National Public Safety Telecommunications Council
Radio Interoperability Best 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[1] 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 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.

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

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[2]. This is simply illustrated as follows:

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.

[2] http://itsm.fwtk.org/index.htm

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 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[3].

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.

[3] Select Interoperability Committee -> Best Practices -> Shared Documents

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 – Retired
Orange County Sheriff's Office
Florida

David Byrum
Pinellas County Sheriff's Office

David Eierman
Motorola Solutions, Maryland

Brent Finster
University of Hawaii
Department of Public Safety

John Johnson – Retired
State of Tennessee

Chris Kindelspire
Grundy County 911, Illinois

John Lenihan – Retired
Los Angeles County Fire Department

Denis Marin – Retired
Orange County Sheriff's Department
California

Larry Schaefer – Retired
U.S. Capitol Police

Mark Schroeder
City of Phoenix Technology Services, Arizona

Keith Victor
Town of West Hartford, Connecticut

Everett Wittig
City of Bisbee Communications, Arizona