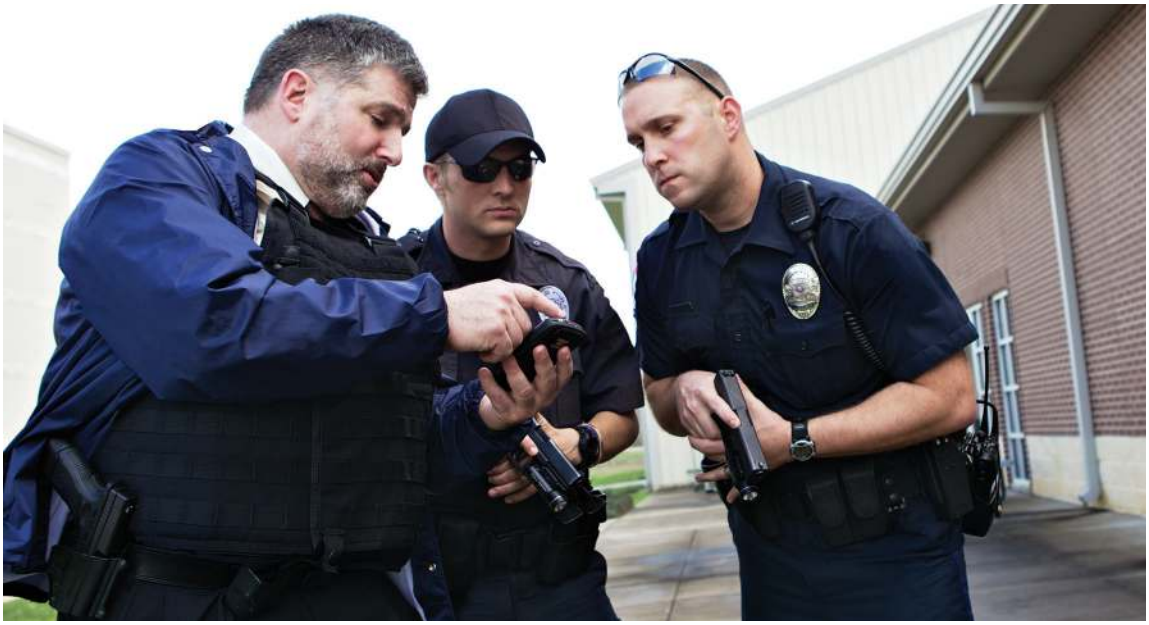
LTE DEVICE MANAGEMENT: WHAT YOU NEED TO KNOW

MOTOROLA

As state, local and federal public safety agencies prepare for the transition to powerful new LTE mobile devices, there can be more questions than answers. There's no question about the importance of these devices. In a public safety environment, the benefits of high-speed broadband communications are entirely delivered through the innovative mobile devices and applications that are used in both everyday and life-and-death situations.



The questions come as you plan and design your LTE system – whether at the local, regional, state, federal or national level. As part of your role as CIO; you've transitioned into a network provider as well. It's essential that you recognize from the outset that you're going to be deploying – and managing – a large number of mobile devices and applications. The question is how will you most effectively accomplish this?

TOP-OF-MIND CHALLENGES

The importance of mobile devices – from smartphones to handheld computers to laptops to tablets – raises a number of questions CIOs are having to ask themselves. Who should have access to the network with a mobile device? What kinds of devices should they have? What are the features they'll need? What kinds of applications should be on their devices? How will you make sure applications and data will be secure?

These are critical questions for sure, but one question that's as crucial as any is also one that is likely to be overlooked. How will you manage your portfolio of hundreds, even thousands of devices? How will you track and update and repair and deliver the right units in the right working order to the right people at the right time?

DEVICE MANAGEMENT OPTIONS

As the public safety industry relies more and more on LTE systems, state, local and federal agencies of all sizes are recognizing the importance of managing mobile devices and applications. Due to the complexity of the LTE network environment, and the rapid pace of change in mobile technologies, devices and applications, this is no simple endeavor. Some agencies will be confident that they have the resources and the expertise to manage and track their device portfolio internally. Others are looking to outsource solutions to both streamline management of devices and software and to reduce management and operational costs.

A LIFECYCLE APPROACH

Whether you choose to manage your LTE devices internally or decide to engage a third-party services organization, you should consider taking a comprehensive lifecycle approach to device management. This approach helps ensure that devices and applications deliver maximum performance – and ROI – throughout their useful lifecycles from deployment to replacement. As your organization explores your mobility management options, whether you choose to go it alone or decide to work with a services provider partner, there are a number of vital questions to ask.

HOW WILL YOU MANAGE AND CONTROL YOUR NEW FLEET OF IP-ENABLED DEVICES?

While many organizations are familiar with management of land mobile radio (LMR) and cellular devices, deploying LTE for public safety use presents larger and more complex management challenges. You'll need to manage and control an expanding fleet of devices, including smartphones, laptops, ruggedized handheld computers and new devices like tablets. Start by developing a mobility strategy that lets you track, monitor and maintain a wide variety of devices, technologies and applications from multiple vendors. Due to the fast pace of innovation, your strategy must also allow you to leverage the innovative new technologies and devices that are on the horizon.

HOW WILL YOU ENABLE INNOVATIVE NEW APPLICATIONS?

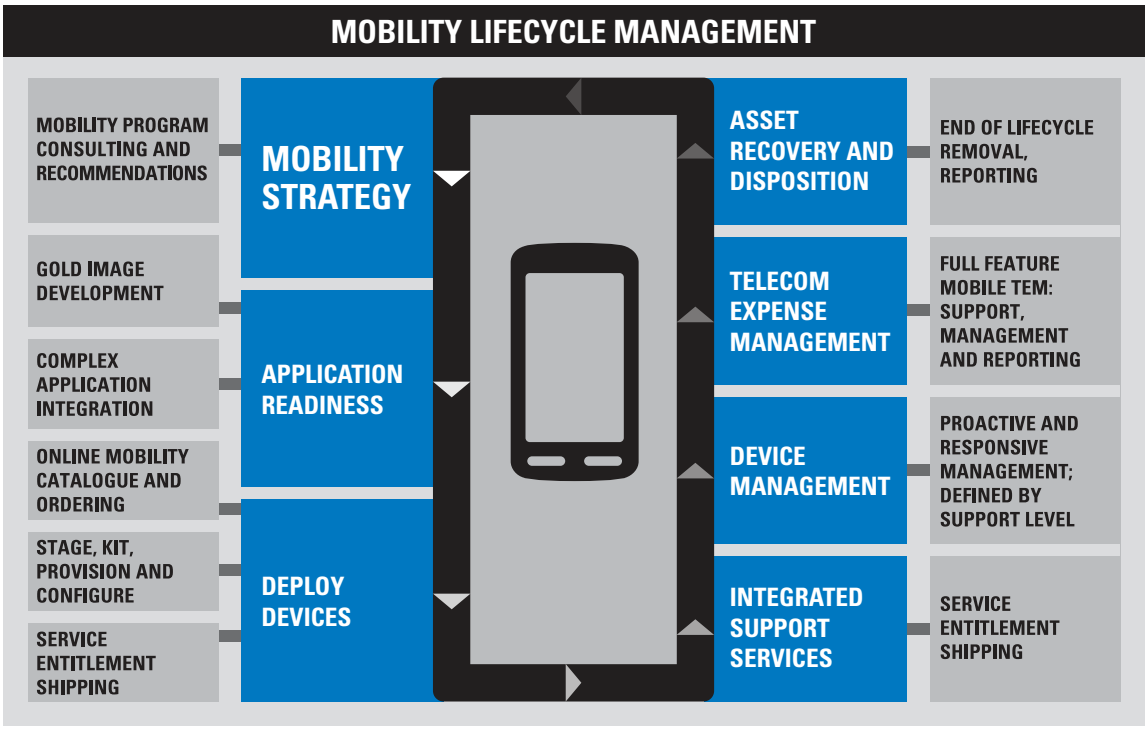
Applications – from streaming video to automated license plate recognition to e-ticketing to biometrics and many more – are key to first responder effectiveness, efficiency and safety. You need an application management strategy that includes a migration path for current applications to LTE devices; and that ensures that applications meet performance goals, are up-to-date with the latest OS patches, software updates and security enhancements, and work consistently across multiple devices. You need to develop a testing strategy to make certain your applications and devices are ready for deployment in mission critical environments. And you need a plan that helps you ensure device security, interoperability and data integrity.

HOW WILL YOU PROVIDE SUPPORT FOR YOUR MOBILE DEVICES?

While executing your mission, ensuring that your mobile devices meet your performance and reliability goals is essential. You must create a strong support strategy based on expertise in hardware repair and replacement, software upgrades and patches with technical and application support such as 24/7/365 help desk and first echelon services. You should consider having a hardware maintenance plan (HMP), software maintenance plan (SMP) or both. To keep devices working at peak performance levels, you should also implement a full reporting and analysis functionality plan.

HOW WILL YOU KEEP MOBILE DEVICES AND DATA SECURE?

As you plan your overall system mobile security strategy, you need to ensure the devices themselves and the data they store for evidentiary purposes and transfer to long-term storage are locked down. This means you must be able to control access to the devices – and the information they hold – by means of secure passwords and authentication control strategies and by choosing the optimum level of encryption to protect your data. You also need a plan for addressing devices that are lost or stolen, including remote deactivation and wiping of data to keep sensitive information from winding up in the wrong hands.



HOW DO YOU ENABLE MOBILE ACCESS OUTSIDE YOUR COVERAGE AREA?

In the public safety LTE world, first responders and other mobile personnel, such as state, local and federal agencies, must have network access even when they travel beyond your coverage area. You need to streamline activating and provisioning of each device for the various networks it may be utilizing, including private LTE networks, carrier networks and Wi-Fi networks. You need to make sure services agreements are in place between different agencies and carriers, so that when a first responder reaches for the network it is always there.

HOW WILL YOU MANAGE YOUR TELECOM EXPENSES?

As LTE systems are increasingly deployed in state, local and federal public safety environments, the technology will enable increased agency and jurisdictional sharing of networks and access. Crucial to LTE economics and ROI is enhanced visibility into your communications usage and expenses. This data gives you accurate billing information for equitable cost allocation, and enables efficient and timely invoicing procedures. Also key to managing your expenses is an effective reporting function for tracking, analyzing and improving data traffic patterns and usage.

There's no question that LTE mobile devices are poised to be a key driver of next-generation state, local and federal public safety systems. The real question is how CIOs will develop their mobility and device management strategies to ensure that the LTE system's powerful handheld computers and other devices will deliver maximum performance, reliability and ROI. It's a good question.

Motorola Solutions, Inc. 1301 E. Algonquin Road, Schaumburg, Illinois 60196 U.S.A. **motorolasolutions.com/services/government**