National Public Safety Telecommunications Council

Radio Interoperability Best Practices

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

Interoperability infrastructure (I/O Infrastructure) should be monitored to assure its readiness, reliability, resiliency, and should provide failure notifications as well as availability status of frequencies and, if applicable, radio system 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 I/O infrastructure,[1] operational and training requirements, deployable resources, or subscriber systems.

For this Best Practice, I/O 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 I/O functionality.

Statement of Importance

[1] 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

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 I/O system.

Telecommunicators need to know which I/O infrastructure solution will work best for any given incident. This requires that they be aware when a particular I/O system is off line for maintenance or is in use by another agency. First responders need to understand the various I/O infrastructure solutions that may be available, so they may request activation of a particular asset. Technicians need to understand how various I/O infrastructure systems are interdependent to fully assess the impact of taking a system offline for maintenance.

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

Successful use of I/O 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 I/O 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 I/O 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 I/O systems.[2] The I/O 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 I/O system components, should have readily available reference documents. (e.g., NIFOG, procedure manuals, wall charts, talkgroup matrix lists, etc.). Availability of assets should be

[2] See BP #4 – Interoperability Relationships - http://npstc.org/radioInteropBP.jsp

managed in such a way that all agencies have immediate visibility into each I/O system's availability. This can be accomplished in a variety of ways, including the use of software or through the identification of a single agency or entity that functions as an I/O gatekeeper.

Control

Each public safety agency needs to know which agency is responsible for the operation and maintenance of each component of I/O 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 I/O system and activate it based on the unique needs of the incident. This process, for accessing and activating the I/O system, should be established through cooperative agreements and documented in written agency policy.

Practice/Testing

Agencies should use the I/O 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.[3]

Failures/Maintenance/Alarm

Faults and failures involving I/O 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.[4]

Changes

Any changes which impact the availability, coverage, and/or operation of an I/O 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 (e.g., the notification should extend beyond the PSAP). This includes field users, telecommunicators, command staff, and appropriate technicians.[5]

SAFECOM Continuum

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

[4] Preventative maintenance of I/O systems should be performed based on the manufacturer's recommendations. Agencies may elect to enhance this schedule depending on local needs.

[5] See BP #2 Interoperability Systems Change Management Practices - http://npstc.org/radioInteropBP.jsp

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 I/O 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 I/O 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 I/O systems.

Migration Path

Develop the Plan

Agencies with access to I/O 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 I/O resources 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, 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 I/O system failure. These tools will help assure the proper steps are taken when I/O systems are utilized or when problems occur. Training on the use of these job aids is a critical component to successful I/O utilization.

Practice and Use

Familiarity with the process to request, access, and recurrent use of the various I/O 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 I/O resource that is contrary to written agency SOPs.
- Familiarize field users with capabilities and features of the various I/O 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 page[6] on the NPSTC website at www.NPSTC.org or by joining NPSTC Committees Community on the National Interoperability Information eXchange at www.NIIX.org.[7]

NPSTC Public Safety Grade Report
Oklahoma State Emergency Operations Center Radio Network Test Log[8]

[6] http://npstc.org/radioInteropBP.jsp
[7] Select Interoperability Committee -> Best Practices -> Shared Documents
[8] http://npstc.org/download.jsp?tableId=37&column=217&id=3873&file=800_MHz_Radio_Test_Log.pdf

Tennessee Homeland Security District 5 Rollcall Script[9]
Arizona Interagency Radio System (AIRS) State Plan[10]
Interoperability Channel Roll Call Log Example[11]

Date Approved
May 23, 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 following participants of the writing group who were instrumental in the development of this individual Best Practice document –

Patti Broderick, Orange County Sheriff's Office, Florida - Retired
Chris Kindelspire, Grundy County 911, Illinois
David Eierman, Motorola Solutions
Brent Finster, University of Hawaii Department of Public Safety
John Johnson – State of Tennessee - Retired
John Lenihan – Los Angeles County Fire Department - Retired
Mark Schroeder, City of Phoenix Technology Services, Arizona
Everett Wittig, City of Bisbee Police Department, Arizona

May 23, 2017

[9] http://npstc.org/download.jsp?tableId=37&column=217&id=3874&file=Homeland_Security_District_5_Roll_Call_Procedures_Script_Appendix_C.pdf
[10] http://npstc.org/radioInteropBP.jsp -> Best Practice Reference Documents
[11] http://npstc.org/download.jsp?tableId=37&column=217&id=3875&file=Interoperability_Channel_Roll_Call_Log_Example.pdf