Broadband Interoperability

EXECUTIVE SUMMARY

As a premier supplier of full-featured interoperability and dispatch products for public safety and first responders and as an independent company without direct ties to any manufacturer or carrier, Catalyst was awarded the United States Department of Homeland Security's (DHS) Science and Technology (S&T) Directorate's Broadband Interoperability project to develop standards-compliant interoperability solutions. Catalyst has been privileged to receive federal funding through both Phase I and Phase II DHS Small Business Innovation Research (SBIR) awards to research this area, build prototypes, and do extensive collaboration, demonstrations, and interviews with vendors and customer agencies. Throughout this project, assumptions about industry direction and industry leaders that were made when Phase I began in 2022 have needed to be adjusted and roadmaps, priorities, and partners continuously reassessed.

Acronyms useful to understand while reading this White Paper

- **LMR** – Land Mobile Radio
- **LTE** – Long Term Evolution
- **3GPP** – Third Generation Partnership Project
- **P25** – Project 25
- **IWF** – The Interworking Function
- **MCPTT** – 3GPP's Mission Critical Push to Talk
- MCVideo – 3GPP's Mission Critical Video
- MCData - 3GPP's Mission Critical Data
- MCX - 3GPP's MCPTT, MCVideo, and MCData collectively
- **PoC** – Push to Talk over Cellular
- **ISSI** – Inter Sub-System Interface
- **EPTT** – Enhanced Push to Talk
- **OTT** – Over the Top Push to Talk

The Catalyst solution has been built from the ground up as an IP-Based interoperability solution that is both fault-tolerant and scalable. Our peer-to-peer communication gateway design inherently provides interoperability that facilitates direct connections between gateway communication interfaces. Before this project began, Catalyst already had a long list of interfaces that its interoperability function (IntelliLink™ is the product name we coined in 2005) could bridge, including Third Generation Partnership Project (3GPP) Mission Critical Push-to-Talk (MCPTT) - compliant Push-to-Talk over Broadband (PTToB) systems.

Catalyst leveraged its commercial product, designed for **interworking between LMR and broadband**, and prototyped enhancements that made the solution work effectively and securely when implementing **interoperability between broadband systems**. The five tasks of the project enhanced operational elements identified in Phase I (listed in the "Project Overview" section below) as critical to meeting the more demanding requirements of broadband-to-broadband interoperability.

The project tasks prototyped the following elements, identified as crucial to broadband interoperability:

1. Manufacturer extensions to the 3GPP-compliant interface coupled with an aware prototype mobile client app that provides a near seamless broadband interoperability user experience.
2. Emergency Alert, Group Texting, and Priority Mapping interoperability across broadband systems.
3. Standards-compliant interoperability even with proprietary PTT systems by using the Project 25 (P25) Console Sub System Interface (CSSI) that is a standard option for various proprietary PTToB systems.

4. Investigation of two related technologies essential to broadband interoperability – solving encryption challenges by using transcoded encryption to provide secure connections and maintaining high voice quality available with broadband systems by using wideband voice codecs (vocoders) to preserve audio quality between broadband interoperability gateways.

The Broadband Interoperability Platform (BIOP) prototyped during this project and described in this report demonstrates that it is **technically feasible** to create highly functional interoperability between incompatible PTToB systems, whether 3GPP-compliant or proprietary. During the period of performance for this Phase II contract, Catalyst deployed elements of the BIOP. The critical next step to further reaping benefits from this Phase II research is to field deploy additional elements of this interoperability solution to further demonstrate its efficacy and to refine it operationally.

PROJECT OVERVIEW

In this report, Catalyst provides a detailed summary of its accomplishments and conclusions for the Phase II SBIR Broadband Interoperability Project. The goal of this project was to expand our working prototypes with features and enhancements identified in our Phase I research as critical for successful broadband-to-broadband interworking.

The project consisted of five tasks that prototyped and demonstrated functionality that focused on broadband-to-broadband interoperability:

1. Task 1 – Prototype 3GPP Client Interface Extensions and Interoperability Enhancements.
2. Task 2 – Prototype CSSI Client Interface to a Proprietary PTToB System.
3. Task 3 – Prototype Rapid Configuration and Next Generation Visualizations.
4. Task 4 – Prototype Secure Transcoded Encryption and Full High-Definition Vocoding.
5. Task 5 – Demonstrate New Functions, Conduct Stress and Scaling Testing.

PHASE I BACKGROUND

The goal of the Phase I research component for this SBIR was to determine the technical feasibility of building a BIOP which could provide PTT voice interoperability between broadband systems for mission critical operations. In the Phase I final report, we demonstrated this feasibility and outlined a plan to build a prototype that could be used to gain acceptance from service providers, their vendors, and the agencies that need this interoperability.

We began with a thorough analysis of public safety requirements as documented by the National Public Safety Telecommunications Council (NPSTC), supplemented by those from the DHS and our twenty-five years of experience providing Internet Protocol-based PTT dispatch and interoperability solutions.

Catalyst leveraged its experience integrating with both PTToB services and a variety of LMR systems to conduct an extensive security analysis, including evaluating the feasibility of end-to-end encryption and transcoded encryption. We concluded that while end-to-end encryption is appropriate for LMR communications, the barrier for Broadband interoperability is the

proprietary nature of the solutions that exist and no agreed upon open-source documented interfaces.

A solution to encryption issues is a major barrier to a viable broadband interoperability solution. We determined that security tools used today for banking and similar highly sensitive internet-based transactions provide cutting-edge security and allow the essential requirements for broadband interoperability to be met with ***transcoded encryption***.

In Task 3 of the Phase 1 project, Catalyst analyzed six established interfaces that PTToB services could utilize for interoperability. We found that using a standards-based client interface enables a near-term solution and is more likely to be accepted by the cellular carriers, their vendors, and other service providers than more invasive connections. Specifically, we recommend using the MCPTT **Client interface** as specified by the 3GPP for 3GPP-compliant MCPTT services such as AT&T's FirstNet® PTT and the Telecommunications Industry Association's (TIA) CSSI standard for proprietary PTToB services like L3Harris' BeOn, now known as XL Virtual.

Strategic Goals of The Phase II Broadband Interoperability Project

When Catalyst Communications began writing the proposal for Phase I of this project almost three years ago, we recognized the importance of broadband interoperability for mission critical operations, and we also understood our unique position as a vendor who has been researching and developing land mobile radio (LMR) to broadband interworking solutions for DHS since 2018. The Request for Proposal from DHS for this SBIR was the next logical evolution toward a multi-vendor, multi-technology interoperability solution.

Phase II SBIRs typically take concepts researched in Phase I to the next level by building prototypes that further prove (or disprove) the **new concepts** and conclusions from Phase I research. The new concept in this Phase II SBIR involved the **interoperating** of **many combinations** of extremely complex but existing (some evolving, but some quite mature) technological concepts, products, and markets. Catalyst was in a unique position to create the prototype BIOP as a result of our prior SBIR work connecting to MCPTT systems for our LMR to Broadband solutions.

Project Results and Takeaways

This section gives a high-level overview of each of the prototypes developed for this project.

Task 1 - Prototype 3GPP Client Interface Extensions and Interoperability Enhancements

Prototype 3GPP Client Interface Extensions

Catalyst has created a Prototype MCPTT-compliant Android app that is being used to test manufacturer extensions and to demonstrate an enhanced user experience. We began with the Mission Critical Open Platform (MCOP) development kit, the result of a collaborative project with financial assistance from the

U.S. Department of Commerce and the National Institute of Standards and Technology (NIST) through the Public Safety Innovation Acceleration Program (PSIAP). The intent was not to build a commercial mobile app, but rather a tool for demonstrating advanced abilities and novel *concepts* to carriers and vendors.

Feature Set

The Android APP User Interface has the following tabs:

1. **Users** – List of End Users on local server
2. **Groups** – List of available talkgroups
3. **Map** – Open Street Map displaying location of an End User
4. **SDS** – Displays received group/private text messages (**S**hort **D**ata **S**ervice)
5. **Interop** – List of End Users on a foreign MCPTT or LMR system

The **Users**, **Groups**, and **SDS** Tabs are typical for these PTT mobile apps and some also provide a **Map** tab. The **Interop** tab here, however, is unique to the Catalyst prototype and is discussed below.

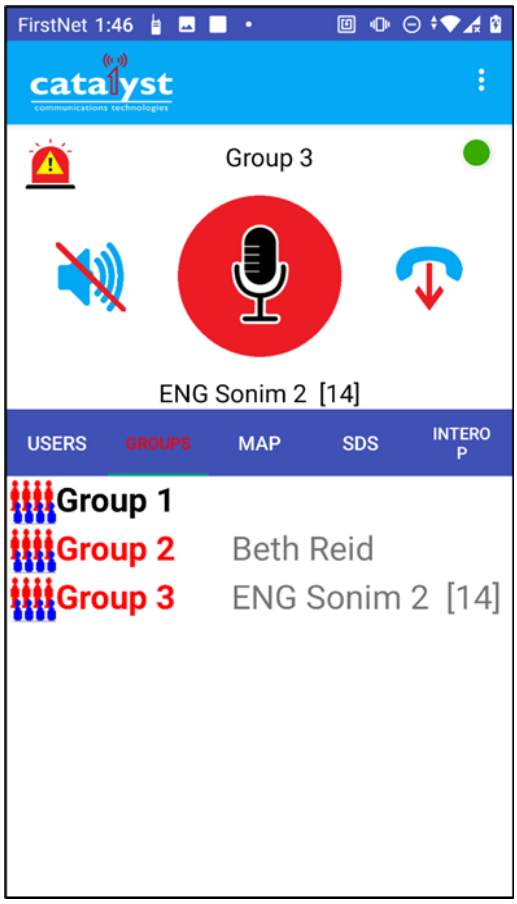

Figure 1 - Concept App: Groups Tab

Typical Use

A screen shot of the Catalyst app with the **Groups** tab in focus is shown in Figure 1. The Catalyst Concept App can manage multiple calls concurrently (typical mobile apps can only receive a single call at a time.)

Our Phase I research and marketing experience determined that the ability to display the ID of the talker on the "foreign" system is a critical capability. Because the app presents this manufacturer extension-enabled information so transparently, it is actually difficult to tell the difference between the local and external users.

The Interop Tab

The **Interop** tab contains a list of all the Talker IDs from external systems from which this mobile app user has received calls. **Error! Reference source not found.** shows that the Talker ID **ENG Sonim 2 [14]** is from an interoperability user from another system. The GPS Icon adjacent to the name indicates that we also have GPS coordinates for this external user.

After selecting a user on the **Interop** tab, both the **Map** tab and **Group** tab update in the background (the update is visible when the Map or Group Tab is selected) using the attributes of the external user. Activating the **Groups** tab shows the selected talkgroup to be the one that the external user was last heard on.
Activating the Map tab shows the location of that external user selected on the **Interop** tab.

Figure 2 - Concept App: Interop Tab

New Broadband Interoperability Features

For Task One, in parallel with the Manufacturer Extension work, Catalyst prototyped three new interoperability capabilities that our Phase I research[i] indicated were especially important for broadband interoperability. These three new capabilities, detailed in the following sections are:

1. Emergency Alert Interoperability
2. Texting Interoperability
3. Call Priority Interoperability

TASK 2 - USE P25 CSSI AS A STANDARDS-COMPLIANT INTERFACE TO PTTOB SYSTEMS

One of the sizeable hurdles for a successful BIOP, as required by the DHS solicitation, is that the platform must support interoperability not only with standards-compliant PTToB systems, but also proprietary PTToB systems. For proprietary PTToB systems, Catalyst proposed using the Project 25 CSSI interface for broadband interoperability. The rationale was to utilize an access method already supported by many proprietary PTToB vendors that provides access to PTToB talkgroups and users in the same way that radio system manufacturers provide access to their talkgroups and users.

The Catalyst approach of using the 3GPP-client interface for 3GPP systems and CSSI for non-3GPP systems implicitly reduces the barrier to connecting to these networks. By choosing already supported interfaces, each service offering provider must still grant permission and enable access to their network to any BIOP. We found this to be a real challenge, even in successfully executing Task 2.

The Standards-Based CSSI for connecting to proprietary PTToB systems

We leveraged our strong relationship with L3Harris (and are grateful for their support) to test and demonstrate with L3Harris/BeOn. Taking a standards-compliant approach enabled us to deliver a working prototype, meeting the aggressive schedule.

A key component of the P25 CSSI prototyping approach was to choose a PTToB provider whose P25 CSSI interface supports encrypted talkgroups (AES 256). As BeOn supports this functionality, we have now demonstrated it and seen it work successfully with our BeOn prototype. Another advantage to the BeOn product is that the audio is end-to-end encrypted. For some agencies, this may be a requirement, even for PTToB.

In addition to the proprietary BeOn PTToB system, as part of our Task 5 demonstration, we demonstrated a second CSSI Client Interface (without encryption) to a proprietary PTToB with Motorola/Kodiak's Enhanced PTT (EPTT) Advanced product.

TASK 3 - PROTOTYPE RAPID CONFIGURATION AND NEXT GENERATION VISUALIZATIONS

For this task, the core objectives were to provide intuitive administration and user interface tools for managing and monitoring the BIOP solution.

Talkgroup Naming Conventions

In researching and prototyping ways to leverage dynamic information on talkgroups and users that we retrieve from MCPTT-compliant system, we discovered that talk group names among public safety were commonly duplicative. We have developed a scheme for connecting different agencies, carriers and vendors by using a special naming convention for talkgroups so that dispatchers and end users were not confused. As we were researching different ways to name talkgroups, we began by analyzing the 2018 NPSTC report "Mission Critical Push-to-Talk Considerations for Interoperability Talk Group Naming and Management ."[ii]

The Catalyst Interop Format

Catalyst has invented a way to construct a display name for interoperability talkgroups such that it tells both our interop administrative tools as well as humans using the PTToB system what the talkgroup interoperates with.

1. There will be "Free Format" talkgroup names for a given agency (e.g. these are actual names from a Catalyst customer; we'll call it Springfield) that may have been in place for many years:
    a. Corey T7
    b. CL_FIRE
    c. VIPERFD
2. To automatically create interoperability with a different agency or a different carrier and be clear about which talkgroup they were working with, the administrator for the other agency or carrier would add via their MCPTT portal new talkgroups in Catalyst Interop-format; for example:
    a. Corey T7@(Springfield)
    b. VIPERFD@(Springfield)
3. The purpose of this Interop talkgroup is to be a "patched" reflection of the free format main talkgroup on the other system. Users on this system who see the new Interop talkgroup can see that they are interoperating with Corey T7 on the Springfield radio system. It also conveys which is the established, main talkgroup and which one has been created to provide interoperability.

The “Interop Format” talkgroup name method provides the following advantages:

- Administrative tools know how to build the patches automatically
- Administrators and Dispatchers instantly know they are interop talkgroups and not the main talkgroups themselves
- Administrators and Dispatchers know what they are patched to just by looking at the Interop-format talkgroup name.

TASK 4 - PROTOTYPE SECURE TRANSCODED ENCRYPTION AND FULL HIGH-DEFINITION VOCODING

For this task, there were two core capabilities that needed to be prototyped to make the BIOP solution support broadband-to-broadband interoperability:

1. Encrypt data between distributed system elements (nodes/gateways/clients) using NIST recommended techniques, policies, and best practices.
2. Upgrade the vocoders used between distributed system elements (nodes/gateways/clients) from current narrowband (radio or toll quality vocoders) to wideband ones capable of reproducing high-definition speech. This was necessary because there was no advantage to using low bit rate voice encoders common in LMR systems for broadband-to- broadband applications with plenty of bandwidth.

Distributed Encryption

Strategy Overview

Internet Protocol (IP) is a core technology that makes the internet possible by allowing computer applications, written in diverse computer languages, running on diverse operating systems and diverse computer hardware, to communicate over computer networks by exchanging standards-based messages. Because the messages adhere to very specific protocol rules, applications on either end (and network devices in-between) can easily understand and exchange information between each other. Because IP messaging is based on published, stable standards, everyone who has access to the messages can understand the messages being exchanged.

In the early days of the public Internet, with its chat room traffic, casual emails, and primitive web browsing, there wasn’t a lot of information that was considered private and sensitive. But in today’s communication systems, messages routinely contain banking information, credit card numbers, social security numbers, and other sensitive information, so that same ability that allows every participant in IP messaging to easily form and understand messages can be a perilous liability. Since any unauthorized program or device on the computer network that can access these messages can also easily understand and form these IP messages, we needed a scheme where only authorized participants can understand or create these messages.

At a very high level, the two primary strategies that have been used to protect from this type of messaging eavesdropping and spoofing are:

1. Controlling access - preventing unauthorized participants from accessing the messages in the first place: using firewalled networks, traffic routing rules, wired networks with physical access restrictions, etc.

2. Encryption – even if unauthorized participants can access the messages, preventing them from making any sense of them or being able to form legitimate ones of their own by using computer algorithms to scramble (encrypt) the messages.

In addition to the content and sensitivity of messaging changing over the years, today's wireless communication (primarily cellular and Wi-Fi) has made the strategy of controlling access much less feasible a protection method than was possible with wired local area networks (LANs). For wireless, encryption is really the only feasible way of protecting these messages.

Broadband Interoperability Project (BIOP) Encryption Scheme

To summarize and to reiterate some three years after it was stated in our final report for the BIOP Phase I[iii] project, we again conclude that, while end-to-end encryption is feasible and appropriate for LMR communications, for broadband interoperability, given today's fielded implementations, there are blocking, multi-vendor, multi-technology barriers to implementation that can only be addressed by the PTToB providers themselves. So, for Phase II prototyping and even for any short-term solution, a BIOP solution is obliged to work with the technology as it exists today. Catalyst determined that the encryption tools used today for highly sensitive internet-based transactions should provide adequate if not superior protection for these interoperability data pathways. Further, this encryption technology supports essential security requirements for broadband interoperability over data networks for what we termed "transcoded encryption". This phrase is also used by the National Public Safety Telecommunications Council (NPSTC) in their requirements for the LMR-to-LTE Interoperability final report and there it also describes using this approach when end-to-end encryption is not feasible.

In the transcoded encryption, shown in Figure , the BIOP gateway computer associated with a given system is treated as an encryption end-point for the interoperable PTToB system. Each gateway computer in the distributed BIOP system also acts as an encryption end-point to other BIOP gateway computers but using an MCPTT- agnostic encryption scheme. This approach is used since the BIOP cannot integrate encryption schemes between systems since they themselves are not compatible with each other. So instead, each BIOP gateway computer isolates them from each other using an independent encryption scheme. Additionally, we would argue that the isolation and the transcoding encryption implementation we have proposed and prototyped, where keys and certificates are not coordinated and integrated between interoperating systems, is in fact more secure over-the-wire than an end-to-end system where the system is one disclosed symmetric key away from full vulnerability. The primary vulnerability to the transcoded approach is that we must ensure that access to the BIOP gateway computers, where local applications pass clear intermediate traffic internally must be, from an

IT security perspective, sufficiently protected such that only authorized, trusted users can login. But that trust is really no different than what is expected of the device users at each end point.

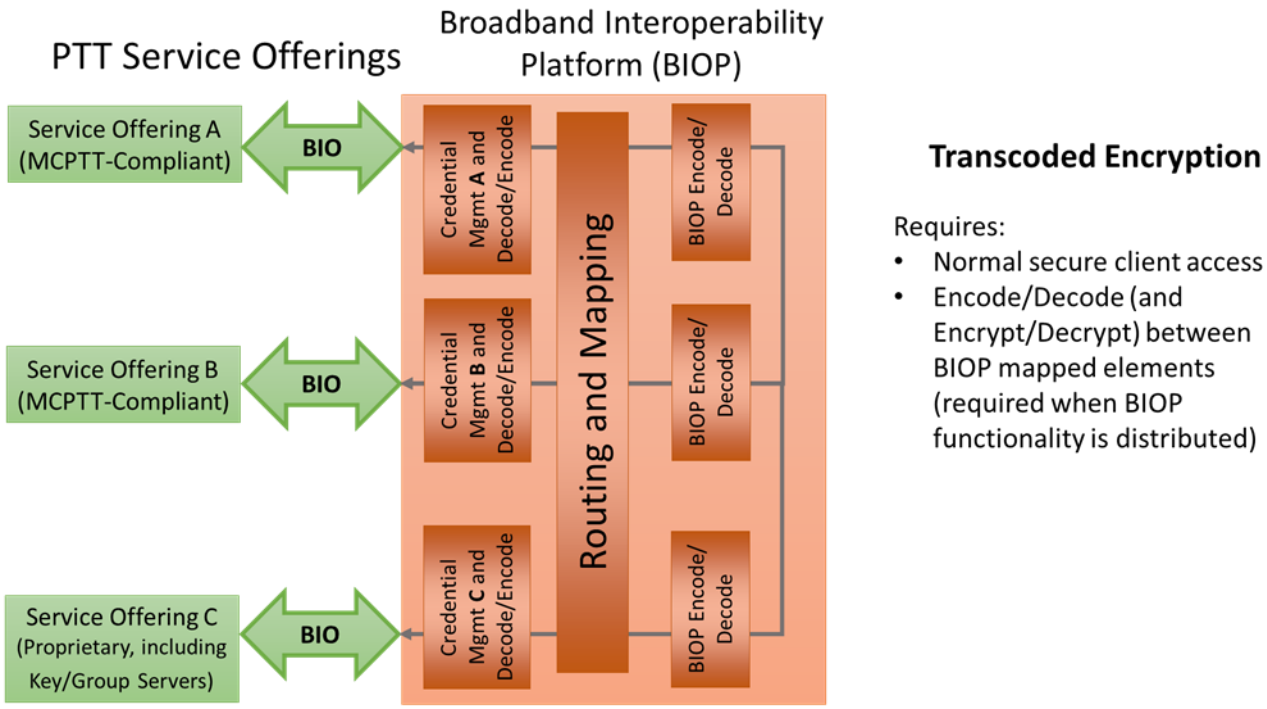

Figure 3 – The BIOP serves as the end points between different systems to encrypt and decrypt communications

Vocoder Strategy Overview

When connecting broadband to broadband, audio quality must be preserved as it passes between the distributed components of the BIOP. The prototype leverages the Catalyst interworking product which, like other products in the critical communication industry, was originally designed to provide interoperability between LMR channels. For bandwidth efficiency, the audio streamed between distributed Catalyst gateway components uses vocoders that are bandwidth-efficient and optimized for "radio quality" speech. For operations that involve LMR systems, LMR-to-LMR interoperability and even broadband-to LMR interworking, these vocoders generally introduce no audible limitations since the fidelity of the audio on at least one leg of the audio path is already "radio quality".

As part of this prototyping effort, Catalyst improved the fidelity of the audio that is sent between gateway components that make up the distributed BIOP by using wideband vocoders. We have chosen two vocoders to prototype as wideband options to our low bandwidth usage, narrow-band, "radio quality" codecs. We spent considerable time researching vocoders and examining tradeoffs between different vocoder technologies. The two vocoders that were prototyped were chosen based on different but complementary criteria.

Our proposal specifically calls out **AMR (technically AMR-WB[iv])** as the primary vocoder to be used to connect BIOP PTToB systems. The reasoning behind this early selection during the proposal phase was that AMR-WB is the codec required by 3GPP for MCPTT. Being able to preserve AMR-WB between interoperable MCPTT compliant systems without transcoding would theoretically provide the best

performance and audio quality for those configurations. Using AMR-WB when connecting proprietary systems or even for interworked systems that include LMR is a less clear-cut choice.

Recognizing that the BIOP would often be transcoding between incompatible vocoders, we tested another wideband vocoder that could be configured to preserve audio quality even more effectively than AMR-WB. This second codec is the **Opus - Open-Source Codec** which was developed by the Xiph.Org Foundation and standardized by the Internet Engineering Task Force. It is designed to efficiently code speech as well as general audio in a single format and is low latency enough for real-time communication and low complexity enough for low-end processors. Opus is a totally open, royalty-free, highly versatile audio codec[v] that compares very favorably against similar codec technologies. For interoperability between non-MCPTT-compliant systems, Opus is capable of providing a more versatile, higher quality and non-voice optimized codec.

Broadband Interoperability Using the Interworking Function (IWF)

Catalyst has been a pioneer in using the MCPTT Dispatch *client interface* for PTToB Dispatch, for PTToB to LMR Interworking, and now PTToB-to-PTToB Interoperability. There will be others in the industry who will be leveraging their P25 interfaces to use the IWF to connect to MCPTT-compliant PTToB systems. They will utilize these LMR-based interfaces for the interworking function the IWF was designed for but may also use the connection for PTToB dispatch or perhaps to accomplish PTToB to PTToB Interoperability. Catalyst plans to continue to use its native 3GPP approach, designed for primary dispatch, to provide PTToB to PTToB Interoperability in its SBIR Phase III commercial deployments.

The industry is exploring the available methods for achieving interworking between PTToB and LMR, including Voice-only Radio-over-IP (RoIP) and the 3GPP-defined Interworking Function (IWF.) RoIP voice-only connections are locked to a single talkgroup and do not provide any signaling data. The more complex IWF solution utilizes a P25 ISSI-style connection and provides a deeper integration between LMR and PTToB systems for interworking. We have found that the problem with this approach is that both are designed for **LMR** Interoperability where radio quality voice is acceptable. For broadband interoperability, hearing radio quality voice between broadband PTT users, especially on Smart Phones, is a significant limitation compared to the higher quality audio normally heard in broadband systems.

Our customers tell us that voice quality, along with latency, signaling information, and reliability are all critical factors. Catalyst believes that the approach we have prototyped is an impressive alternative for comprehensive interoperability that might otherwise be years away from being fully available and operational.

TASK 5 – DEMONSTRATE NEW FUNCTIONS, CONDUCT STRESS AND SCALING TESTING

1. Conduct Stress Testing
2. Conduct Scaling Testing
3. Demonstrate the prototyped functions and features to DHS

Demonstrate New Functions

A demonstration of representative prototyped functionality was conducted by Catalyst for DHS remotely on April 8, 2025 through Microsoft Teams. We demonstrated interoperability between two 3GPP

MCPTT-Compliant and two proprietary PTToB systems. Figure 4 shows a block diagram of the four systems involved in the demonstration, indicating the 3GPP-compliant Client Interface (BIO in the diagram) and P25 CSSI connections.

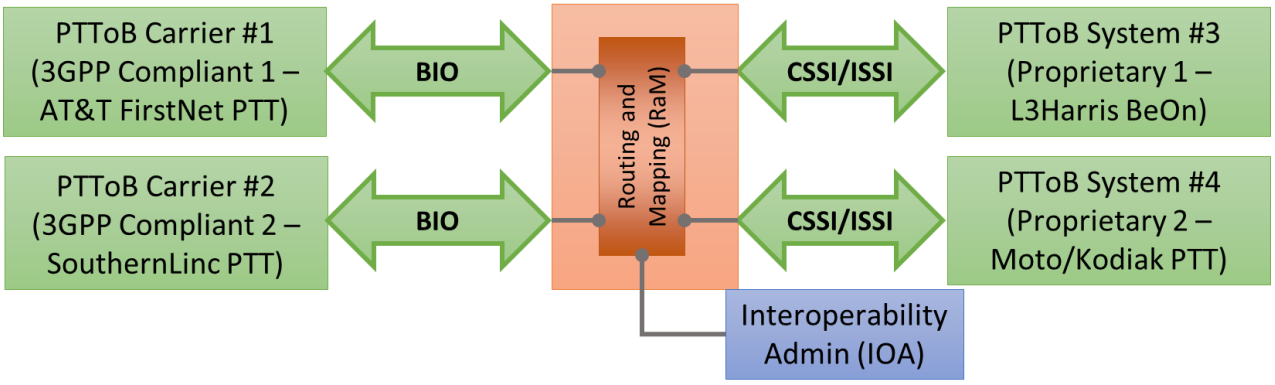

Figure 4 - Four PTToB Systems Used to Demonstrate Interoperability

The two 3GPP-Compliant PTToB Systems were:

- FirstNet PTT (Samsung built MCX Core)
- Southern Linc PTT (Ericsson/Genaker MCX Core)

The two CSSI Client Interface to a Proprietary PTToB Systems were:

- L3Harris BeOn (with P25 Encryption)
    - A key component of the approach was to choose a PTToB provider whose P25 CSSI interface supports encrypted talkgroups (AES 256)
- Motorola/Kodiak EPTT Advanced
    - Connects via CSSI without encryption
    - The technology demonstrated is EPTT Advanced and not Rapid Response
        - Industry experts tell us that the features available via CSSI are the same for both products
        - We can make emergency calls using this interface technology

The demonstration showed that any of the four PTToB systems could interoperate with any other by patching their respective talkgroups using the Catalyst Propulsion Interoperability Admin tool. The MCPTT-compliant systems offered additional interoperability features such as group texting interop. But the proprietary systems still offer basic functionality, including emergency calls. The BIOP is a workable, reliable technical solution, however as we seek buy-in from vendors and carriers, there are PTToB vendors who openly oppose interoperability with any other PTToB system.

We also demonstrated the following features developed and prototyped as part of this project:

- Emergency Alert Interoperability
- Texting Interoperability
- Examples of the usage of the Catalyst Interop Format Naming Convention

- Automatic patching using the Interop Format
- Encryption - Certificate-based, asymmetric encryption for connection negotiation and AES 256 symmetric encryption for steady state, secure messaging between BIOP gateways and clients.

Note that all audio passed between gateways and clients used AMR-WB vocoding

INDUSTRY BUY-IN

Industry buy-in to the concepts and technologies described in this report will be essential if the mission critical communications marketplace is to achieve interoperability among the various and many PTT systems. Throughout the course of this SBIR, Catalyst has been very active educating the marketplace about the availability, capabilities and value of our broadband interoperability solutions and the importance of this SBIR initiative to the industry. Our **marketing activities** included a multitude of initiatives to raise awareness among users and influence the service providers to support this initiative based on the benefits to the overall Public Safety marketplace.

Deployments

In addition to the extensive lab testing and public demonstrations, Catalyst has begun deploying portions of the BIOP. As of April 2025, we have three deployments we can discuss:

Dallas, GA

Dallas GA purchased a Catalyst system that we installed in the first quarter of 2024. The system initially included AT&T's FirstNet PTT, using the 3GPP-compliant interface, and AT&T's Rapid Response, a proprietary PTT solution that we interfaced to using the P25 CSSI protocol, as well as LMR. Later, Dallas requested that we add the L3Harris Beon PTT service interfaced via three control stations. Dallas continues to report that the system is working well as documented in this recent Urgent Communications interview https://urgentcomm.com/push-to-x/dallas-ga-joe-duvall-updates-progress-on-city-police-s-transition-from-lmr-to-lte-mcptt. Since this article was published, Dallas requested that Catalyst include Southern Linc's 3GPP-compliant service, Critical Linc.

Prominent Research Corporation

An MCPTT/LMR lab system configured for research and evaluation purposes was purchased from Catalyst and was installed in December 2024. It initially included AT&T's FirstNet® PTT and Southern Linc's Critical Linc, both using the 3GPP-compliant interface to these commercial carriers, as well as LMR and integrated, dual-mode dispatch. Later, we added an additional 3GPP-compliant interface for a private LTE system using the StreamWide MCX core. The customer has independently verified basic group call interoperability between these PTT services and the following advanced features: Emergency, Individual Call, Texting, and Patching to LMR. The customer reports that the system is working well.

Texas A&M University

Catalyst updated the Interworking system that we provided to the US Coast Guard at the conclusion of the previous DHS SBIR and installed it at Texas A&M University (TAMU). Today that system provides interworking between LMR and Southern Linc's Critical Linc, a 3GPP-compliant MCPTT service. TAMU reports that it is working well.

INDUSTRY NEXT STEPS

Catalyst has been working with PTToB for many years starting in 2009 with 3G PTT and has been working with 3GPP-compliant MCPTT since 2019. In North America, public safety and others who use critical communications are not seeing a comprehensive, nationwide PTToB system, but instead see a plethora of disjointed systems that cannot interoperate. DHS apparently had that same concern when they wrote the solicitation for this project in 2022. Our read on the PTToB market today (January 2026) is:

1. Public safety customers are asking for extremely reliable, simple, secure, voice communications that mirror LMR functionality with little tangible interest in advanced functionality. We conclude that because:
    a. Most public safety customers using mission critical PTToB are not using smartphones, ruggedized or otherwise, but instead using LMR radios that also support broadband.
    b. Public safety customers appear to be looking to fill LMR coverage gaps or replace insufficient LMR coverage with cellular coverage but essentially using LMR devices.
    c. Most public safety leaders aren't ready to trust cellular carriers and hence retain LMR either as their primary or as a backup. Access to multiple carriers for both backup and coverage is highly desired.
    d. Public Safety requires Direct Mode (also known as Talk Around) and dual mode LMR/Broadband devices to fill this need.
    e. Significant advanced broadband features won't even operate on these dual mode devices.
2. The National Broadband Public Safety Network, FirstNet® Built with AT&T, has made great strides in many areas but is still a work in progress for PTT. In fact, recent technology changes have further delayed the widescale adoption of an open, 3GPP-compliant MCPTT service on FirstNet as the nationwide, "first choice" system.
3. In Catalyst's opinion, the importance and even the definition of 3GPP compliance is not well understood in the industry by customers or vendors:
    a. The advanced technology features (e.g. data features, location, video) that were the promise of mission critical cellular are not fully deployed and available on 3GPP-compliant systems.
    b. Even the more basic features that LMR already has such as the ability to elevate a talkgroup to emergency status have been very slow to be deployed on 3GPP-compliant systems.
    c. Mature, non-3GPP-compliant services appear to be more fully featured but remain siloed, isolated, and without motivation to interoperate.
    d. Catalyst includes in the non-3GPP-compliant category vendors who claim to have 3GPP-compliant solutions, perhaps even demonstrate interoperability with 3GPP-compliant vendors at European Telecommunications Standards Institute (ETSI) plugtests, but do not allow 3GPP-compliant products to natively connect using 3GPP messaging on their deployed systems. For all intents and purposes, these are proprietary PTToB services and that is how we must classify them for this report.

4. The conclusion is that the only feasible, nationwide PTToB system that could be widely adopted and carrier agnostic in the short and medium term would be composed of many interoperating disparate PTToB systems.

Given the systemic, fragmented, broken, siloed state of PTToB in North America today, the nationwide communication system mandated by legislation in 2012 can only be achieved in 2026 by expanding interoperability between the PTToB islands that exist today. As we conclude this broadband interoperability project, Catalyst's recommendations on next steps are:

1. The type of broadband interoperability prototyped in this project, connecting disparate PTToB systems, is the only workable way of making today's fragmented systems work together in the short term.
2. The FirstNet PTT portal that supports agency talkgroup sharing is a very forward-thinking, innovative tool for inter-agency cooperation, but will soon be deprecated. This excellent tool needs to be reincarnated using a multi-technology, multi-vendor, multi-carrier approach.
3. A reliable BIOP solution, one that provides basic functionality while addressing coverage gaps, meets the broadband interoperability requirements of what the industry needs today. Catalyst's BIOP solution meets and exceeds these requirements by supporting broadband voice quality, meeting security requirements, and providing virtually all advanced functionality that the industry will require in the short term and does so without requiring an invasive system-to-system interface.
4. Many public safety agencies want to use cellular and multi-carrier to span coverage gaps. They are not actively seeking (and the PTToB systems do not seem able to provide at scale or nationwide) highly advanced functionality, though providing this functionality could attract some customers, such as early adopters.
5. Government policies and mandates as well as customer and market pressure are needed to prevent PTToB providers from stonewalling interoperability:
    a. Catalyst has over 25 years of experience in providing technology that can enable solutions to interoperate, but system vendors can and do routinely create technical and economic roadblocks to interoperability and actively campaign to hinder interoperable communications.
    b. PTToB suppliers demonstrate over and over that they must be compelled to provide standards-based solutions and interoperability. Both are in the public's best interest and allow free market economics to drive solutions to be more accessible, more capable, and less expensive.
    c. Just as was required for P25, mandating PTToB standards to receive federal funding is one step toward stopping the unfettered predominance of proprietary, siloed PTToB systems. For critical communication, the 3GPP MCX standards are the only vetted contenders for broadband standards.

Perhaps more effective than mandates are informed, educated customers who will reward supportive, forward-thinking vendors with their business.

CONCLUSION

Now that the BIOP project has been completed, Catalyst concludes with more confidence than ever that the key to creating a successful, nationwide PTToB network in North America will be the ability to create effective interoperability between the many disparate PTToB systems deployed today AND interworking with LMR. Over the last two years, Catalyst has demonstrated via our prototype that this solution is technically viable. This project focused on features and requirements especially important when connecting broadband systems. Examples of these are manufacturer extensions to standard MCPTT messaging that can be used to provide Talker IDs and other Talker information for external users to the interoperating system, interoperable group texting, priorities, and emergency alerts. Other examples are better administrative tools and talkgroup naming conventions that facilitate interoperating talkgroups on disparate systems. And, finally, preserving broadband voice quality and messaging between PTToB systems using highly secure encryption techniques. Catalyst has demonstrated all of these capabilities and fully met the operational objectives of this Phase II SBIR.

---

[i] Catalyst Communications Technologies, Inc., *PTT Over Broadband Interoperability Platform Feasibility Study, Phase 1 SBIR, Final Report,* October 9, 2022

[ii] NPSTC Mission Critical Push to Talk (MCPTT), Considerations for Interoperability Talkgroup Naming and Management, November 2018

[iii] Catalyst Communications Technologies, Inc., PTT Over Broadband Interoperability Platform Feasibility Study, Phase 1 SBIR, Final Report, October 9, 2022

[iv] VoiceAge, AMR-WB/G.722.2, https://voiceage.com/AMR-WB.G.722.2.html

[v] Opus Comparison – Codec Landscape https://opus-codec.org/comparison/