident Use Case Examples

Use Case 1. High-speed pursuits often occur in an area where three law enforcement agencies share a state and county border. This area has overlapping radio coverage from each agencies' dispatch center. Previously, all three agencies would work incidents on their own radio channels, which often resulted in poor coordination of mutual aid communications support with other agencies. To resolve this each agency agreed to identify channels B1 - B4 as channels to use during these types of incidents programmed them exactly the same into each radio, and identified which agency would support each channel in their radio dispatch center consoles.

Use Case 2. The three agencies also created a mutual aid agreement that included the designated radio channels B1 – B4 to always be programmed exactly the same in each radio, and that when a mutual incident occurred in the jurisdiction of an agency, the mutual aid responders would always be assigned to one of these channels and supported by one of the agency dispatch centers. Previously, these same channels were in each of the radios, but were programmed into different areas of each agency's radio.

Use Case 3. A large wildfire has ignited and an Incident Command base is still being established while hotshot crews are already staged and ready to deploy. As a part of the pre-deployment safety checklist for the incident, and as a standard practice to ensure that each crew member is properly equipped, the crew leader examines each of the radios used by the crew member to verify that the radios are in good working order and also are programmed to exactly meet the incident communications plan (ICS 205) for the channels that would be used by the crew member or crew leader. During the inspection, a few of the radios are found to not be programmed correctly as the channels that are assigned are not in the same zone or channel position that has been established in the incident communications plan. The crew leader contacts the COML and asks for either replacement radios or technical support to have the radios programmed properly. Once this has been completed, the crew leader completes a form stating that the crew has been confirmed to meet all equipment and safety requirements, before formally being deployed to support the incident.

Migration Path

Implementation of this Best Practice requires the involvement of all stakeholders within the mutual aid plan or agreement involved, and may be easiest to implement by agencies already in an established interoperability relationship.⁹³ Utilizing those relationships, agencies should agree upon what channels will be programmed and can be assigned for use within an IDLH type environment. Agencies that are not currently involved in a mutual aid or joint response agreement should develop one with an adjoining agency with which they have geographical or functional interaction. Generally, these types of agreements should always be in place between bordering agencies where mutual aid is likely to occur.

To avoid confusion and save time on the scene of an emergency, this plan should include identical channel names, technical parameters, and designate the responsible agency for channel use. The plan should take into consideration all of the users who may be assigned to an incident, regardless of discipline, and structured to meet the needs of a variety of incident types. Ideally agencies should also strive to develop an agreement to ensure their procurement procedures specify radios that support this communications plan.

An example might be a communications plan for a harbor area where a variety of incidents may occur. The plan may include a zone that has Marine channels, lifeguard channels, DHS agency channels, in addition to the Law/Fire/EMS channels. These channels are part of a pre-established and agreed plan that every radio will be programmed to include this zone. When an agreed upon communications plan is in place as part of an approved mutual aid, joint response or first response preplanned agreement, interoperability communications decisions can be made within the first minute of an incident, and channel assignments should include only those channels. No additional radio channels should be assigned during an incident unless it is known that all responders that are assigned to use those channels are capable of communicating on those channels.

Incident Channel Plans work best when the channel line-up is the same in each responder's radio and associated dispatch center's consoles. This will help the responder to quickly access the proper channel by simply selecting the channel position and not wasting time trying to remember (or look up) where a channel by name is located in the radio. However, during early stages of an incident, this can present a challenge if radios are not programmed identically, as there is no opportunity to reprogram them.

⁹³ See Best Practice #4 – Interoperability Relationships

Following approval of the communications plan, agencies should share all device and console programming information, system information, and communications plans with the other agencies involved. Agencies should agree that they will fully support the use of designated channels and will strive not to send resources that cannot utilize the plan unless compliant loaner devices are available at the scene. Agencies should only use the proper channel name when communicating information about the channel. When channel assignments are made to a first responder, the channel radio zone/channel position should also be included.

Training and exercises involving actual communication plans and channel assignments should be incorporated into all training and planned events. Inter-agency drills can develop relationships that build trust in the responders and the process, reveal areas of improvement, and establish confidence with the plan.

Interoperability works best when communications plans, agency SOPs and training are implemented in a standardized way. Operational practices should not require a first responder to use a reference card, application, or other external tool. While those reference aids may be useful, they can also lead to delays. Individual agency needs may require that not all radios and radio programming can be identical, but when agencies come together to support an incident every effort should be made to ensure compliance with the plan and improve first responder safety.

Reference Materials

The following list points to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practice Working Group page on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.

Yarnell Hill Fire Report - <https://dffm.az.gov/yarnell-hill-report-available>

Waldo Canyon Fire Study -

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=5&cad=rja&uact=8&ved=0ahUKEwihYS6n7rYAhUE0YMKHYSEDOoQFgg-MAQ&url=https%3A%2F%2Fwww.nist.gov%2Fdocument%2F03wui-fires-and-nfrl-updatesmay-02-2016for-web-postingpdf&usg=AOvVaw3e-BRiB-SSkMjpsnlCJ05>

Aurora Theatre Shooting After Action Report - http://www.policefoundation.org/wp-content/uploads/2016/08/Aurora-Century-16-Theater-Shooting_AAR.pdf

Chimney Tops 2 Fire Review Report -

<https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=3&cad=rja&uact=8&ved=0ahUKEwjqv4-JoLrYAhVK64MKHTcGDr4QFgg0MAI&url=https%3A%2F%2Fwww.wildfirelessons.net%2Fviewdocument%2Fchimney-tops-2-fire-review-2017&usg=AOvVaw1qZEhwfOfH3PgXVf3nTC2N>

2017 Kentucky Statewide Communication Interoperability Plan (SCIP) -

<https://kwiec.ky.gov/SiteCollectionDocuments/Approved%20Kentucky%20SCIP%20Jan%202017.pdf>

2016 Oregon Statewide Communication Interoperability Plan (SCIP) -

<http://www.oregon.gov/siec/Documents/SCIP/Final%20Oregon%20SCIP%20-%20SIEC%20Approved%20080916%20Signed.pdf>

Phoenix Regional Dispatch Interop Guide -

http://npstc.org/download.jsp?tableId=37&column=217&id=4026&file=Phoenix_Regional_Dispatch_IO_Guide_Remove_Appendix_B_170829.pdf

Date Approved

January 9, 2018

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.

7.13 Best Practice #13 - Interoperability Resources Information – Storage and Access

Best Practice #13 - Interoperability Resources Information – Storage and Access

This Best Practice is part of a larger, ongoing effort on the part of NPSTC to identify best practice recommendations for a variety of topics dealing with interoperability. Readers are encouraged to read the Radio Interoperability Best Practices Report companion document for a more detailed explanation of the history, development process, and intent of this document.

Best Practice Statement

Information on available interoperability resources and communications plans in any given area must be documented and maintained in a central location for immediate access by first responders and PSAP personnel.

Scope of this Best Practice

This Best Practice is intended to support the necessity for current information on all interoperability resources and channels in any given area to be available using a shared database or other similar technology.

This Best Practice does not address or encourage the disclosure of confidential communications information which may compromise agency operations, but does speak to the need to make known all information relevant to interoperability assets.

Statement of Importance

The FCC Nationwide Interoperability Channels were authorized as a tool for promoting interoperability and many other channels exist at the local, regional, and state level to supplement those resources. For optimal utilization of these resources, information on channel availability must be accessible at all times. This includes, but is not limited to, their geographic coverage footprint, operational status, and if they are actively monitored by a PSAP.

First responders are often deployed to assist at major incidents or national disasters without knowledge of available interoperability resources or which agency controls or monitors them. If information on communication plans and resources is not well known or quickly available, communications can be compromised. One solution may involve a database containing interoperability information that is easily accessible by authorized users and managed by the responsible agencies who keep it up-to-date at all times.

There are currently Internet accessible commercial and government operated database systems providing access to authorized public safety users. Some of these systems are not updated consistently and have a complicated authorization and access process. These restrictions keep

the database from being a useful tool in supporting interoperability during an emergency response.

Interoperability resources by definition are intended to be available to more than just the host agency and information on system configuration, where assets are located, and how to access them, should be available at any time to first responders. Concerns regarding the confidentiality of this information should be balanced against the interoperability needs of other public safety agencies. Information on these systems is widely available through the FCC and the Internet. An agency that restricts access to this information does not necessarily ensure privacy, but instead hampers interoperability.

Supporting Elements

Time is often the most perishable commodity during an incident. This applies to all areas from the initial notification and response to time spent establishing communications. First responders need to have access to information on available interoperability resources without the built in delays that come with restrictive authorizations, complex retrieval processes and incorrect information.

Often bad information is worse, and, possibly more dangerous, than no information at all. For instance, an officer responding to a call with reports of an armed suspect may approach the scene differently than if no weapons were reported. Unless all radios in the region contain an approved interoperability zone or zones, agencies responding for mutual aid may need to reference the requesting agencies communication plan to confirm the assigned channel is available in their radios. Ideally this information would be available to the responding agency through a shared database. However even in this case, if changes have been made since the initial entry and the database has not been updated, the units responding to a mutual aid incident may arrive on the scene without the ability to communicate.

One method to ensure accessibility is the creation of a common repository for this information and developing an easy retrieval method when it is needed. Policy governing this database must include a process that ensures the information is accurate. Interoperability can be compromised and response delayed if the database supporting the process is not up-to-date at the time the information is needed. Users may be reluctant to rely on the resource in a future emergency situation if they do not trust the source.

A number of regional solutions exist and are currently in use. The Los Angeles County Firefighters Association manages their process with an app that is available to all first responders in the area. Florida uses commercially available software and information in the Florida Interoperable Network (FIN) gateway to share information. Other state or national examples include Communication Assets Survey & Mapping (CASM) Tool from DHS, the Urban Area Security Initiative (UASI) Tactical Interoperable Communications Plans (TICP), and

information maintained by the Statewide Interoperability Coordinators (SWIC).⁹⁴ Even with consistent use of these processes, the information may be limited by regional or state agreements and access restrictions.

National collection programs often meet some but not all of the recommendation in this best practice. Limited participation, lack of active management, complicated authorization and access processes, and the issue of information not being updated dynamically are a few of the concerns that keep these solutions from being an effective real time tool for public safety in an emergency.

This Best Practice recognizes that a nationwide database system meeting all of these recommendations does not exist at this time, but instead, promotes the need for extended use of the systems currently available and points to the need for the development of a nationwide solution.

SAFECOM Continuum

This Best Practice touches the Governance, Standard Operating Procedures, Technology and Usage and Training lanes of the SAFECOM continuum.

Incident Use Case Examples

A strike team from the southern part of a western state is deployed to assist at the scene of a large wildfire spanning the border with their northern neighbor. The strike team consists of several engines, brush trucks, and supporting tankers. In a remote area several hours into their response, the team comes across a fully involved Volkswagen van that has started a small brush fire alongside the road. The strike team pulls a line from one of the engines and begins extinguishing the brush fire around the van. The strike team leader uses his interoperability resource application on his GPS-enabled device to identify the local interoperability channels monitored in the area. He uses that information to contact the local agency and relay a request that additional equipment with foam capability be dispatched.

Migration Path

Other Best Practices exist which describe the process of developing and gathering information on interoperable resources. Some of these include:

- BP #1 – Nationwide Interoperability Channel Naming and Usage
- BP #2 – Interoperability Change Management Practices
- BP #4 - Interoperability relationships
- BP #5 - Infrastructure management
- BP #6 - Channel assignment based on infrastructure coverage

⁹⁴ The capabilities and resources of each SWIC vary greatly from state to state based on funding and governance.

- BP #8 - Radio device management
- BP #9 - Deployment for Interoperability Resources

Stakeholders in a local, regional, or statewide agreement should meet to determine the process for gathering this information in a single source location. Examples of information that should be available for each agency in this database include:

- Systems that are in place
- Which channels are monitored in each frequency and who is the responsible agency
- How are they activated and is dispatch intervention necessary
- What channels are programmed into each agency's radios and consoles
- Footprint of reliable coverage
- If the resource can be patched, and, if so, who is responsible
- The radio template for channels and channel positions in the interoperability zone on each agencies radio
- 24-hour contact information for the agency

Shared knowledge of the radio programming allows for pre-planning on how to construct a mutual communications plan and minimizes the need for technical support.

The policy and procedures governing this location should include:

- Requirements and process for the information to be dynamically maintained
- Process for the review of information on a regular basis
- An authorization process that provides for easy retrieval but ensures the safety of the information
- Change management process that includes distribution of the information
- An activity log which displays the time and date of any changes made to the database as well as the party who was responsible for the change
- An indicator that allows the viewer to see when a resource is being utilized, and by whom, but does not remove it from the list

One of the most important decisions is to identify a location which can store the information in a shared database and allows for a means of access to the information when it is needed. A number of technologies exist including website portals and/or smart phone applications. These applications could potentially be GPS enabled and recommend channels for use based upon the location of the device when the information is accessed.

A future solution may be the development of a database that meets the requirements of this Best Practice and is available nationwide. The benefits of a nationwide database may become more apparent as agencies migrate into the LTE environment.

Reference Resources

The following list points to reference materials used in developing this Best Practice or otherwise referenced in the document. Additional supporting documents can be found on the Best Practice Working Group page on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.

CASM - <https://casmnextgen.com/>

Safecom, <https://www.dhs.gov/safecom/resources> now hosts many of the files previously stored at <http://www.publicsafetytools.info/>

HSIN Community of Interest - “[OEC Connect](#)” - has been established and hosts many of the remaining resources from the Public Safety Tools website.

Arizona AIRS SOP -

http://npstc.org/download.jsp?tableId=37&column=217&id=3928&file=Arizona_AIRS_SOP_101_92010.pdf

Date Approved

January 9, 2018

Contributors List

Numerous members of the Radio Interoperability Best Practices Working Group representing the public safety, government, academia, and industry communities contributed to the creation and review of this document.

NPSTC would in particular like to thank the participants of the writing group who were instrumental in the development of this individual Best Practice document.