BEST PRACTICES GUIDE

Push to Talk Application Selection/Deployment

JANUARY 11, 2021

Introduction

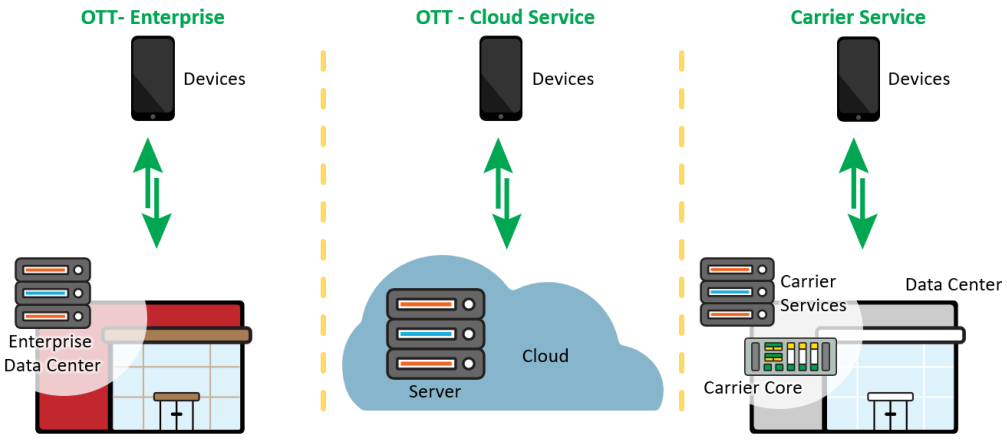
Despite a very strong statewide land mobile radio (LMR) network, there is substantial interest in push to talk (PTT) over cellular (PTToC) in Minnesota. Based on the 398 responses, representing approximately 300 agencies and departments, to the *Minnesota Wireless Broadband Data Use and Application Survey* conducted by the State in early 2020, while 8% of survey respondents reported having PTT capabilities, another 36% wanted it, resulting in a 44% net interest level. Push to talk applications are becoming more and more like LMR radio and 3rd Generation Partnership Project (3GPP) mission critical push to talk (MCPTT) standards are becoming very mature. Though PTT doesn't replace the need for LMR, it can complement the existing network by providing access to group communications across a wider area and working on commercial devices such as smartphones, which are not only cost effective but enable participation by users who may be in plain clothes or may not otherwise be assigned radios.

There are currently many PTT options, including carrier supplied, LMR infrastructure vendor solutions, cloud services, and enterprise services. This Best Practices Guide will help public safety agencies assess their options as they decide on the best app for their needs.

Throughout this document, we will refer to the *Best Practices Guide for Basic Application Selection/Deployment*, which includes best practices applicable to any application deployment or selection. We recommend reviewing that document prior to, or in conjunction with this guide for additional considerations that will help you make a well-informed decision.

Basic PTT Configurations

To frame some of the major decisions you will need to make, it is important to understand how push to talk over cellular works, and the basic varieties of service providers. Solutions that are sold directly by your cellular carrier are hosted by the carrier in their data centers. The carrier also controls the priority for the PTT traffic including the messaging and the voice data that is digitized and put into internet packets. Because of this, the carrier can allocate higher data priorities to reduce delays setting up calls and streaming voice data, and the voice content is less likely to get garbled due to congestion on the cellular network. The other class of PTT app is "over the top" (OTT). The OTT app sends data over the cellular network just like all other applications. And while your device may get higher priority than consumer traffic due to a specialized public safety service, the OTT priority level is not likely to be as high as the priority for the carrier provided application. However, a benefit of the OTT solution is that it works across carriers (e.g., if your agency-funded devices use one carrier, and volunteers or subscriber-paid devices use a different carrier). The OTT solution itself can also be purchased for operations in your own data center. The OTT vendors will generally offer a cloud solution where the service is hosted by the vendor and provided as a service as well.



While there are other differences between the various solutions on the market, these are some fundamental differences that are likely to have a major impact on your decision and your ability to communicate with users in other agencies using a different vendor. The interoperability section of this document goes into detail regarding the implications and impacts of communicating with other groups, which may be a deciding factor when considering a carrier provided versus OTT solution.

In addition to this complexity, there is a new solution that has recently hit the marketplace, called Mission Critical Push-To-Talk (MCPTT). It is based on a standard developed by the same entity that developed LTE standards. It is a global standard and is intended to provide similar functionality and experience as a Land Mobile Radio (LMR) network like ARMER. It is intended to be much faster than current PTToC solutions, with less delay to set up calls. However, PTT solutions that run over cellular networks are not full replacements for land mobile radio. LMR networks like ARMER are built "public safety grade" and are designed and operated to deliver a high grade of service especially when mother nature strikes, and public safety communications are needed most. Cellular networks are not designed this way. In addition, an LMR radio has fallback capabilities which provides direct communications between subscriber units – generally called "talkaround." While these PTToC solutions are not a replacement for LMR, they are complementary. They can provide PTT capabilities on the nationwide cellular networks, not limited to the ARMER coverage in Minnesota. They can also be operated on devices that are generally less expensive and are more discrete (such as in undercover situations).

Functional Requirements and Features

As mentioned in our basic application guide, you should engage with your end users early in your process to fully understand their functional requirements and desired solution features. At the core, most of the major vendors for PTT services support basic (one-to-one), group, and on-demand push to talk calls. They allow agencies to create multiple talkgroups, just like on your land mobile radios. The calls are encrypted over the air back to a core system for your protection. Additionally, they offer a dispatch application that operates on a personal computer, which allows dispatchers to manage communications and users. The different solutions are generally user friendly for simple navigation.

The core PTT capabilities of these applications heavily depend on the basic PTT configurations referenced above. The following table highlights the key differentiating attributes of these basic configurations.

PTT Configuration	Primary Attributes
Carrier provided MCPTT	• Very high priority level • Quicker call setup / lower latency • Large group size • Expected to include other "mission critical" features over time
Carrier provided PTT	• High priority level • Frequently includes other features such as text messaging and real-time geolocation of users
OTT	• Generally available as an enterprise application[1] or cloud service[2] • Interoperable across carriers • Frequently includes additional features such as text messaging and real-time geolocation of users

Another major difference between push to talk applications is their support of other collaboration methods. Several push-to-talk applications also offer text messaging along with push to talk. Although text messaging offerings generally include file and picture sharing in the form of attachments, some applications may not support multimedia messaging (including pictures *embedded* in texts). A few also offer real-time video streaming. As a result, it will be important to evaluate your needs and determine whether these collaboration capabilities are necessary to your organization.

Different applications also have varying core PTT functionalities that may be important to you. One important feature is likely to be an interface with your LMR users and talkgroups, which is discussed in detail in the *Interoperability and Integration* section. The following list provides some other ways that the push to talk capabilities may differ among the PTT vendors:

- **Location-Based Features:** Some applications provide a variety of location-based features. "Geofencing" means that the application can perform actions based on an area (maybe a circle/square on a map or a user-drawn area). Some applications will let you create a new talkgroup for users in that area. Others will dynamically add or remove users when they enter or leave that area. The applications that provide these features will allow a user to see the locations of other users in your agency on a map, and some will also display "breadcrumbs" on the map to show where those users have been.
- **Group size and number of groups:** Depending on the size of your organization and the size needed for your talkgroups, these factors may influence your decision. Some applications limit the number of users in a group call to 250, while others can support thousands of users in a call.

[1] An enterprise application is one where the software is installed on the agency's server in the agency's data center. In this scenario, the agency is responsible for operations of the hardware and software, upgrades, and other maintenance.

[2] A cloud service is one where the software vendor installs and hosts the service on cloud servers and is responsible for ongoing upgrades and maintenance.

Then, you can organize your talk groups much like you can in your radios, with zones. Applications in this category may offer six zones of 16 talk groups to organize your communications and make it easier to navigate among your agency's talkgroups.

- **Logging/Voice Recording:** If you are concerned about logging and recording calls, pay close attention and ask questions about these often-complicated features. The various solutions differ with regard to their recording capabilities. Some support recording via the same recording systems you use for 9-1-1 and land mobile radio calls, while others allow dispatchers to record calls. If you primarily intend to use the PTT solution associated with your LMR talk groups, you can continue recording there as well. But if you will have standalone talkgroups that exist only over broadband, then you should understand the vendor's recording capabilities and your requirements.
- **Priority Scanning:** Much like your land mobile radio, PTToC solutions can scan a set of talkgroups. Some can also perform priority scanning such that your preferred talkgroups preempt less important talkgroups. If priority scanning is important to you, add this feature to the checklist to discuss with the vendors.
- **Late Entry:** Some of the solutions also support late entry into calls, while others will only allow users to participate when the call begins. If late entry is a critical requirement for your users, check which vendors support this capability.
- **Latency/Delay:** A variety of factors can contribute to latency or delay of both the time to set up a call, and the delay in the streaming of the voice content of a call. Initial anecdotal reports suggest that the MCPTT solutions set up calls very quickly. This could be due to a streamlined process or that the MCPTT traffic on an LTE network gets a much higher priority than other PTT solutions over the same carrier network. In addition, agencies have reported substantial delays, up to a few seconds, between the LMR audio and the PTToC audio when connected to land mobile radio networks. Agencies should test solutions in different operating scenarios and locations to ensure that the call setup and audio delays are acceptable.
- **Audio Quality/Volume:** The various solutions will often use different voice coders (called codecs) that will produce different audio quality. Agencies should conduct their own voice quality tests to identify any issues. Voice quality impairments are most likely to occur when on the fringe of network coverage but can also result from congestion on the network. Agencies have reported that the audio volume levels of some solutions is low, as well. Your agency should check to ensure that the audio levels are sufficient in all operating scenarios, and that your standard-issue smartphones can generate sufficient volume to support your operations. You may determine through testing and listening to the audio on these apps, that your agency will need to change out devices in order to make full use of the PTT application.
- **Phone Call/PTT Preemption:** Some solutions are capable of prioritizing phone calls or PTT calls. For example, if your users do not want to interrupt their phone calls for a PTT call, the solution would need to allow for phone calls to be the priority. Or, if PTT calls should be the priority, you would need a PTT call to interrupt a phone call. Some solutions allow full control over the priority between phone and PTT, while others will always prioritize PTT. Make sure you understand your requirements and use case scenarios to determine which solution supports your priority needs.

- **Mission Critical standards-based:** Because MCPTT standards are new, at this time, there are not many products available. Hopefully more products and services will be offered that support the standards. For example, standards-based communications may mean an agency could purchase MCPTT service from a carrier and use client software offered by a separate vendor and still expect them to interoperate. However, for now, it is unclear if the carrier MCPTT solutions will allow third-party software. In addition, the standards also allow for interoperability between different MCPTT services. This could theoretically support carrier-to-carrier interoperability (e.g., an agency using MCPTT on carrier "A" can communicate directly with an MCPTT user on carrier "V"). However, while the standards and systems might support such interoperability, it's possible, and currently likely, that some of the carriers will not allow direct interoperability with other carrier solutions.
- **Emergency Alert:** MCPTT services are expected to support Emergency Alerts, where a user of either an LMR radio or MCPTT enabled cellular device activates an Emergency Alert indicating that the user of the device has an emergency condition. Determine if your PTToC user requirements include the capability to either initiate an Emergency Alert or receive Emergency Alert notifications from other users and if the PTT application under consideration supports this feature.

In summary, when it comes to Functionality and Features for PTT applications, it is important to have clearly defined requirements. What are your must-have core features, what are secondary and how are they ranked? Work with your stakeholders and end users and discuss different scenarios about how and where PTT will be used in your organization. The vendor features for PTT often depend on how their systems are configured and connected. You should understand and ask questions about specific features, and how PTT can be integrated with your other emergency communication systems and applications.

Interoperability and Integration

The results from the *Minnesota Wireless Broadband Data Use and Application Survey* indicate that the most widely used PTT vendors are AT&T (36%), Verizon (24%), and Motorola (20%). Interoperability between and among the different solutions is complex. At the core, there are very few vendor pairs whose solutions are directly interoperable.[3] You can achieve interoperability between disparate vendors by connecting both to the same land mobile radio network (e.g., ARMER) and using the same talkgroups. But if your PTToC solution is intended to be standalone and not interface with ARMER, then interoperability may be a challenge.

It is critically important for you to understand your interoperability requirements. If you need to interoperate with other agencies on PTToC, find out what systems your neighbors (or other agencies you interact with) are using. Then, you will need to explore what is required in order to interoperate with them. Is only one talkgroup between your agencies needed, or dozens? Are those talkgroups

[3] Some vendors use the same basic software platform and are interoperable only because it is the same platform. Only one true inter-vendor interoperable solution is known by the committee, and that is between ESChat and Mutualink.

operating on ARMER or a land mobile radio system? If not, you may need direct interoperability for the PTToC systems.

If you do conclude that you need direct PTToC interoperability (i.e., not going through a Land Mobile Radio network to communicate), you should begin collaborating within your region to select vendors that will allow interoperability.

- Are your interoperability partners on the same carrier? If so, you could potentially select a solution provided by that carrier.
- Are you on different carriers or want to have the flexibility to be able to change carriers? If so, you could explore "cross licensing" approaches from a carrier, or you can explore the various OTT solutions.

Once you have identified your requirements and understand the existing vendors for your mutual aid partners, you should start a dialog with the vendors to understand how they propose to achieve interoperability given your specific needs. It is very likely that they will not have a good solution and you will need to make critical tradeoffs. You may need to balance interoperability needs with functionality.

Another key element of interoperability and integration is with regards to the interface with your land mobile radio system. There are two basic forms of interfacing the PTToC solution to the LMR network: Radio over IP and a direct IP interface. Radio over IP (RoIP) solutions are essentially a hardware gateway that amounts to a public safety radio and PTToC client that are "back to back." These solutions only support one talkgroup at a time. Some of them may allow remote control of the public safety radio to change the talkgroup, but most generally use a standard radio that is configured to operate on a single talkgroup and requires a manual change of that talkgroup. This means that for each LMR talkgroup you want to interface with, you must have an additional piece of hardware to allow for simultaneous communication on all talkgroups. And, the hardware must be in good coverage of your LMR system and possibly the cellular network(s) supporting the PTToC solution as well, depending on the specific PTToC solution and how it is deployed.[4] A direct IP interface to the LMR network allows for many talkgroups at the same time. The IP interface also supports passing radio IDs (i.e., a PTToC user's ID would be displayed on a land mobile radio device and vice versa), emergency alerts, and other features that are not possible with a Radio over IP solution.

Most agencies in Minnesota operate on ARMER, a standards-based Project 25 system. At the time of the development of this guide, the Land Mobile Radio Committee of the Statewide Emergency Communications Board is currently developing its standards for interfacing with ARMER. The Committee will have specific requirements and standards for interfacing with ARMER that must be followed. As a Project 25 system, ARMER can theoretically support direct interfaces with other systems via the Inter Sub-System Interface (ISSI) or Console Subsystem Interface (CSSI). These types of interfaces can support any configured talkgroup between the PTToC and LMR systems, support multiple simultaneous talkgroup communications, and can pass data between the systems like radio ID.

[4] The RoIP gateway will also need to be connected to the supporting cellular network(s) through an internet connection or be in good wireless coverage of that network for a wireless connection.

However, at the time of developing this guide, the Committee's work is not yet finalized, and it is possible that direct IP based interfaces may be prohibited. Agencies are encouraged to visit the Committee's website and consult with Committee members or ECN to understand the current allowable interfaces with ARMER.[5]

The PTT solutions may also differ in their ability to integrate with other applications. For example, if you require your PTT solution to be launched by your situational awareness application, there is at least one product that can do this. In that example, you can start a PTT call from the application while in the situational awareness interface. Likewise, if there are other applications you need to make calls from, some PTT software vendors may support Application Program Interfaces (API) that allow such interactions. If you have specific needs to integrate with other applications, including the ability to allow single sign on, make sure you address these concerns up front with the vendors to determine if that will affect your decision.

Security

Many important security elements, such as transport/data/service protection, authentication and confidentiality, have been discussed in the *Best Practices Guide for Basic Application Selection/Deployment*. Those are relevant to all apps, but there are PTT-specific elements to consider as well.

First, there may be specific security related requirements associated with connecting to your land mobile radio system. As discussed above, the Land Mobile Radio Committee's standards for such connections are under development; however, they will likely include specific security requirements to ensure ARMER is protected.

LMR system are generally a closed operating system. Allowing connection to systems with cellular devices could expose the combined system to malicious applications or malware that could monitor, record, or intercept non-encrypted audio from the PTT application. Therefore, some form of device anti-malware and application auditing is required.

One aspect of PTT security is encryption of sensitive voice communication. While the wireless broadband networks are encrypted over the air, it is a best practice to have them encrypted beyond the wireless element of the network, and all the way back to a protected data center. Or, better yet, end-to-end encryption of audio (from one device all the way to all other devices receiving the communication) would be ideal, along with the ability to change encryption keys and perform encryption key management. It should be noted that no known PTT solutions will encrypt traffic end-to-end with a radio network. In the case of RoIP, the voice content is decrypted and re-encrypted each time. And in the case of the ISSI/CSSI based solutions, while it is feasible that the data could pass through the interface without decryption, because most if not all P25 and PTToC use different voice coders, encryption would need to be broken anyway to perform audio transcoding.

[5] See https://dps.mn.gov/entity/secb/committees/Pages/land-mobile-radio.aspx for more information or contact ECN (https://dps.mn.gov/divisions/ecn/contact/Pages/default.aspx) to get an update on the Committee's final standards.

Due to the nature of PTT, PTT apps do not require login each time the application is used. Instead, users initially log in, and the application is available to the user as long as device operation is available (usually via a PIN after it times out). For that reason, it is important to have policies in place to ensure the device remains locked and is not easily unlocked. And, if a device is lost or compromised, it is important that it can be remotely disabled which highlights the need for users to report a lost, stolen, or otherwise compromised device as soon as possible.

Deployment Factors

There are a variety of general factors to consider, including the procurement process, policies and agreements that will affect the app's use, software and/or server deployment, and staffing impacts. These are discussed in the *Best Practices Guide for Basic Application Selection/Deployment*. Additionally, there will be PTT-specific factors that influence your deployment. The following paragraphs highlight unique PTT deployment factors. You should develop a detailed plan and checklist for how you will acquire, implement, and transition operations on to the new platform.

Your deployment plan should start with identifying your user agencies and understanding your objectives for use of PTToC. Some agencies find that in certain circumstances land mobile radios are not necessary, and the cost of radios are prohibitive. For example, hospitals that need to monitor communication with EMS units may prefer a simple smartphone instead of a portable radio or a consolette. In other situations, indoor coverage may be limited on your radio network, and you can leverage cellular or wi-fi coverage to provide PTT capabilities. Your plan should identify these user groups and take advantage of the benefits of PTToC. If your plan involves allowing employee-owned devices to be used for the PTT service, you may need a specific plan to address their needs, including, for example, whether the application be completely shut down so that users are not tracked when off.

The biggest impact with regards to deployment will be whether or not your software vendor or carrier will host the application. In that case, it relieves your agency of the burden of planning to integrate the PTT solution into your data center, acquire the servers, and conduct the design, acquisition, installation, configuration, and testing of these systems.

Whether or not you will integrate the PTT solution with your LMR network is also a key deployment factor. Depending on the solution, this could trigger needing additional hardware for a RoIP solution, or it could trigger licensing and other configurations if you are employing P25 ISSI or CSSI. You may need technical support for such solutions as well if your existing staff lacks the expertise or access to make such changes. As mentioned above, ARMER standards could dictate what kind of hardware, configuration, and approvals are required in order to be consistent with State guidelines and would need to be added to your plan.

When interfacing PTToC with any radio network, including ARMER, while there can be tremendous benefits, it is important to understand the potential dangers. The interfaces could easily be misconfigured, causing very undesirable results for your radio users and others. It is highly recommended that a professional familiar with implementing radio gateways and ARMER standards should be employed to install and configure the gateway. Additionally, the increase in the number of users and usage on the interface can also have undesirable side effects that you need to consider. The

location, number of talkgroups, and number of users can all impact the resources on the host radio system and cause critical calls to go unserved. If you plan to interface with ARMER, your local System Administrator **must** be consulted to ensure proper operations.

Specialized hardware may also become a necessity part of your plan. After trialing different solutions, you may decide that you need ruggedized devices that have superior speakers (higher volume, better clarity). You may also decide that you need a device with a dedicated PTT button or a dedicated emergency button. Do some of your users need speaker/mic accessories? Your plan should investigate how your agency will use the PTT solution to better inform your decisions. It should also consider your dispatch plan. Will you need new dispatch "consoles" to manage the PTToC solution? Will you integrate the capability into existing dispatch positions, and if so, how will you manage the screen "real estate" for this new responsibility? Note that the PTT applications often have tracking and other features that centralized management may want to access, and therefore, your plan should address who needs access to these management capabilities.

Your deployment plan should address your PTToC fleet map. It should address interoperability with other agencies as well as your Land Mobile Radio system. Your plan should identify all of the talkgroups that will be configured on PTToC, the zones for those talkgroups, who will have access to the talkgroups and zones, and which mutual aid or LMR talkgroups they may be associated with. The plan should address whether certain users, or groups of users, can talk on certain talkgroups or whether they should be in "listen only" mode. Some agencies might decide that it is not worth the risk of accidental transmission on mission critical talkgroups and decide to prevent talking for many PTT devices. As with any software deployment, your plan will need to address how you will distribute the PTT software to end users, managers, and dispatchers.

Your plan will also need to consider other integrations. For example, some PTT solutions allow integration with other credentialing systems (such as your Microsoft account). Your deployment plan will need to include the development of a comprehensive user list. Work with the vendor to understand what it will take to interface your existing credentialing and access management system or if there are other interfaces that will make user management easier. It may be that implementation as a cloud service will simplify the process of user management. Additionally, an interface with your current platform could mean that your users only have to remember and manage passwords for one system that shares credentials with your PTT system, a big potential timesaver and convenience factor for both your users and administrators. For example, when an employee leaves, removing that employee from access to your Windows systems could also remove access to the PTT application. Your plan might also address other integrations such as those mentioned above with a situational awareness application.

Your plan should consider policies associated with the new capability. If you are expanding your PTT capabilities to users who are not familiar with PTT use (i.e., are not users on your LMR network), then you might consider policies associated with responsible use on the new system, especially if it is providing them access and talking rights on talkgroups that operate on your LMR system. Your policies should address their responsibilities associated with security, such as notifying administrators if their device is lost or stolen. As with any mutual aid plans, your policies and standard operating procedures should address how and when talkgroup sharing with other agencies will occur.

Finally, your deployment plan should address training. Will your users receive formal training during the roll-out? While PTT applications are often not terribly complex, they might include advanced capabilities that are not entirely intuitive. Your plan should assess the application and whether you will institute a training program, direct users to videos, leverage vendor training, or employ a training program by internal staff. In the case of internal training, you may also seek to have train-the-trainer sessions with the vendor. You will want to include dispatcher training in your program to address any new features such as location and texting via the PTT application, and also the handling of any PTToC-only talkgroups that are not simply an extension of existing LMR talkgroups. You will also want to include administrative training to address the management of users and access to the application. And, once users have been trained and the system is fully operational with all the required functionality and capabilities, you can then transition your deployment team to close out your deployment and move to operations.

Your deployment planning process should also identify one time (i.e., during the deployment phase) and operational elements for budgeting and resource identification. Your plan will need to identify the staff needed to execute on cutting over to the new capability as well as the ongoing operational staff needed to support it. The next section will discuss operational needs in more detail.

Operational Factors

The same general operational factors apply as were identified in the *Best Practices Guide for Basic Application Selection/Deployment.* Depending on whether the system is hosted by your vendor or your own agency, the level of operational obligations can change dramatically; however, your operational plan will still need to account for supporting your users, staffing levels, ongoing training, upgrades, system maintenance, maintenance of interfaces with other systems, and vendor management. The costs associated with managing and implementing your operational plan are addressed below, but it is important to make sure that your budget covers all the anticipated operational costs during the life of the new solution.

With a PTT solution, there will invariably be situations where users inadvertently hit the PTT button, emergency button, or other factors that may cause disruptions and require intervention. And, there will be lost or stolen devices that must be disabled. As discussed above, you may introduce new talkgroups that require dispatch monitoring, which may require additional dispatch resources to be allocated. Your plan might also include new hardware that must be managed such as smartphones, Bluetooth PTT buttons, speaker/mics, and even new PCs or monitors for dispatch stations. All of these elements need to be maintained and considered in your operational plan. You will need to identify if the application or service provider offers the capability to monitor and analyze usage to make sure that personnel are using the new capability appropriately and as anticipated and identify how this information is accessed. You will also need to be prepared to staff user support to handle issues from password resets, coverage issues, hardware issues, and training issues.

Users must also be aware of any potential impacts of using the PTT application, such as additional battery drain if the application is left open, or what to do if a device with the application is lost or stolen.

If you opt to host the service yourself, there are many additional responsibilities that you will need to plan for, including user access management and control, talkgroup access, application support, asset management, server maintenance, upgrades, software upgrades, data center upgrades, and others. Your plan will need to address the additional workload for data center maintenance personnel and engineers to continue providing a high availability solution. And with a self-hosted service, your personnel will be fully responsible for network security and the associated monitoring, risk mitigation, and threat response.

Your plan should address ongoing services needed by your vendor such as continued support for your interface with a land mobile radio system, training, and any other identified needs. Especially if the solution is "mission critical," you might establish a service level agreement (SLA) with your vendor to ensure a highly reliable solution.

Financial Factors

The *Best Practices Guide for Basic Application Selection/Deployment* captures the bulk of types of costs to identify and budget for in the deployment and operational phases of your new PTT capability. As a best practice, you should go into this initiative with a full understanding of the one-time startup and ongoing operational expenses associated with these new capabilities. While you may choose to capture cost savings as part of your deployment (e.g., that some user groups no longer require radios and ongoing radio cots), it is important to make sure that your capital and operating budgets will accommodate the new PTT capability. In this section we will identify specific costs associated with PTToC capabilities.

During the deployment phase, some important elements that should be part of your budget, if applicable, include:

- **User Device Hardware:** Your deployment may require new ruggedized smartphones with dedicated PTT buttons and other accessories such as speaker/mics, Bluetooth PTT buttons, hands-free kits, and others.
- **Installation/Distribution:** If you are deploying new devices or associated hardware, make sure to budget for the installation of the equipment. Especially if your deployment impacts operational units including most of your agency, you will need to budget to manage a minimal impact plan.
- **LMR Interface:** If interfacing the PTToC solution with your LMR network, you could have hardware costs for a RoIP interface or licensing costs for an ISSI/CSSI solution. The number of talkgroups you plan to use in common with LMR may impact these costs. The hardware based RoIP solution generally requires one configuration per talkgroup, while the ISSI/CSSI is licensed for a pool of talkgroup communications. And, if you go the ISSI/CSSI route, does the vendor charge for encryption or setting up a VPN connection to their system?
- **Agency Hosted:** If your agency is hosting the solution, you'll have costs associated with servers, data center impacts, as well as the associated cost designing, implementing, and configuring the solution. The agency hosted model may include upfront one-time licensing fees that need to be included in your budget.

- **Training:** If you choose a formal training program, you'll need to budget for trainers and to make sure you accommodate the downtime for operational personnel as necessary.
- **Staffing:** Include project management time, management time to create policies, plans and other upfront efforts.

On an ongoing, operational basis, there are a number of other costs that need to be factored into your annual budget. Below are some key costs to include in your operational budget for your PTToC solution:

- Per user licensing/subscription fees: The carrier and cloud hosted solutions include a per user fee; your budget will need to include this as well as any changes expected over the near future (e.g., are you adding new departments in year 2?). There may be different add-on costs, such as user tracking, whether it uses a LMR interface, or depending on other carrier services.
- Additional LTE service subscriptions fees must also be included if additional subscriptions are required to implement your solution and include all the planned users.
- Will there be other ongoing licensing costs? Does your LMR interface have ongoing subscription or licensing costs associated with it? These costs may also be based on the number of users (IDs) and/or talkgroups that must be supported by the interface.
- Will it affect costs if you need to hire staff or divert existing employees' time to operations or to provide ongoing training for your PTT system?
- Will you need to maintain spares for hardware dedicated to your PTT solution, or establish a budget for insurance costs and repairs or insurance claims and management? Note previous references regarding new rugged handsets and accessories. These items should be added to your budget too, if applicable.
- Will you need dispatch or other monitoring of new talkgroups dedicated to PTToC? While it may not trigger new employee costs, the additional load should be considered in your budget planning.
- Will you need to pay for upgrades to the system?
- Consider how you will budget for refresh of hardware and software, including anticipated life-cycle replacement cost of the user equipment. Ensure to include the technology lifecycle in your capital improvement or forecasting budgets as appropriate. It is especially important in the case where initial equipment costs are grant funded, to make sure these costs are not forgotten.

You should develop spreadsheets outlining your one time and annual costs to ensure that you have enough budget to implement the solution and then sustain it to the appropriate level of service.