NATIONAL TELECOMMUNICATIONS AND INFORMATION ADMINISTRATION
FIRST RESPONDER NETWORK AUTHORITY

RESPONSE TO NOTICE OF INQUIRY [DOCKET NO. 120928505–2505–01]

NOVEMBER 1, 2012

Submitted to:

National Telecommunications and Information Administration
Herbert C. Hoover Building (HCHB)
U.S. Department of Commerce/NTIA
1401 Constitution Avenue N.W.
Washington, DC 20230
Attn: FirstNet NOI
firstnetnoi@ntia.doc.gov

Prepared by:

Keith McFarland
Solutions Architect, GSG Professional Services
275 West Street
Annapolis, MD 21401
Phone: 443.875.7135
Email: kmcfarland@telecomsys.com
www.telecomsys.com

TCS Proprietary Level 2

External Distribution: Media containing proprietary information of this level should be delivered directly and may require signature of receipt using approved carriers.

Electronic Distribution: Media containing proprietary information of this level should be encrypted; however, it is not required.

Disposal: When electronic media or printed media containing TCS proprietary information are no longer needed and any applicable retention period has lapsed, the data should be electronically deleted or physically destroyed. All Proprietary Level 2 printed media must be shredded or securely disposed of.

TCS Proprietary Level 2 Guidelines

TCS Proprietary Level 2 is applied to information assets that are classified as Business Critical or Highly Confidential. Below is a summary of the instructions for handling.

- **Accessibility:** Media must be kept from view of unauthorized individuals. Documents or other media should not be left in view on computer screens, desks, or tabletops. When not in use, they should be stored out of plain sight. When removable media (e.g., thumb drives or CDs) or email is used to store or transmit this level of information, encryption is recommended. Care should be taken that distribution is only to the intended recipients.
- **External Distribution:** Media containing proprietary information of this level should be delivered directly and may require signature of receipt using approved carriers.
- **Electronic Distribution:** Media containing proprietary information of this level should be encrypted; however, it is not required.
- **Disposal:** When electronic media or printed media containing TCS proprietary information are no longer needed and any applicable retention period has lapsed, the data should be electronically deleted or physically destroyed. All Proprietary Level 2 printed media must be shredded or securely disposed of.

The following information is TCS confidential and proprietary and may be protected under one or more United States and foreign patent(s) and/or patent applications.

Notices

TCS currently holds 249 issued patents and has more than 350 patent applications pending worldwide. Its patents cover a broad spectrum of technologies, including wireless data, text and voice telecommunications, location-based services, GIS/mapping, intercarrier messaging, secure communications, public safety/E9-1-1, and mobile navigation.

NASDAQ GM: TSYS

TABLE OF CONTENTS

EXECUTIVE SUMMARY **1**

1.0 INTRODUCTION **3**

2.0 PUBLIC SAFETY MOBILE MANAGEMENT FRAMEWORK **5**

2.1. Integrated MDM and TEM **6**

2.1.1. MDM and TEM Deployment and Integration Models *7*

2.1.2. TCS MDM Overview *7*

2.1.3. TCS Telecom Expense Management System Overview *10*

2.1.4. Integrated MDM and TEM Benefits for FirstNet Users *16*

2.2. Mobile Application Framework **17**

2.2.1. OTT Application Services *17*

2.2.2. Mobile Application Management *18*

2.2.3. Trusted and Verified Applications *19*

2.2.4. Grade of Service *21*

3.0 PUBLIC SAFETY ACCESS NETWORK DIVERSITY **25**

3.1. TCS SwiftCell – Deployable LTE Communications **25**

3.2. TCS IBW Solution Overview **26**

3.2.1. TCS In-Building Cellular Capabilities *26*

3.2.2. TCS Wi-Fi Offerings *27*

3.3. IBW and Deployable LTE Benefits **27**

4.0 CONCLUSION **28**

LIST OF EXHIBITS

Exhibit 1. Administrative Data 1
Exhibit 2. Summary Recommendations Table 4
Exhibit 3. Enterprise Integration Services 8
Exhibit 4. TCS-Recommended QoS-Enabling Architecture for Applications 23

ACRONYMS

Acronym	Definition
3GPP	Third Generation Partnership Project
3T	Tactical Transportable Troposcatter
AC	Access Class
AD	Active Directory
API	Application Program Interface
ARP	Allocation Retention Priority
BGAN	Broadband Global Area Network
BYOD	Bring Your Own Device
CIG	Cyber Intelligence Group
COOP	Continuity of Operations
COW	Cellular on Wheels
DLP	Data Loss Prevention
DSCP	Differentiated Services Code Point
E9-1-1	Enhanced 9-1-1
EAS	Exchange ActiveSync
EIS	Enterprise Integration Service
EP	Emergency Preparedness
ERP	Enterprise Resource Planning
FCC	Federal Communications Commission
FIPS	Federal Information Processing Standard
FirstNet	First Responder Network Authority
FNN	FirstNet Network
GBR	Guaranteed Bit Rate
IA	Information Assurance
IBW	In-Building Wireless
IPSec	Internet Protocol Security
IT	Information Technology
L2TP	Layer 2 Tunneling Protocol
LBS	Location-Based Services
LDAP	Lightweight Directory Access Protocol
LMR	Land Mobile Radio
LoS	Line of Sight
LTE	Long Term Evolution
MAM	Mobile Application Management
MAS	Mobile Application Store

Acronym	Definition
MDM	Mobile Device Management
MNO	Mobile Network Operator
NG9-1-1	Next Generation 9-1-1
NS/EP	National Security/Emergency Preparedness
NTIA	National Telecommunications and Information Administration
OTT	Over the Top
PCRF	Policy Charging and Rules Function
PII	Personally Identifiable Information
PKI	Public Key Infrastructure
PPTP	Point-to-Point Tunneling Protocol
PSBN	Public Safety Broadband Network
QCI	QoS Class Indicator
QoS	Quality of Service
RAN	Radio Access Network
RF	Radio Frequency
RFI	Request for Information
SaaS	Software as a Service
SCM	Supply Chain Management
SDK	Software Development Kit
SEG	Secure Email Gateway
SIEM	Security Information and Event Management
SQL	Structured Query Language
SSL	Secure Socket Layer
TCS	TeleCommunication Systems, Inc.
TEM	Telecom Expense Management
VoIP	Voice over Internet Protocol
VPN	Virtual Private Network
VSAT	Very Small Aperture Terminal
WEP	Wired Equivalent Privacy
WPA	Wi-Fi Protected Access
WPS	Wireless Priority Services
WWSS	World-Wide Satellite Systems
XSS	Cross-Site Scripting

EXECUTIVE SUMMARY

On behalf of the First Responder Network Authority (FirstNet), the National Telecommunications and Information Administration (NTIA), requests comments on the FirstNet board's conceptual proposals for nationwide network architecture and public safety application framework. TeleCommunication Systems, Inc. (TCS) offers its feedback to these proposals as well as additional input and recommendations to create a reliable, ubiquitous, redundant, and interoperable broadband network for public safety users. TCS produces end-to-end solutions for both government and commercial customers who demand communications with proven high levels of reliability, security, and availability. TCS' corporate expertise, detailed in Exhibit 1 below, enables TCS to make innovative and comprehensive recommendations to the FirstNet board.

Exhibit 1. Administrative Data

Business Name and Address	TeleCommunication Systems, Inc. (TCS) 275 West Street, Annapolis, MD 21401
Point of Contact	Keith McFarland, Solutions Architect 410.280.1209 kmcfarland@telecomsys.com
Corporate Expertise	TCS' innovative technologies encompass secure, deployable communication systems; location-based wireless infrastructure; smart phone apps across all leading mobile operating systems; telematics and navigation; Voice over Internet Protocol (VoIP) Enhanced 9-1-1 (E9-1-1) services; text messaging infrastructure for wireless operators; information assurance (IA) and cybersecurity; engineered satellite-based services; and professional services for communications solutions.

About TCS

TCS has pioneered the development of a suite of wireless applications, including text messaging, location-based services (LBS) infrastructure and applications, internet content and hyperlocal search, public safety services (E9-1-1, E1-1-2), and other enhanced communication services. As a world leader in LBS end-to-end solutions and as a national leader in text messaging and E9-1-1, TCS maintains a commanding market share for its commercial operations.

TCS is also a global leader in deployable communications, with a long and proven track record of delivering seamlessly integrated, end-to-end communications solutions – wherever customer personnel and equipment are located. TCS' solutions are technically advanced and based on international communications experience in design, production, deployment, installation, training, operation, service, and maintenance. TCS' deployable systems and fixed land earth stations enable communications in some of the most hostile and remote locations, including Afghanistan and Iraq. The company's certified and cleared personnel serve as trusted advisors to key government agencies. TCS' professional services consist of cybersecurity, continuity of operations (COOP) and emergency preparedness (EP), and business and technology management.

Supporting and developing every facet of network operations, information technology (IT) and cybersecurity infrastructure, TCS' Cyber Intelligence Group (CIG) draws from a deep pool of professional expertise. Several of TCS' cybersecurity experts serve on working groups of the Federal Communications Commission (FCC) Communications Security, Reliability and Interoperability Council. The mission of the council is to provide recommendations to the FCC to ensure optimal security, reliability, and interoperability of communications systems.

TCS delivers a host of network operations, computer network defense, and cyber solutions to commercial and government agencies. From program management, software engineering, and IA to enterprise architecture and cyber warfare, TCS' CIG helps harden high-value entities, systems, and networks against cyber attack.

The strength of TCS' products and solutions is built on listening to its customers, predicting and harnessing emerging market and technology trends, and then translating requirements and raw technology into an end-to-end solution with supporting services. TCS has developed a suite of products under the SwiftLink® brand designed for federal, state, and local governments and commercial customers who require highly reliable communications solutions, managed services, and seamless, secure connectivity. More than 2,000 of TCS' deployable communication systems are currently used around the world for security, defense, and law enforcement purposes.

TCS' customers include leading operators around the world, public safety agencies, state and local governments, the U.S. Special Operations and Intelligence communities, and agencies of the U.S. Departments of Defense, State, Justice, and Homeland Security.

Founded in 1987 by a U.S. Naval Academy graduate, TCS is U.S. owned and operated. The company is publicly traded on the NASDAQ Global Market under the symbol TSYS. In 2006, TCS was named one of six prime contractors on the U.S. Army's World-Wide Satellite Systems (WWSS) contract vehicle, with a ceiling value of up to $5 billion in procurements through 2014.

1.0 INTRODUCTION

Over the years, various technological advances have resulted in proliferation, growth, and extensive use of wireless networks for both communication as well as access to information. These include but are not limited to:

- Feasibility and availability of "seamless and interconnected" wireless broadband (e.g., Wi-Fi, 3G, and 4G) due to standardized interfaces for interoperability and roaming between these networks.
- Emergence of an alternative application delivery architecture often referred to as the Over the Top (OTT) model, which is independent of device and network. In the OTT model, the operator wireless network primarily provides data connectivity, while applications are facilitated via software on the phone and an application core in the network cloud.
- The emergence of smartphones and their application stores, permitting users to install and enable applications implemented in this OTT manner whenever they choose.

FirstNet should leverage these advances to achieve a ubiquitous, reliable, redundant network for public safety users in an economical and timely fashion rather than building a standalone purpose built network from scratch. The conceptual proposals shared by the FirstNet board indicate that the board is in agreement. However, it should not be overlooked that these advances were focused and optimized for enabling commercial usage, not mission-critical usage that would be desired when they are used for public safety purposes.

TCS' responses to the FirstNet inquiry in subsequent sections are focused on highlighting the additional capabilities that the FirstNet architecture and applications should include to make the organization mission-critical ready. TCS has extensive experience developing products that operate in mission-critical environments, both domestic and international, where success is measured in lives saved and operational excellence is achieved by reducing downtime to minutes per year.

TCS input and recommendations (Exhibit 2) address both the architecture and application framework proposal. TCS' comprehensive recommendations focus on key areas like mobile application framework, device management, expense management, security, Quality of Service (QoS), and access network diversity, all of which are critical to the successful enablement and operation of FirstNet.

Exhibit 2. Summary Recommendations Table

Key Areas	Summary Recommendations	Summary of Benefits
Mobile Management Framework	TCS recommends that a framework for application development and delivery be included within a broad, comprehensive solution consisting of people, processes, and technology focused on managing the increasing array of diverse mobile devices.	• Addresses three major factors prohibiting adoption of a mobile workforce: policies and management of devices; security; and cost controls. • Provides comprehensive approach to mobility management and avoids the pitfalls of silo management.
Integrated Mobile Device Management (MDM) and Telecom Expense Management (TEM)	TCS recommends the use of an integrated MDM and TEM offering to provide full lifecycle management of an agency's mobility workforce.	• Reduces the operational management barrier for adoption by agencies. • Provides specific security and privacy to enable mobility for Public Safety Broadband Network (PSBN) users. • Reduces cost barrier. Monitors and optimizes costs across all Long Term Evolution (LTE) networks routinely
Mobile Application Framework	TCS recommends that the FirstNet Network (FNN) authority enable a framework designed to facilitate: • OTT application services • Mobile Application Management (MAM) • Trusted and verified applications • QoS management	• Enables the mission of FirstNet by delivering secure and specialized applications through an app catalog. • Provides OTT applications, which are more cost effective than the traditional network integration model for user services. • Allows OTT applications to be integrated with QoS requirements for use across all networks. • Provides seamless operation and user experience across diverse networks and devices. • Centralizes management of internal, public, and purchased applications. • Ensures security objectives are achieved through advanced app verification and distribution. • Enhances mobile strategy by understanding how apps are being used.
Access Network Diversity	TCS recommends that FNN's proposed access diversity is augmented through: • The use of rapidly deployable LTE solutions for emergency network augmentation. • For specifically high-value locations, the implementation of campus or In-Building Wireless (IBW) solutions.	• Provides dedicated FNN-specific coverage in high-value buildings and campus environments through the use of IBW. • Uses diverse methodologies and networks to provide ubiquitous nationwide access, integrating with the FirstNet design approach. • Rapid deployable LTE systems can interconnect to the broader FNN or act as a stand-alone miniature FNN.

2.0 PUBLIC SAFETY MOBILE MANAGEMENT FRAMEWORK

The NTIA's FirstNet board recognizes the need to offer innovative services through dedicated applications for PSBN users. TCS believes that the PSBN is ideally suited to be the primary Mobile Network Operator (MNO) for the millions of federal, state, and local government employees. However, the PSBN will be unique in that it will be the only LTE network specifically designed to deliver complete service through an extensive interweaving of native PSBN and multiple competing commercial operators. TCS believes that this network approach is the ideal mix to bring service online in the most expeditious manner while minimizing the outlay required in advance of network service readiness. This unique architecture approach and the class of PSBN users will create unique opportunities and challenges. TCS wants to remove these challenges, which left unaddressed would prohibit adoption of the PSBN by its primary target audience, which will come from a diverse set of agency backgrounds and mobility funding.

Earlier in 2012, Yankee Group identified five major trends in the mobility market space:

- A continually growing mobile workforce.
- Mobile as an increasingly important channel for businesses.
- Smartphones and tablets emerging as legitimate enterprise computing devices.
- Consumerization and bring your own device (BYOD) driving user and enterprise technology decisions.
- The rise of mobile applications to address worker and customer needs.

Due to the rapid evolution of the mobile market and increased adoption rates, many federal, state, and local agencies are unable to effectively and securely manage their mobile workforce. TCS has seen the effects of this firsthand while working with its clients. When it comes to mobility, full-scale adoption by enterprises is primarily prohibited through a series of three factors. First, enterprises are unable to manage and develop policies for the vast array of devices. Second, many public and private enterprises are focused on their primary objectives; they may be unable or unaware of methodologies and tools to facilitate mobile employee efficiencies without compromising classified or sensitive information. Third, TCS has seen that, in a budget-reducing environment, mobility expenses create a situation of risk and uncertainty for those who manage mobility budgets. This financial risk and uncertainty prohibits even broader adoption and use.

Therefore, TCS recommends that a framework for application development and delivery be included within a broader, comprehensive solution consisting of people, processes, and technology focused on managing the increasing array of diverse mobile devices within an organization. This enterprise mobility management solution would address the challenges faced by PSBN users and their respective enterprises. Enterprise mobility management solutions are designed to enable broad use of mobile computing efficiently and securely. This approach to mobility management is not just about managing devices. It facilitates the entire lifecycle of a mobility workforce in an integrated manner, from procurement and cost controls to operations, security, and services to end-users. As a result, this approach will lead to a higher adoption rate and increased usage of the PSBN.

Enterprise Mobility Management Solution

- Integrated MDM and TEM
  - Software Management
  - Network Service Management
  - Hardware Management
  - Security Management
  - Order Management
  - Expense Management
- MAM
  - Mobile Application Store (MAS), Mobile Application Policies
  - Trusted Ecosystem of Secure Mobile Applications
- Grade of Service Management

TCS believes that the FNN is the preferable location for deploying a centralized enterprise mobility management solution. Deploying this solution within the FNN network centralizes and standardizes the approach across many of the different agencies utilizing the network. Additionally, this centralized deployment model within the FNN will create economies of scale for all enterprises that use the PSBN and these services, producing significant cost savings. Smaller agencies will be relieved of the burden of learning and managing these methodologies on their own. They can leverage the economies of scale for policies, management, and savings garnered through a national approach.

2.1. Integrated MDM and TEM

Due to the unique architecture of the PSBN and its respective users, agencies will consider management of their enterprise, expenses, security, services and reliability relative to their adoption and use of the network. To address those considerations, TCS recommends strengthening an MDM offering through the addition of TEM services in an integrated solution. TCS understands the new IT challenges FNN users face, from security, compliance, and management to cost and human capital management. These challenges typically force organizations to invest in MDM products and services in an ad hoc manner, resulting in higher costs and reduced capability.

An integrated MDM and TEM solution is part of a comprehensive mobility management methodology. Pulling together these two components into an integrated offering, agency administrators can now manage the full lifecycle of mobile devices. Device inventory, management, and expense controls can be managed together with device services, security, and integrity functions. The addition of TEM services can result in significant cost savings. Although savings will vary from each agency, when TCS works with its customers on TEM services, the customer typically realizes double-digit percent savings on overall mobility costs. In conclusion, enabling centralized management of an agency mobile workforce and providing cost control mechanisms will increase adoption of the PSBN.

2.1.1. MDM and TEM Deployment and Integration Models

TEM and MDM models typically support two models for deployment:

- The software-as-a-service (SaaS), or cloud, delivery model, which provides FNN greater flexibility, scalability, and cost effectiveness. Some service providers support an additional model that takes a hybrid approach, using SaaS and strategic on-site servers to provide flexibility and security in an enterprise network.
- A more traditional model is the in-network or enterprise hosted model, which would be deployed within the FNN.

TCS recommends that FNN consider the cloud-based MDM services model with hybrid extensions, as it is more economical and flexible than a purely on-site hosted solution. TCS recommends that the solution reside in a carrier-grade data center with a multilayered security strategy to protect agency network integrity and a disaster protection approach that ensures optimal availability engineered for performance and data redundancy. Cloud-based solutions are engineered to support deployments of multiple agencies and thousands of devices through a scalable architecture that is fully redundant and configurable. TCS and its partners have experience with each of the deployment models presented here.

2.1.2. TCS MDM Overview

The TCS MDM solution contains the traditional capabilities, as defined by Gartner in its May 2012 report: software management, network service management, hardware management, and security management. TCS' solution stands apart from those of many other providers and includes integrated MAM and enterprise content management, which has been driven by the demand for consumer mobility and BYOD adoption. The following information, though not exhaustive, highlights many of the TCS solution features and benefits specific for use by PBSN users and their enterprises.

In support of a cloud-based deployment, two services are deployed on-premise to ensure enhanced capabilities and security of TCS' solution:

- *The Secure Email Gateway (SEG)* provides the highest level of security, visibility, and control in managing mobile email through tight integration with the FNN infrastructure. This ensures that only those devices provisioned within the solution and those that comply with associated rules are allowed to communicate.
- *The Enterprise Integration Service (EIS)* server connects the FNN cloud instance to its on-premise services directly from an FNN console through a secure, self-service process. For on-premise environments deployed in tiered network models, the EIS server enables TCS' MDM solution to communicate with various corporate services across network layers. Additional EIS highlights are outlined in

- Exhibit 3.

Exhibit 3. Enterprise Integration Services

Directory Services	Solutions integration with Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) allows the FNN to take advantage of existing groups to manage users and devices. The FNN also can assign profiles, applications, and content based on a user's role and group membership. If a user belongs to multiple groups, the TCS solution ensures that the user receives the right access, and restrictions are applied for all groups a user is a member of. Ongoing AD/LDAP synchronization detects any changes within the system and can automatically perform necessary updates across all devices or require administrative approval before any changes occur.
Certificates and Public Key Infrastructure (PKI)	For enterprises leveraging certificates for advanced user authentication and secure access to corporate systems, the TCS solution provides direct integration to Microsoft CA, CA, or SCEP certificate services providers, such as MSCEP and VeriSign. Certificates can be configured for a number of systems, including Wi-Fi, Virtual Private Network (VPN), and Exchange ActiveSync (EAS). The solution automatically distributes these certificates down to the devices and configures Wi-Fi, VPN, or EAS access without any user interaction. Administrators have complete visibility into certificate information such as installed, expiring, and revoked certificates through a certificate management dashboard.
Email Infrastructure	The TCS solution's SEG provides the highest level of security, visibility, and control in managing mobile email through tight integration with FNN's email infrastructure.
Corporate Networks	TCS can configure Wi-Fi and VPN network settings and provision device profiles containing user credentials for access. It also can configure Wired Equivalent Privacy (WEP) and Wi-Fi Protected Access (WPA)/WPA2 Enterprise Wi-Fi settings and connect users to enterprise VPN networks, including Secure Socket Layer (SSL; Juniper, F5, Cisco), Internet Protocol Security (IPSec), Layer 2 Tunneling Protocol (L2TP), and Point-to-Point Tunneling Protocol (PPTP). The advanced VPN On Demand capability will detect when a user is accessing specific corporate sites and automatically authenticate and launch a VPN session in the background. This process is invisible and seamless to users, allowing them to continue working without interruption.
File Systems	Enterprises using the TCS solution's Secure Content Locker application to deliver secure mobile access to corporate documents can integrate directly with their existing file systems, including SharePoint, file servers, and networks shares. This allows enterprises to distribute and synchronize files from their enterprise or cloud servers to a mobile user's device. Users are authenticated with a username, password, and certificate before they can access corporate content.
Internal Apps (Software Development Kit [SDK])	TCS' SDK enables enterprises to build business apps that leverage TCS' core security, integration, and management capabilities. The FNN can leverage TCS' direct AD/LDAP integration to standardize user authentication across all business apps, and can use Application Program Interfaces (APIs) to send app data to other enterprise systems or third-party apps.
APIs	The TCS solution provides a collection of APIs that allow external programs to use core product functionality. Enterprises can use this to integrate with existing IT infrastructures and third-party applications. Available web services include user enrollment, device registration, device groups, user information, device data, and remote device commands.
Security Information and Event Management (SIEM)	The TCS solution integrates with SIEM solutions for enhanced logging of events occurring in the console. Administrators can view events; filter by event type, category, and module; and export events. Event logging settings can be configured based on severity levels, with the ability to send specific levels to external systems via Syslog integration.

2.1.2.1. Enhanced Security

The TCS solution enables government agencies to leverage advanced mobile devices and applications without compromising security and compliance. Its advanced security capabilities include strong user authentication using AD/LDAP; certificate-based access to enterprise email, Wi-Fi, and VPN; and secure distribution of apps and documents. The solution meets Federal Information Processing Standard (FIPS) Publication 140-2 compliance standards and ensures confidential data is protected.

2.1.2.2. Compliance Monitoring

The solution constantly monitors the device fleet for unauthorized users, compromised devices, blacklisted apps, and other risks. When a threat is identified, the TCS solution can block access to enterprise email, applications, and resources, then lock and wipe a device automatically through TCS' configurable compliance engine.

2.1.2.3. Secure Content Locker

With the Secure Content Locker mobile application, agencies can now securely distribute and access sensitive documents from a mobile device; transmit documents over industry standard 256-bit SSL encrypted connections; and prevent access for unauthorized users or noncompliant devices. The application also allows agencies to control a user's ability to edit, share, or open files in unauthorized applications, and can remotely wipe documents from the console.

2.1.2.4. Containerization

Amid the growing demand for mobility, TCS leads the way in security and compliance, through the utilization of containerization, which separates the corporate and personal content on devices. The original approach of complete corporate containerization, locks down the corporate footprint, with total separation of business and personal content. Managing the corporate container instead of the device grants isolation and protection of corporate content, with no restrictions on personal usage. However, the native email clients and browsers are not available in the container, which would not be acceptable to users in a BYOD environment. The TCS approach is to utilize containerization for individual applications, folders, and files while ensuring the native services on the device are unaffected. TCS provides SDKs to enforce credentials, encryption, and other policies through application wrapping.

2.1.2.5. VPN On Demand

The TCS solution provides the ability to provision a VPN profile to devices to automatically configure access to corporate networks and file systems. TCS' advanced VPN On Demand capability allows mobile users to securely access specific websites through a VPN tunnel. This process is invisible and seamless to users, allowing them to continue working without interruption.

2.1.3. TCS Telecom Expense Management System Overview

TCS has addressed the needs of large and diverse commercial enterprises with full-cycle TEM management for more than 20 years. In that time, the company's ManageRight solution has outpaced the wireless marketplace by balancing the competing needs of demanding mobile workforces with economical contract sourcing and analytical utilization strategies.

TCS' workflow model is seamless; it does not utilize separate systems and processes requiring manual integration (swivel chair). ManageRight is built on a single platform, with all application modules and workflow driving off the same database. ManageRight provides integration of purchasing, inventory/asset management, invoice management, and financial management. The infrastructure links carriers and internal business systems through an electronic interface, automating the wireless service supply chain, allowing for maximum sharing of information, and enabling a closed loop solution.

2.1.3.1. Wireless TEM System Capabilities

Featuring modularity and an intuitive user interface, ManageRight presents on-demand visibility to agency spend, analytics, procurement, and optimization.

2.1.3.2. Inventory Management

Inventory management functions facilitate administrative cost controls for devices and accessories. Inventory management functions:

- Track multiple devices and items per users.
- Track serialized and non-serialized inventory.
- Allow acquisitions, updates, moves or dispositions.
- Allow bulk data uploads for enterprise resource and accounting systems used during initial setup and periodic updates phases.

2.1.3.3. Automated Invoice Processing

The ManageRight Solution will receive and handle all wireless invoices regardless of format, carrier, or service. Each wireless invoice is received and entered into the process for verification and payment. The "receipt-to-pay" activities are performed efficiently within five business days. To facilitate efficient invoice processing, TCS works with carriers to organize and consolidate invoices and convert them into electronic media. TCS supports all wireless invoice formats, including international carriers, as well as all electronic formats (EDI, CDs, downloads). Scanning paper invoices and manually entering data is performed as necessary.

2.1.3.4. Automated Invoice Reconciliation

The ManageRight Solution performs automated invoice audits. The solution automatically checks the invoices against contract and plan terms, inventory, taxes, and regulatory fees. As errors are identified, disputes are opened with the carrier and managed to resolution. Eighty percent of the work involved in resolving disputes is in management of the process with the vendors. TCS has a track record of results, including a 98 percent recovery rate, usually within a single billing cycle.

2.1.3.5. Invoice Accounting and Payment

By outsourcing to TCS, agencies will eliminate the burdens associated with invoice-coding and payment. TCS' technology applies agency specific accounting rules and applies them to wireless invoices. This results in:

- Complete visibility and an "open book" invoice management process.
- 100 percent review – every invoice line item, subcomponent, and amount is validated against real-time inventory and contract/tariff.
- Proactive management of the invoice "receipt-to-pay" process.
- Anytime, "at your fingertips" access to personal data.
- Disputes filed and credits recovered on customers behalf.
- An electronic bond to enterprise accounting and finance systems.

2.1.3.6. Comprehensive Mobile Analytics and Reporting

TCS' management reporting provides superior visibility and insight into wireless utilization via:

- A single, web-based portal that provides a complete picture of all wireless communications in an organization, agency, department, or user level regardless of how many providers are delivering mobile services.
- Full management of the details of cellular/mobile communications, including identification of personal calls and assigning account codes to cellular calls for external or project-based chargeback.
- A full suite of management, trending, and exception reports built specifically to manage a wireless environment.
- Documented results of policy implementation and its direct effect on costs.
- Auditing for compliance with security, legal and regulatory requirements related to communications.

2.1.3.7. Procurement and Provisioning

Procurement and provisioning provides users with a short, simple, pain-free process to select new or changed equipment and plans. Once selected, TCS provides all carrier interaction, policy compliance, and procurement approval process compliance:

- Web portal containing client-specific plans and devices.
- Email order status communication and post-order follow-up.
- Full carrier interaction for procurement and provisioning of devices.
- Enforcement of client wireless purchasing policy.
- Enforcement of client carrier device and plan options.
- Purchasing approval compliance.
- Integration with request ticketing system.
- Data upload to client Enterprise Resource Planning (ERP) or financial purchasing module as required.

- Content maintenance of procurement portal.
- Customized PDA and smartphone provisioning process (options include setup, initial synchronization, application installation, and training).

2.1.3.8. Mobile Rate Plan Optimization

TCS' Rate Plan Analysis technologies have set the standard for the wireless industry over the past 15 years, and have continued to evolve as the best of breed for saving significant agency money.

Three to six months of historical billing establishes a baseline average for individual and group usage agency-wide. Using the specific needs of an organization and established functional, operational, and financial goals for the project, TCS can process this information through its rating engine to formulate its recommendations.

TCS' rating engine algorithms incorporate all imaginable aspects of wireless usage to arrive at a set of rate plans, both pooled and stand-alone, which will save money, regardless of carrier, on a per-line basis and accumulatively for hundreds or thousands of lines agency-wide.

- TCS' analytic software tools evaluate both voice and data lines for all rate plans, whether pooled, flat, or stand-alone, and report alternative choices.
- TCS' rate plan analysis results usually report agency-wide savings from 30 to 50 percent, which amounts to significant reduction in wireless spending.
- TCS' analytic software tools evaluate local and national plans, split lines, and usage by city or region.
- TCS' rate engine has evolved to address complex requirements of very large and diverse corporations and provide insight into enterprise-wide wireless spending, and savings through optimization.
- TCS' analytic tools provide comprehensive reports that are sufficiently detailed for carriers to change rate plans on a per-line basis. The tools also provide diagnostic overviews of all wireless activity involving all carriers.

TCS will provide a NetChange Report, which will provide a detailed and summary view of costs, savings, and usage levels for wireless activities for new, disconnected, and continued lines by category. This objective trending report is highly valued by upper management and telecom managers alike because it identifies agency-wide wireless trends, zero usage lines, and incorrect discounts, and also tracks rate plan changes to grade predicted savings levels.

TCS offers a comprehensive reporting system that is sufficiently detailed for carriers to change rate plans on a per-line basis and provide diagnostic overviews of all wireless activity involving all carriers.

This reporting system:

- Provides management with a status report of wireless devices.
- Shows the change in costs, usage, and lines month to month.
- Is used by the company and the carrier to track any changes.
- Is used by C-level management to show overall status.
- Is used by IT departments to validate and explain monthly billing.
- Validates estimated savings, which can be completed in three months.
- Tracks and resolves billing errors.
- Establishes controls and monitors compliance by cost center.
- Shows the cost/minute and cost/line by new and active employees.

2.1.3.9. TCS Wireless TEM Services – Features, Advantages, Motives, and Benefits

Features	Advantages	Motives	Benefits
What the Solution Has:	**What the Features Offer the Customer:**	**What Customer Motives the Features Satisfy:**	**How Features Benefit the Customer:**
Customized User Portal	• Accessible anytime, anywhere • Ease of use for telecom staff and end-users • Built-in enforcement of mobile policies • Access to all applicable capabilities • Ease of ordering service and devices • Ease of reporting troubles • Ease of viewing usage • Ease of viewing expenses	• Imbedded policy enforcement • Easy to manage mobile phones and service • End-users empowered to manage their mobile phones and service • Improves customer satisfaction	• Administrators have an easy way to access tools they need to manage mobility • Web-based portal is available whenever and wherever needed • Easy to get support • Intuitive so that even the occasional user doesn't get frustrated

Features	Advantages	Motives	Benefits
What the Solution Has:	**What the Features Offer the Customer:**	**What Customer Motives the Features Satisfy:**	**How Features Benefit the Customer:**
Customer Support Center	• Single place to report problems • Single place to order equipment or service • Single place to manage accounts • Manage troubles from report to resolution • Manage procurement from request to delivery • Uses knowledge of customer to serve as customer advocate • Accessible via portal, email, or phone • Incident system to track trouble reporting and procurement service levels	• Enhances support levels for mobile end-users without burdening existing IT staff • Extends hours of support without extending staff • Accurate reporting and tracking of trouble resolution and procurement • Manages complexity internally and externally • Knowledge of customer and environment • Published and proven performance measurements	• Simple, efficient way to resolve problems with mobile devices • Simple way to consolidate procurement for mobility • Simple, common process for trouble reporting and procurement requests • User chooses access method
Procurement	• Manage orders of devices, accessories, and service plans • Purchase via predefined process from approved vendors and providers • Manage from request to delivery	• Orders filled following client-defined policies and procedures • Simplifies ordering process • Limits endless number of devices and plans in the enterprise	• Users get the phones and plans they need for their jobs • Enterprise gets control over mobility
Purchasing Policy Enforcement	• Procurement follows pre-defined process from approved vendors and providers • Predefined availability of specific equipment and service plans for job functions and level in organization	• Orders filled following company-defined policies and procedures • Reduces number of device types used • Reduces complexity in number of carriers and plans	• Users get the phones and plans they need for their jobs • Enterprise gets control over mobility
Customizable Interfaces: • Cost coding • Organization coding • Contracts • A/P • G/L	• Predefined protocols for electronic interfaces	• Quicker integration within the enterprise	• Increased speed of data availability • Increased accuracy of data

Features	Advantages	Motives	Benefits
What the Solution Has:	**What the Features Offer the Customer:**	**What Customer Motives the Features Satisfy:**	**How Features Benefit the Customer:**
Inventory Management	• Establishes baseline mobile inventory of devices, accessories, and service plans • Updates inventory as it evolves • Ensures payment for what is actually being used	• Improved visibility into current mobile landscape • Understand inventory levels going forward • Pay for what is actually used	• Enterprises now know what they are paying for and what each user is using for mobility
Invoice Management	• Manages mobile spend for equipment and service • Prepares invoices for payment by enterprise • Tracks invoices and verify correctness of invoices • Ensures timely payment of invoices	• Get control of mobile expenses • Pay for what is actually used • Reduce late charges • Reconcile billing discrepancies	• Accurate payment of invoices • Pay on time to avoid penalties and service interruption • Focus on service, not billing issues
Rate Plan Analysis	• Evaluates rate plans for all carriers, internationally • Optimizes both voice and data • Covers all types of rate plans and usage types • Optimizes to overall effective rate per minute, not individual least cost • Implements approved recommendations • Monthly and periodic analysis available • Comprehensive reporting package • Scenario and planning support	• Saves significant money by matching usage to available carrier offers • Establishes wireless stability and overage avoidance • Enables clear decisions in mobile usage and purchasing policy, plan management, and contract negotiations • Implements approved changes to ensure savings are achieved • Provides ongoing guidance and trending through extensive and comprehensive reporting	• Average of $242 per optimized device saved annually; 10% annual reductions in effective rate per minute with monthly management • Provides corporate-wide governance and savings • Goes beyond just rates into plan structure and strategy • Proactive management through significant “what-if” capabilities • Identifies actionable opportunities within the boundaries set by the company

Features	Advantages	Motives	Benefits
What the Solution Has:	**What the Features Offer the Customer:**	**What Customer Motives the Features Satisfy:**	**How Features Benefit the Customer:**
Mobile Reporting	• Full set of reports to track mobile usage • Full set of reports to track mobile spending • Full set of reports to view mobile inventory – equipment and service plans • Mobile-specific reports such as top 10 users, zero users, top dialed numbers • Mobile dashboard	• Slow demand by reducing abuse and fraud • Look for cost reduction opportunities • Identify unused or low-use devices • Justify growing mobile spending	• Information available on demand • Visibility into critical component of corporate communications landscape

2.1.4. Integrated MDM and TEM Benefits for FirstNet Users

An integrated MDM and TEM solution will produce tangible benefits toward FNN adoption and utilization. Such a solution:

- Enables agency adoption of a mobility workforce by providing tools for mobile device management.
- Enforces mobile security, compliance, and Data Loss Prevention (DLP).
- Implements a secure way to distribute and access confidential documents.
- Ensures protected sites are accessed through a secure VPN tunnel.
- Implements a scalable solution to support a growing mobile deployment.
- Adopts a flexible platform that supports corporate devices and BYOD programs.
- Reduces cost barriers as well as monitors and optimizes costs across all LTE networks.

2.2. Mobile Application Framework

With the emergence of intelligent mobile devices powered by flexible operating systems, applications have emerged as the differentiator. The applications make the difference between enabling a productive mobile workforce or merely a frustrated workforce. PSBN users will require dedicated applications with specific emphasis in the areas of privacy, security, and reliability.

TCS does not attempt to recognize all the possible applications for use by PSBN users. Rather, TCS believes that it is more important to enable a secure framework for delivery of user services which cannot be predicted at this time. TCS recommends that the FNN authority enable a framework designed to facilitate:

- *OTT Application Services* - Seamless user experience for services across devices and networks
- *MAM* - Secure application delivery system through policies and technology
- *Trusted and Verified Applications*
    - Encourage application development
    - Offer secure applications
    - Offer verified applications
- *QoS Management* - Reliability and preferential treatment

2.2.1. OTT Application Services

Until recently, the only way to deliver applications over wireless networks was to use the conventional method of operator-offered applications. This resulted in higher application costs, reduced interoperability (applications would work over some phones but not others, or in home networks but not while roaming), and delays in getting compelling and innovative applications to the market. Two recent trends have changed this model completely:

- Easy, convenient, and economical availability of wireless broadband (e.g., Wi-Fi, 3G, and 4G), facilitating easy access to the internet.
- The emergence of smartphones and their application stores, permitting application providers to bypass operators and users to install applications of their choice.

This has resulted in an alternative application delivery architecture often referred to as the OTT model. In the OTT model, the operator wireless network primarily provides data connectivity, while applications are facilitated via software on the smartphone and an application core in the network cloud. A significant benefit of OTT is the independence of applications, network, and device.

TCS recommends this as an ideal model for supporting PSBN users. This approach will encourage specific purpose-built applications designed for the FirstNet user community.

2.2.1.1. OTT Application Benefits for FirstNet Users

The specific benefits that can be realized by FNN users through adoption and use of OTT-styled services include:

- Enabling the mission of FirstNet users by delivering secure and specialized applications.
- Allowing agencies to utilize only the applications that benefit them.
- Encouraging industry and agency participation to solve FNN-specific mobility challenges.
- Applications that are more cost effective than the traditional network integration model for user services.
- Applications that can be integrated with QoS requirements for use across all networks.
- Seamless operation and user experience across diverse networks and devices.

2.2.2. Mobile Application Management

Utilization of OTT application services will enable agencies to efficiently fulfill their primary objectives through the use of specialized applications. However, to enable agency adoption of approved OTT applications, the PSBN should utilize a framework for delivering those applications to user devices. TCS recommends the MAM, which is an ideal mechanism for categorizing and distributing PSBN application services. A MAM will consist of two primary functions: administrative policies and application stores. Together, these technologies facilitate application services delivery to all appropriate users.

2.2.2.1. TCS Mobile Application Management

The TCS MAM solution enables an organization to manage internal, public, and purchased apps across employee, corporate, or shared devices. TCS' Enterprise App Catalog provides the ability to distribute, track, update, and secure enterprise applications over the air. TCS offers the most complete offering in this area by providing access to software updates and public and enterprise app stores, with the ability to blacklist and whitelist applications.

Administration	• Create a customized, branded Enterprise App Catalog where users can view, install, and update apps. • Manage and deploy apps based on user groups with unique requirements and access. • Define advanced distribution rules selecting eligible devices based on both inclusion and exclusion criteria. • Enforce the installation of required applications.
Distribution	• Automatically install apps during enrollment or allow users to install apps on-demand from the App Catalog. • Integrate with public app stores, like the Apple App Store and Google Play Store, to distribute public apps. • Integrate with Apple's Volume Purchase Program to provide purchased business apps.

Security	• Authenticate users before allowing them to view and download internal apps. • Limit access to the Enterprise App Catalog based on user role or device function. • Enforce application compliance through custom groups of blacklisted or whitelisted apps. • Restrict access to pre-installed apps on a device and control installation of publicly available apps. • Monitor and enforce device compliance with corporate application policies. • Prevent data backup and automatically remove apps on unenrollment from TCS' solution.
Tracking	• Track and view installed/approved/blacklisted applications at the device/user level. • Receive instant alerts when an end user has installed an unapproved app. • Generate application inventory, version history, and compliance reports.
Versions	• Deploy and manage multiple concurrent versions of the same internal app. • Assign different app versions to different device groups simultaneously. • Allow devices to "roll back" to a previous version.
Management	• Install, update, and remove managed apps from a device remotely. • Delegate authority to IT managers responsible for specific apps or users within the system. • Disable access and remove corporate apps if an end-user leaves or loses his device. • Remotely manage application settings on supported apps through Application Profiles.
MAM Benefits	• Centralize management of internal, public, and purchased applications. • Secure applications with integrated MDM and MAM management. • Enhance the user mobile experience with a customized app catalog. • Ensure that security objectives are achieved through advanced app distribution. • Enhance mobile strategy by understanding how apps are being used. • Leverage TCS SDKs to integrate MDM and MAM features into custom apps.

2.2.3. Trusted and Verified Applications

A mobile application framework contains an entire ecosystem of tools, policies, and expertise to enable the OTT services' development, delivery, and utilization. The PSBN MAM should be populated with only trusted applications as defined for nationwide or agency-specific use. Applications must be assessed for a security posture and validated to enable the first responder mission while minimizing the risk for privacy or security compromise. Applications developed for the consumer may not be of sufficient rigor to withstand the operating, privacy, and security conditions of PSBN users. The industry-leading application stores employ security and privacy checks specific for consumer use. TCS recommends an industry-specific approach that addresses the needs of the first responder community.

2.2.3.1. TCS Trusted Ecosystem

TCS provides a trusted ecosystem for secure mobile applications. This includes penetration testing of the network components, delivery system, and application store, but more importantly the applications (app and server) go through rigorous testing to be validated as "TCS Trusted."

A TCS trusted application is one in which:

- The app is free of known malicious code or software such as malware, including but not limited to viruses, worms, Trojan horses, spyware, adware, rootkits, backdoors, keystroke loggers, and/or botnets.
- A scan of the app using scanning software does not reveal any known malicious code or software objects.
- A penetration test has validated items that may have been vulnerabilities in scanning and has confirmed the vulnerability or proved it is not vulnerable.
- The app owner ensures that the app's security procedures comply at all times with generally recognized industry best practices and are explained or made available to users.
- If the app collects, stores, or transmits any personally identifiable information (PII), such information is collected, stored, and transmitted using a secure protocol via one or more industry-accepted methods for guarding against identity theft.

TCS assesses an application by execution the following methodology:

- Evaluating the source and executable code for malware, virus signatures, and obfuscated sources.
- Generating a threat model of the application for potential areas of vulnerability and using this to guide the test strategy.
- Developing a test strategy and executing a vulnerability test suite based on threat and risk models.
- Completing specific tests, including code-based fault injection, penetration/abuse cases, trust boundaries mapping, and code review (manual, static, dynamic).

TCS also offers remediation services to development teams, because often the development teams have not been trained and do not have an understanding of the issues. Penetration testing will highlight Structured Query Language (SQL) injection, cross-site scripting (XSS), or buffer overflows, but the developer might not know how to go about finding the code, tracing the issue, or resolving the vulnerability. TCS can find the vulnerabilities in the code, recommend resolution of the issues in the code, and work with the developer to verify via testing that the code has been corrected and the vulnerabilities no longer exist.

2.2.3.2. Trusted and Verified Application Benefits for FirstNet Users

Trusted and verified applications will enable the mission of the first responder community. The following tangible benefits can be realized through an application verification framework:

- Custom and commercial applications undergo validation procedures prior to publishing in the FNN MAS.
- First responder security and privacy postures can be validated against FNN-approved applications.
- Device compromise reduced by specifically checking for presence of malware and malicious code.
- The "who to trust" problem is eliminated when working with OTT applications in MAM solutions.
- Publicized application framework, which includes submission and approval methodologies, encourages industry participation and submission to an FNN MAS.

2.2.4. Grade of Service

Wireless networks based on new standards like LTE provide control mechanisms for both priority service (the ability to pre-empt other users) and QoS. These are crucial to achieving mission-critical grade of service, especially when the applications are used over commercial networks in a congested state. TCS' proposed solution uses the LTE standard mechanisms described below to implement required service quality and priority.

- *Access Classes (ACs)* – During national security/emergency preparedness (NS/EP) events, it is desirable to prevent overload of access channels for the network and permit at least high priority users to get through. This is accomplished via AC control based on ACs assigned to mobile users at subscription time. Certain AC values (11-15) are set aside for high-priority users.
- *Allocation Retention Priority (ARP)* – ARP indicates the priority of allocation and retention of network resources assigned to a user during contention and congestion. It contains information about the priority level (1-15), the preemption capability (Y/N), and the preemption vulnerability (Y/N). The priority level information is used to ensure that the network resource request with the higher priority level is preferred. The pre-emption information is used during times of resource contention and congestion to determine whether a higher priority request can preempt resources associated with a lower priority request, and if so, which ones.
- *Packet Forwarding Treatment* – The aforementioned parameters only affect the admission and processing of a new resource request. Once the network resources have been assigned for a request, the packet forwarding and handling treatment (e.g., scheduling weights, admission thresholds, queue management thresholds, Differentiated Services Code Point [DSCP] setting) is controlled by setting the following parameters:

- *QoS Class Indicator (QCI)*[1] – This is a scalar with values ranges from 1 to 9 that maps to value ranges for the following performance parameters:
  - Resource Type (Guaranteed Bit Rate [GBR] or non-GBR)
  - Priority
  - Packet Delay Budget
  - Packet Error Loss Rate
- *Bit Rate Thresholds* – Depending upon the type of bearer (GBR or non-GBR), various bit rate thresholds control the total amount of traffic that is allowed to pass through per mobile user, per mobile user per bearer, and per mobile user to a specific data network. These affect the bandwidth reservation and also determine the traffic/rate shaping functions that result in excess traffic being discarded.

OTT applications do not benefit from these mechanisms unless there is integration with the carrier networks to influence the same. Without such integration, the OTT application data will only receive best effort QoS over wireless networks, which will prevent the applications from obtaining the desired grade of service over commercial wireless networks, especially during times of disaster when networks are heavily congested.

Some of the parameters discussed above, like the AC, user, and packet network specific bit rate thresholds, are more static in nature and could be specified at FNN user subscription time. Others, like QCI, ARP, and bit rate threshold for a GBR bearer, are more dynamic in nature. While these also could be configured in a static manner, they would need to be supported by complex network design and strong coupling between their settings and the FNN data network architecture. This is not operationally desirable.

[1] Table 6.1.7 in 3GPP TR 23.203 makes recommendations in this context on QCI settings per service type (e.g., QCI=2 for live video; QCI=6 for buffered video).

2.2.4.1. TCS Quality of Service Server

For this reason, TCS recommends an architecture that includes a QoS server within the FNN data centers as shown in Exhibit 4. The QoS server integrates with FNN services on the one side and with multiple commercial carrier networks on the other via the Policy Charging and Rules Function (PCRF). The PCRF function exposes a Diameter Rx protocol interface for applications to request QoS assignments. The PCRF function expects session and media details from the QoS server that can be validated against existing PCRF provisioned policy. Subsequent to PCRF validation, it can issue assignment of QCI values to the requested services. The QoS server dynamically provides the grade of service impacting parameters to the PCRF on a per user basis for active services that the FNN user traffic might transit. TCS' own applications proposed in this Request for Information (RFI) response are developed to benefit from the capabilities offered by this QoS server.

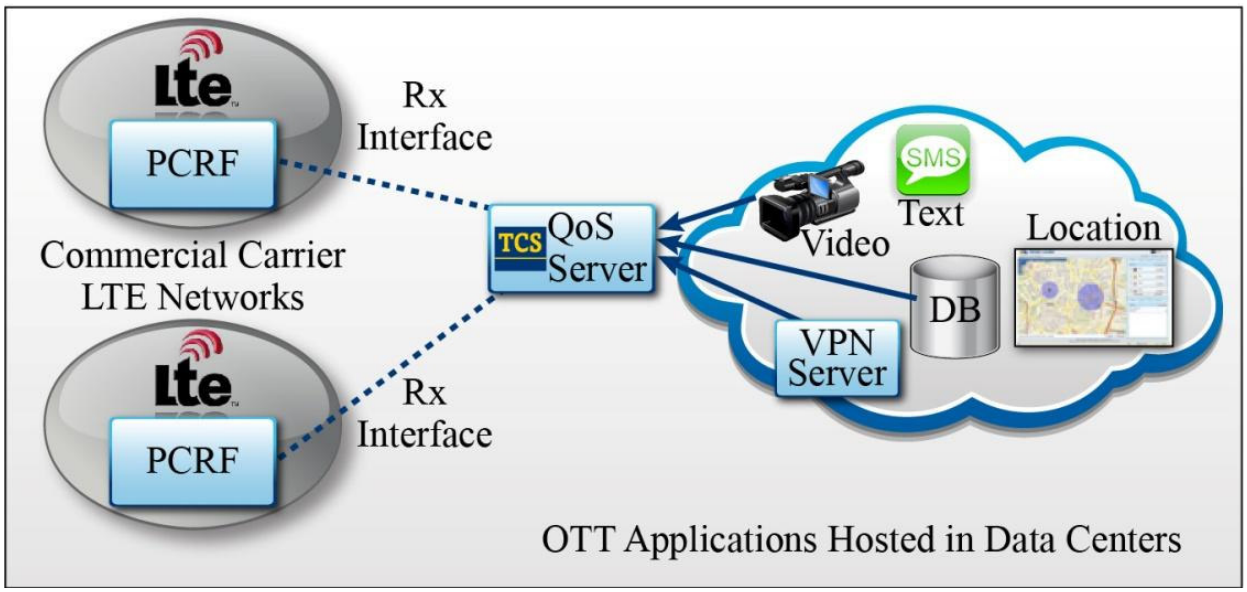


Exhibit 4. TCS-Recommended QoS-Enabling Architecture for Applications

2.2.4.2. QoS Benefits and Challenges

In support of TCS' recommended approaches, we have identified three major factors that enable the FNN to provide services to end-users.

First, there is the emergence of OTT applications, which is mainly driven by higher bandwidth and more capable smartphones and tablets. This trend is expected to naturally accelerate as mobile devices become the most popular computing devices.

Second, the OTT application market is mostly built upon noncritical services delivery. In order to deliver critical services, operators must enhance their commercial plans and support the introduction of new plan offerings based upon priority and preferential treatment options.

Third, OTT applications are designed to be operator agnostic, working over multiple broadband facilities. However, OTT applications used for critical services should be assigned appropriate priority and preferential treatment.

To facilitate the QoS, TCS recommends using a QoS server to integrate with multiple operator networks and multiple OTT applications. This would have the following benefits:

- Centralized operation, planning, and management through a cloud-based offering.
- An approach that complies with Third Generation Partnership Project (3GPP) standards.
- Extended coverage with diversity and resiliency (Wi-Fi, 3G, 4G, field deployable systems).
- Consistent user experience for both normal and priority services across all access pathways.
- Authenticated and secured user communications.
- Common mobile/tablet device support.
- Consistent approach to priority and preferential treatment for multiple access technologies and commercial cellular networks.
- Independent of operator wireless evolution path.
- Facilitates next generation of Wireless Priority Services (WPS).
- Leverages emerging commercial mobile development trends to provide new applications and services for the NS/EP mission.

Currently, commercial operators do not offer QoS-based mobile data plans. Although this suggested approach for critical services is not new, operators have been hesitant to implement it. Many cellular market analysts believe it is a matter of when, not if, these plans will emerge as mobile offerings. However, TCS recommends FirstNet work with commercial operators to drive these mobile offerings and expose their PCRF to FNN for an integrated QoS approach across all networks.

3.0 PUBLIC SAFETY ACCESS NETWORK DIVERSITY

To provide extended and reliable coverage for FNN users, a FirstNet access architecture must employ access diversity as a holistic approach. For instance, this approach should include device access to the Radio Access Network (RAN) and application services delivered to end-users. For this project, TCS recommends the use of all major operators (AT&T, Verizon Wireless, and Sprint) for LTE spectrum to extend nationwide access for FNN LTE users. In addition, approved Wi-Fi profiles, controlled via an enterprise management solution, could be leveraged by an OTT application to increase access where commercial networks are unavailable or not preferred.

However, in some instances reliance on commercial MNOs may not be sufficient. From a technological or strategic standpoint, the FNN authority may deem certain buildings, locations, or operating scenarios as too important to fail. TCS recommends that the access diversity proposed by the FNN authority is augmented by two additional considerations.

1. For operational scenarios involving outage, lack of coverage, or additional capacity requiring fast deployment, TCS recommends the use of rapidly deployable LTE solutions. These solutions can operate independently of the broader LTE network and interconnect to the larger FNN when interconnection is available, which provides specific advantages to Cellular on Wheels (COW) systems. A COW system is meant to augment an existing network coverage and must have interconnectivity back to the parent network to provide service.
2. Specific building and campuses may be deemed ahead-of-time strategic locations for native LTE FNN service. In these situations, a high volume of users, building design, and underground locations may prevent FNN LTE service. For these specifically high-value locations, TCS recommends the implementation of campus or IBW solutions.

TCS provides solutions that solve these problems where the difference means lives are saved. TCS has an entire line of rapidly deployable communication solutions which are designed to augment an FNN architecture. In addition, TCS' IBW solutions bring cellular and radio signals from the outside the structure and distribute them throughout the building so there is no loss of communication when using cellular and radio devices within the building.

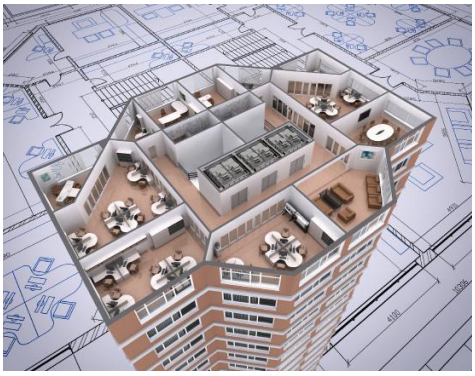
3.1. TCS SwiftCell – Deployable LTE Communications

All U.S.-based wireless carriers currently have coverage gaps in rural areas throughout the nation. In addition to these gaps, there are substantial gaps across the southern and northern continental U.S. borders. In some rural and border markets where coverage does exist, the network capability is normally limited to 2G-based services. These localized networks are designed for limited data use and a small number of users. As a result, there is a reasonable probability that localized demands by FNN on these reduced-capacity networks could overwhelm them. In turn, these localized networks could develop significant latency and restricted data use, producing a bottleneck and prohibiting the delivery of critical information for in-field FNN personnel.

TCS develops multiple deployable communication platforms that can be leveraged to alleviate instances of no coverage or limited coverage using wireless mobile LTE/Wi-Fi devices. TCS offers a full suite of deployable communication systems, including Very Small Aperture Terminals (VSATs), Broadband Global Area Network (BGAN), deployable wireless, and LTE. In support of FNN architecture, TCS recommends using a deployable full LTE network operating in the FNN licensed spectrum. The TCS deployable LTE (SwiftCell™) system will interconnect with the larger FNN LTE network as a roaming network. Alternatively, the TCS SwiftCell will operate as a fully functioning stand-alone entity when interconnectivity is unavailable. Quickly deployed into a remote operating environment, a TCS SwiftCell system can interconnect from the field through a variety of TCS-offered secure connectivity options, including Line of Sight (LoS), Tactical Transportable Troposcatter (3T), or satellite.

3.2. TCS IBW Solution Overview

Wireless technology has become the primary communications method in public venues and commercial buildings for both personal communication and first responder services. As wireless penetration rates approach and exceed 100 percent, users demand that their wireless connected electronic devices work just as effectively indoors as they do outdoors. First responders also require reliable, ubiquitous radio coverage to ensure the safety of the public as well as themselves in emergency situations. TCS' IBW solution provides the products and services to address these complex challenges.



TCS delivers IBW coverage solutions that enable flexible and secure communications inside structures where radio frequency (RF) signals do not penetrate or are interrupted. TCS designs, installs, and services carrier-certified IBW solutions. TCS' customers receive the highest quality engineering and equipment available and are ensured reliability, quality, and optimum performance. As a systems integration company, TCS starts all solutions with a definition of customer need and requirements analysis. The company leverages its knowledge of wireless technologies, expertise on how to implement the technologies, and commitment to solving the customer's problems.

3.2.1. TCS IBW Capabilities

The TCS IBW offering is a fully developed, multicarrier wireless solution engineered for flexible solutions of all sizes. Its key features and capabilities include:

- Extends wireless coverage into buildings.
- Extends cellular coverage (2G, 3G, 4G) from 698 MHz to 2,700 MHz.
- Provides FNN coverage.
- Provides Land Mobile Radio (LMR) coverage (first responders).
- Provides pager coverage (SkyTel, USA Mobility).
- Provides Wireless Local Area Network coverage (WLAN/Wi-Fi).

- Provides enhanced location service for emergency response.
- Design, install, test, commission, operations and maintenance, and warranty.

3.2.2. TCS Wi-Fi Offerings

TCS provides integrated Wi-Fi solutions manufactured through its partners. TCS engineers analyze the technical specifications and conduct on-site verification to engineer a solution that allows governments and enterprises to consolidate multiple services within the same access points. A TCS Wi-Fi solution also allows mobile users to operate in locations that support untethered communications capabilities, and allows users to move from one wireless access point to another seamlessly, without session loss or the need to log in to the new access point. After analysis, TCS engineers evaluate the various wireless offerings to select the most appropriate technical solution. In order to provide the best possible solution for the customer, TCS' established Supply Chain Management (SCM) process thoroughly qualifies the vendor. The TCS SCM process allows the company to draw upon its many partners, which are Wi-Fi Alliance, VeriSign PCI, FIPS 140-2, and ISO 9001 certified. TCS' partners offer innovative system designs, data processing, and radio engineering to provide unique and flexible capabilities. As a result, TCS can select the best possible components and maintenance solutions to form an end-to-end solution which meets or exceeds the specific demands of each operating environment.

3.3. IBW and Deployable LTE Benefits

The use of IBW and rapidly deployable LTE systems provides increased diversity of access and augments the network capacity to fulfill the first responders' mission. Benefits of TCS' IBW solution include:

- Dedicated FNN-specific coverage in high-value buildings and facilities.
- Integration with the FirstNet design approach using diverse methodologies and networks to provide ubiquitous nationwide access.
- Approved Wi-Fi networks can affordably augment FNN access.
- Deployable LTE systems that can interconnect to the broader FNN or act as a stand-alone miniature FNN.
- Rapidly deployable LTE methodology supports critical rapid response operations, supplementing network coverage or outages.
- The use of IBW and deployable LTE solutions provides cost-effective and critical enhancements to FNN access diversity approaches.

4.0 CONCLUSION

FirstNet has an unprecedented opportunity to be the nationwide wireless service provider to the U.S. first responder community and its respective public safety organizations. To fulfill this mission, it is important that the FNN leverage the combined efforts of the public sector and the commercial wireless industry.

Through this response, TCS has highlighted the challenges, recommendations, and solutions it offers to make FNN operational in a timely fashion. A comprehensive, FNN-managed, multitenant model for device management, application management, services, security, and cost control through an enterprise mobility management solution will reduce the operational management and cost barrier for adoption by public safety agencies. A mobile application framework supported by verified and trusted OTT applications that are capable of achieving desired QoS from underlying transport networks will increase the breadth of mission-critical public safety applications that can be offered to public safety users. Access network diversity augmented by rapidly deployable LTE networks and IBW solutions for high-value locations will ensure economically viable, high-quality network coverage wherever it is required. Addressing these issues is critical to the success of FNN, both in terms of readiness and being able to offer a compelling differentiator to the legacy networks and applications currently used by public safety agencies.

TCS already has extensive experience offering thought leadership, products, and services to the public safety community. TCS looks forward to working closely with FirstNet to make a nationwide public safety broadband network for first responders and public safety users a reality.