SAMSUNG

White Paper:

The Ultimate Law Enforcement Agency Guide to Going Mobile

From In-Vehicle to Handheld

Progressive agencies are beginning to embrace the smartphone, recognizing both its utility and potential to augment, even replace, the traditional car-mounted laptop.

Today's police officers rely on technology more and more to ensure their safety and effectiveness in the field. In addition to providing powerful query access to regional and national databases, in-car computers support mission-essential functions like computer-aided dispatch (CAD), control of video units and automated license plate reader systems.

Traditionally, this level of computing power was only available to personnel with a desktop computer inside a secure police facility. In today's fully-equipped patrol vehicle, a uniformed officer often has access to more powerful technology than their counterparts in the office. Some of the newer and more powerful data systems provide officers with real-time and near-real-time actionable data that can improve situational awareness and, by extension, officer safety.

While in-car computers serve as an incredible information platform, their effectiveness ends once an officer steps outside the vehicle. This puts personnel in a difficult position, since being an effective officer means engaging with the community and leaving their mobile base of operations and the information flows it supports.

On foot, officers that need to check a database must rely on their radio. In-vehicle mobile computers originally came into use because radio systems were overtaxed, and interaction with dispatch meant that two people were needed to conduct even the most basic query.

Handheld mobile technologies are now overcoming the inherent limitations imposed by reliance on in-car computers. Progressive agencies are beginning to embrace the smartphone, recognizing both its utility and potential to augment — and even replace — the traditional car-mounted laptop.

The smartphone, combined with new peripheral technologies, is truly a game-changer for public safety. This paper will inform forward-thinking administrators of mobile's possibilities, and provide an informed and thoughtful discussion of best practices to implement an effective mobile-based information platform.

Today's Opportunities

Although agencies usually utilize smartphones at some level, phones often are only issued to administrators or investigators and are used for basic calling and email functions. That's now changing as some departments realize the significant benefits for field officers.

Smartphones provide practical communications benefits to officers and extend their resources beyond the patrol car. Officer can conduct phone follow-ups with witnesses, contact parents of a detained juvenile or check space availability at a mental health facility, saving time and providing return on investment for departments.

In addition, smartphones can be employed in more sophisticated ways and alongside other technologies, unlocking the door for a wide range of potential applications.

Here's a partial list of what's already available today using a combination of baseline applications and, when needed, attached or wireless peripherals:

- Camera for still image and video capture
- Voice recorder
- Ready resource for department policies and case law notes
- Situational awareness through location services
- Officer under duress alerting (SOS)
- Electronic citations
- Biometrics supporting facial recognition, fingerprint and iris scanning
- Forward Looking Infrared (FLIR) imaging
- Dictated reports
- Language translator
- Pill identification
- Fusion of disparate sensors transmitting real-time data to other field units and command
- Computer-aided dispatch
- License plate recognition
- Two-way radio
- Driver's license scanner and identification card verification

This list is not all inclusive and it's noteworthy that many law enforcement agencies are actively working with application developers to gain new capabilities that better protect the public and improve the safety of officers.

Real World Benefits of Smartphone Technology

Equipping individual deputies with smartphones and peripheral technologies allows for effective deployment and real-time awareness of the relevant factors in an evolving situation.

Sheriff's deputies can serve as a real-life example of applied smartphone technology. Imagine a campground where a hiker is potentially lost. Each deputy is equipped with a commercially available smartphone with relevant law enforcement applications. Because their phones are equipped with their agency's computer-aided dispatch application, deputies already have relevant details, along with a photo of the missing hiker provided by the reporting party. The hiker is diabetic and their extended absence may indicate a medical emergency. It's midday and temperatures are above 100 degrees.

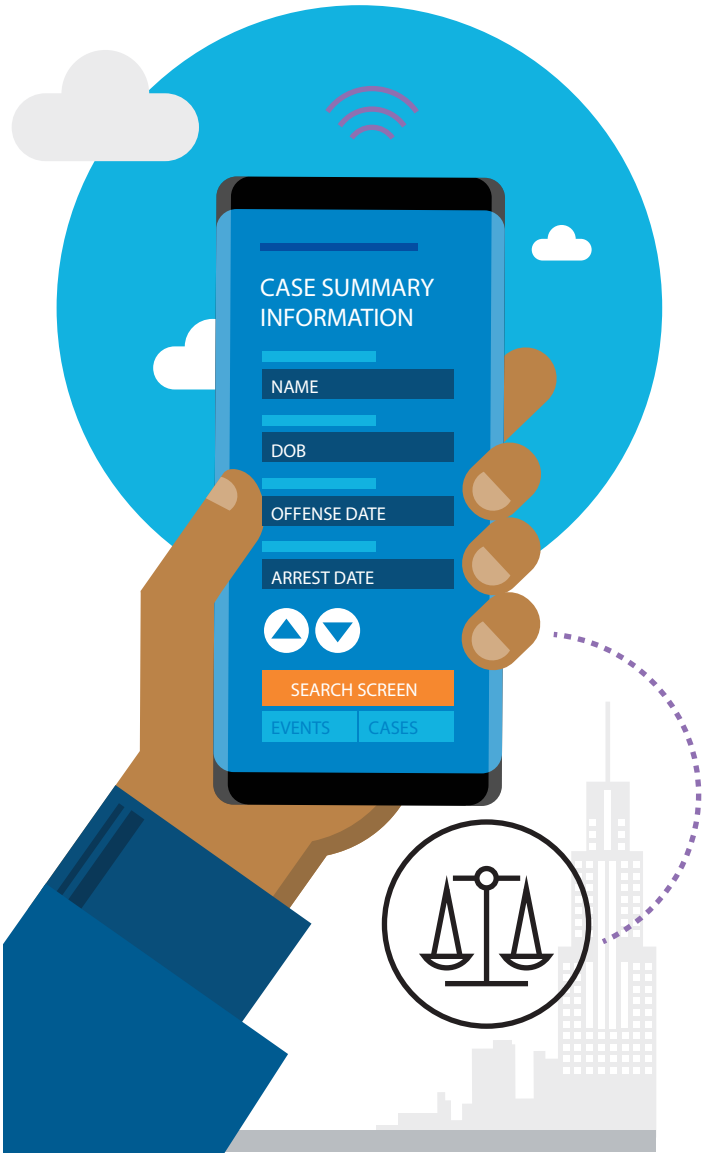
If the lost hiker is located, the smartphones carried by the deputies can determine basic vitals such as pulse rate and oxygen level. If transport of the hiker is needed, exact location can easily be determined even without a notable landmark and other deputies can readily determine their proximity.

If the hiker is not quickly located and the search becomes prolonged, it's important to consider the safety and condition of the individual rescuers. In this case, each deputy is equipped with a basic fitness band which is wirelessly communicating real-time data back to the command post via the smartphone. If pre-established thresholds of body temperature or pulse-rate are reached, an alert is provided to a supervisor who can proactively address the situation and ensure that a rescuer doesn't become a victim. In this scenario, equipping individual deputies with smartphones and peripheral technologies allows for effective deployment and real-time awareness of the relevant factors in an evolving situation.

Planning for Success

If you intend for your smartphones to have full criminal justice query capability, you will need a much higher level of security safeguarding your data transactions because of Criminal Justice Information System (CJIS) requirements.[1]

Modern smartphones offer such a broad and versatile range of benefits to agencies that they have become an essential tool for deployment to all officers. When public safety organizations commit to a mobile strategy for operational transformation, they are making a significant commitment in terms of budget and personnel resources.



The good news is that organizations will reap a return on the investment and, properly planned and managed, the rollout can be done with minimal risk and disruption to daily operations. In fact, a large-scale deployment that is well planned and utilizes effective mobile management tools can require less IT resourcing than a partial initiative that is poorly planned and managed. The following is an approach that has proven effective in many agencies:

Determine the desired outcome

What capabilities do you want your personnel to gain?

This question will drive a majority of your future decisions, including software and hardware evaluation and implementation timelines. One advantage of leveraging smartphones is you can start with basic capabilities and build upon that foundation.

This is particularly true when it comes to query capabilities. If you intend for your smartphones to have full criminal justice query capability, you will need a much higher level of security safeguarding your data transactions because of Criminal Justice Information System (CJIS) requirements.[1]

Assess your current systems

If your intention is to have your smartphones replicate or replace existing query devices, you will need to do an assessment of existing software components and determine whether they have an effective mobile interface. If not, inquire as to what it will take to get the software operating on your mobile devices.

Increasingly, vendors of key operational software, like computer-aided dispatch and records management systems, are recognizing the interest in mobile devices and updating their product offerings. However, a mobile experience is not a given and you'll want to be fully aware of any limitations. Start by talking to vendors of the software that you want to use on your smartphones. Then you can plan your deployment, training and expectations accordingly.

BYOD Is Not the Answer

When you're using smartphones to access, gather and send criminal justice information, a BYOD approach is certainly not the most secure.

Some agencies have programs that allow officers to receive a stipend for using their personal smartphone — a so-called bring your own device (BYOD) policy — for department business. This may be acceptable for basic phone functions, but when you're using smartphones to access, gather and send criminal justice information, a BYOD approach is certainly not the most secure.

Agencies must effectively manage and control devices and that becomes difficult at best —near impossible at worst — when you consider the CJIS requirements for cellular devices in a BYOD environment. Agency-issued phones combined with a strong enterprise mobility management (EMM) infrastructure comprise the best and most secure strategy, and will save you both time and money in the long run.

Identify and engage your stakeholders

A successful project of this type will depend on the committed support and engagement of key stakeholders. Although this will vary somewhat by agency type, labor environment and project scope, you should be overly inclusive to avoid unexpected roadblocks or resistance. Outfitting a mobile-first agency will be a tech-intensive project, and you're going to need assistance and ongoing support from the IT staff that currently supports your agency's technology; they will be key to the success of your deployment.

If you want to bring computer-aided dispatch and records management systems to smartphones, you should include the dispatch and record supervisors in the discussion. If your agency has a labor bargaining unit, then you should bring them into the planning process to address any privacy concerns, especially if you will be leveraging the geo-location and sensor capabilities of the smartphone.

These labor discussions can sometimes be sensitive, but successful engagement often begins with an emphasis on the officer safety benefits and transparency regarding personnel expectations. It is helpful to seek input from experienced field training officers, as they are key to implementing change within an organization, and will be able to provide feedback on what features are most needed or a hindrance.

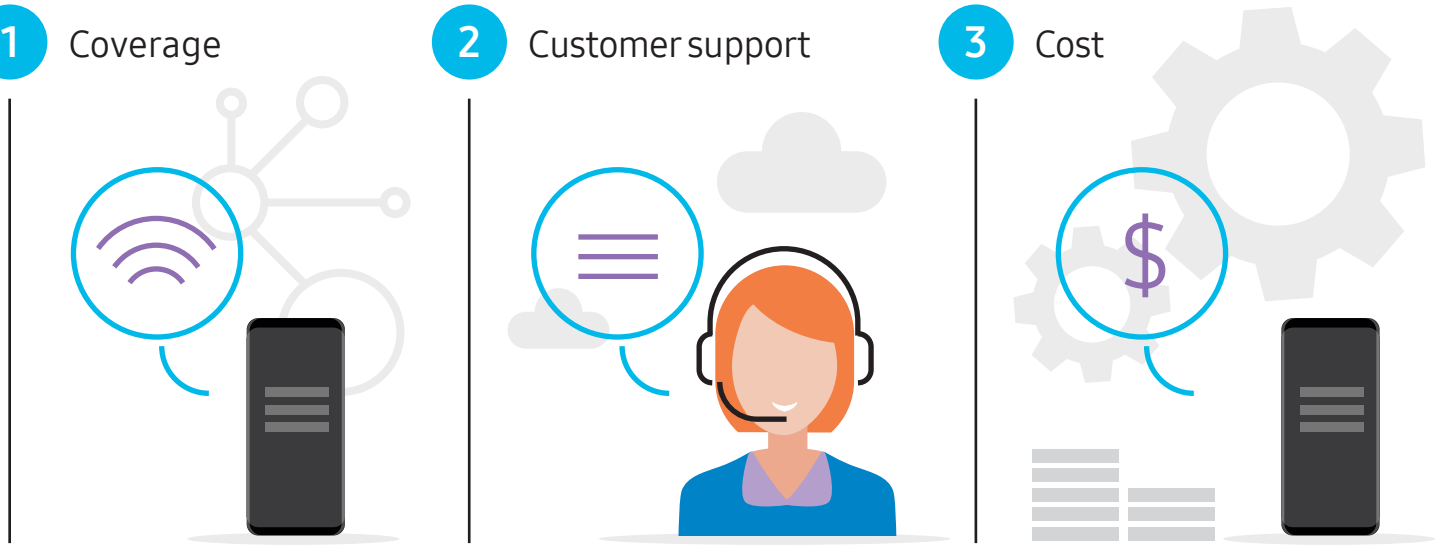
Carrier Selection Options

When it comes to carriers, remember the "three C" priorities in this order:

1 Coverage

2 Customer support

3 Cost



Choose a carrier that makes sense for your area and agency

Hardware is important, but a smartphone becomes an expensive paperweight if you can't access data or run desired applications. When it comes to carriers, remember the "three C" priorities in this order: coverage, customer support and cost.

Coverage should be the number-one determining factor. Yes, conventional wisdom in government purchasing is to go after the lowest bid, but this is a time when service quality should be the determining factor. A low-cost data plan is no bargain if coverage is spotty and upload/download speeds are inadequate to meet operational needs.

After coverage, you need to be concerned about the quality and availability of support. Law enforcement understands the importance of a trusted partner, and this should be the benchmark for customer service. There should be a single point of contact that provides information in a timely and user-friendly manner. Since this will be an ongoing relationship, you should pay attention to the first few meetings. If you find the carrier representative is lacking during the initial due diligence, it's time to reconsider your choice of carrier or look into the options provided by fully flexible, unlocked devices.

Beyond coverage and customer support, it's time to consider cost. Most agencies that use smartphones as primary query devices sign up for unlimited data, and there is generally some type of overarching package deal for public safety agencies.

Ask about the definition of "unlimited data" and what you can expect in terms of download and upload speed. Remember that advertised speeds generally are preceded by the words "up to," and will seldom maintain the advertised rate.

Also, ask whether data speeds will be throttled after a certain level of consumption is reached. These are relatively basic questions that your carrier should be able to answer. If possible, do your own speed and coverage testing.

Unlocked smartphones, which can be purchased through technology providers without a carrier service plan, also present a good alternative for public safety organizations looking for flexibility. By standardizing on an unlocked smartphone model and purchasing upfront, IT managers are then in a position to negotiate lower rates on a connectivity plan with the carrier or carriers of their preference. Alternatively, they may opt to “rent” unlocked devices in a mobility-as-a-service business model from a solution provider, who can also provide mobile management and other services.

Mobile Device Management (MDM) and Enterprise Mobility Management (EMM)

Security management and detection features within the EMM are critically important because CJIS policy prohibits the storage or transmission of criminal justice data from a device that has been rooted or jailbroken, per CJIS Policy Section 5.13.2.[2]

Smartphones being used by police officers for criminal justice information exchange need to have the best protection possible. Regardless of agency size, you will benefit from a robust and comprehensive approach to managing your mobile devices, and the best way to do that is with an effective MDM service or capability. When device management is expanded to include application and content management, as well as containerization, it is often referred to as EMM.

An effective EMM can significantly reduce the workload placed on your IT team in managing a mobile initiative, streamlining everything from inventory management to setting device policies and real-time monitoring. The EMM will aid in time-effective device deployment and assignment because phones can be preconfigured with desired application access, password protocols and data access controls. Mobility managers can also use these tools to to limit which applications can access information, something that is particularly important when dealing with criminal justice information.

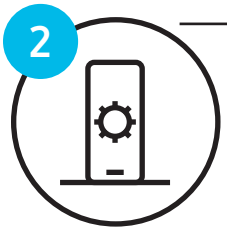
Security management and detection features within the EMM can prevent unauthorized changes, such as rooting or jailbreaking. This is critically important because CJIS policy prohibits the storage or transmission of criminal justice data from a device that has been rooted or jailbroken, per CJIS Policy Section 5.13.2.[2]

Implementing an EMM is an area that requires a thoughtful and and comprehensive approach. Working with experts who specialize in mobile device security and have a comprehensive understanding of CJIS requirements will ensure a proper implementation. You should check with the manufacturer of your smartphone device as well as other law enforcement agencies that have deployed an EMM system.

Phase Your Rollout

Start with a pilot group of selected participants who agree to provide feedback. Stress the importance of the project and the value of their input. A pilot group lets you address unexpected challenges on a smaller scale and permits corrections without major expense.

If you've selected your pilot participants carefully, they can serve as program liaisons and assist onboarding other officers. Once your pilot is completed to your satisfaction, you can begin device deployment across your entire organization. Depending on the size and organizational structure of your agency, consider deployment of devices to one group or division at a time, instead of all at once.



Configure Your Devices

Agencies will be well served to configure device settings and controls before they issue smartphone devices to officers. Security settings can be established that ensure PINs and passwords meet the security needs of a public safety environment. Using biometrics to unlock or enable certain functions can be part of the initial configuration and provide a powerful, yet user-friendly, level of additional security.

Agencies can invoke protocols such as blocking access to public WiFi, downloading unapproved apps or accessing specific types of web content or urls. Key applications can be preloaded and other undesirable applications such as “bloatware” can be disabled. Think of this pre-issue configuration process as being akin to creating a master image for your devices. It will save a tremendous amount of time for your IT personnel because devices will have all applicable settings and limitations applied over the air when the device is turned on. Configurations may be varied or customized to address the needs of different groups. For instance, you may allow a higher or broader level of access to a certain group of officers or investigators because they have a specific need.

Establish a Written Policy

Agencies should have a policy that gives an overview of the purpose of the mobile program and outlines the expectations for device usage. If the agency intends to issue individual smartphones and allow some degree of personal use, the policy should clearly state what is and is not permitted. Agency policy should also underscore security protocols and expectations, and include applicable CJIS related requirements, for both the federal and state level.

Conduct Regular Training

If possible, use some of the personnel who were involved in your pilot effort to provide training. Choose those who will champion the effort and will share the benefits of having a smartphone in the field. Training should include a candid — but positive — discussion of the security protocols that will safeguard devices.

This information will be better received if it is paired with context about why it is important to protect device information and maintain system integrity. Draw a parallel with officer safety: If officers are complacent with their passwords or access methods, they will be taking on significant and unnecessary risk. They could end up the victim of a data breach, or potentially expose sensitive information to suspects while on the scene.

Ensure that training is ongoing so that evolving needs or new applications are properly addressed. These training sessions are also a great opportunity to share success stories made possible by the use of the mobile devices. Recognizing new capabilities and the results is a good way to encourage further engagement and use.

CJIS: Criminal Justice Information Services

By definition, criminal justice information that is subject to CJIS compliance includes, but is not limited to, biometric, identity history, biographic, property, and case/incident history data, notes CJIS Policy Section 4.1.[3]

For most law enforcement agencies, fully utilizing smartphones means accessing criminal justice information databases and routine review of criminal justice information. These actions dictate that agencies comply with requirements established by the Criminal Justice Information Services (CJIS) division of the FBI, and follow the rules set by their respective state's CJIS oversight and auditing entity. Note that CJIS compliance is mandatory if you're accessing CJIS-controlled databases.

The rules for CJIS compliance are somewhat complex and subject to a degree of interpretation by the different states. The intent is to safeguard both the criminal justice database systems and sensitive data associated with personal information, such as an individual's criminal history. It also includes biometric data, an area that is quickly emerging in terms of its importance to law enforcement operations. By definition, criminal justice information that is subject to CJIS compliance includes, but is not limited to, biometric, identity history, biographic, property, and case/incident history data, notes CJIS Policy Section 4.1.[3]

Smartphones with an Android OS are considered by CJIS to have a "limited-feature operating system," which means the device is inherently more resistant to certain types of network-based technical attacks than a full-feature operating system. However, limited-feature OSes also mean user control of the device is more restricted, and thus a mobile device management (MDM) solution is required, explains CJIS Policy, Appendix A.[4]

CJIS Policy Section 5.13.2 sets out specific requirements for MDM configuration and requires the software to perform these tasks as a minimum standard:

- Remote locking of device
- Remote wiping of device
- Setting and locking device configuration
- Detection of "rooted" and "jailbroken" devices
- Enforcement of folder- or disk-level encryption
- Application of mandatory policy settings on the device
- Detection of unauthorized configurations
- Detection of unauthorized software or applications
- Ability to determine the location of agency-controlled devices
- Prevention of unpatched devices from accessing CJI or CJI systems
- Automatic device wiping after a specified number of failed access attempts

Agency administrators should closely review CJIS Policy Section 5.13, which specifically covers mobile cellular devices. The requirements set forth in CJIS Policy Sections 5.5 and 5.6, which deal with access and authentication requirements respectively, should also be considered.

All agencies that use CJIS systems are subject to periodic audits, and failure to maintain compliance can result in denial of access to essential databases. With this need for specialization, each agency should have a designated CJIS compliance point of contact.

The Power of Samsung Knox

Knox offers a suite of security enhancements, together with tools for device management and configuration.

In today's heightened era of security, mobile device manufacturers are starting to integrate security measures into the hardware and providing complementary software programs. The Samsung Knox platform consists of overlapping defense and security mechanisms, such as encryption and hardware root of trust, that protect against intrusion, malware and malicious threats. This protection carries multiple layers, from the hardware root of trust through secure boot protection, real-time kernel protection and Android-specific security enhancements. Knox protection is built in at the chip level and proved itself as the platform that received more "Strong" ratings than any other in an extensive comparison conducted by Gartner in 2016.

Knox Workspace provides a secure encrypted container that can be remotely managed by integrating it with either the Knox Manage MDM or with a major third-party MDM/EMM platform. Knox Workspace containers are unique in that the encryption and decryption keys are in the chipset of the device itself, making it virtually impervious to attack. All apps, email or files stored in the Workspace container are encrypted. When the container is locked, it can only be decrypted and accessed via PIN, password, pattern or biometric authentication. If a device is somehow compromised, the Knox Warranty Bit will trigger, resulting in a permanent lockdown to prevent data access. This separation solution is ideal for agencies that are highly regulated, and have users accessing both personal and professional data on their device.

Knox Configure allows for customization of devices before they are out of the box. Devices can become purpose-built appliances with a specific, single purpose, or include limited multi-purpose capabilities. Advanced settings can be remotely configured at a granular level. Connectivity to Wi-Fi, Bluetooth, GPS, NFC and Flight mode can all be restricted as needed. Additionally, updates can be done via push notifications to ensure security compliance.

Knox Manage provides a cloud-based solution that functions like a command-and-control center. Hundreds of devices can be configured or modified at once, saving hours of time and ensuring a much higher level of confidence in agency-wide security for mobile devices.

The Knox Manage MDM provides remote IT support, so an employee with a problem can allow IT direct access to the device for quick troubleshooting. It can locate a lost or stolen device, and have its content locked, rebooted or wiped clean. Knox Manage also allows for whitelisting of permitted applications, and can limit or prevent certain phone functions. It's capable of more than 280 unique policy settings, thus permitting an agency to uniquely tailor devices to their specific needs and concerns.

The Knox platform and solutions (which are licensed separately) offer a suite of hardened security enhancements that provide effective device management and control. Having this level of control for an entire fleet of devices can help public safety organizations address security concerns and create devices that are compatible with CJIS regulations.

Learn more:
samsung.com/us/knox

Samsung DeX Could Revolutionize Police Computing

Using the DeX docking station in a patrol vehicle centers the workflow around one smartphone, which makes it useful for query and geo-location services, in or out of the vehicle.

Current in-car computers are relatively expensive and lose their value once an officer leaves the vehicle. Forward-thinking police leaders are finding that today's smartphones provide an option that negates the need for a dedicated in-car computer and allow officers to take their computing device with them.

Samsung DeX was designed to link a smartphone with desktop peripherals to provide a full-featured, desktop-like experience for the user in the office or at home. DeX makes it possible for agencies to replace the expensive and limited-purpose in-car computer of today with a smartphone device that links seamlessly to a dedicated display and keyboard.

Using the DeX docking station in a patrol vehicle centers the workflow on one smartphone, which makes it useful for query and geo-location services, in or out of the vehicle. The benefits of Samsung DeX are not limited to replacing the in-car computer. An officer can use the smartphone in the field for query or evidence collection, then dock the device in the patrol vehicle to support computer-aided dispatch and geo-location functions. The officer can go back to the station where the same smartphone can be dropped into a DeX docking station and continue writing an incident report.

The technology is relatively new and is still evolving, but the solutions coming to market represent a game changer in cost savings and productivity. If the IT infrastructure of the department is adequate, the officer's smartphone is securely protected through these environments and stays inside an architecture that supports full interaction with criminal justice systems. The sheer utility of the smartphone provides benefits in many situations; the more an officer can rely on a single device to provide a variety of functions, the more proficient the officer will become in using that device to maximum benefit.

Learn more:
samsung.com/dexforwork

Looking to the Future

Smartphones have rapidly become a cost-effective force multiplier for public safety.

Smartphones have rapidly become a cost-effective force multiplier for public safety, and the Android platform is the ideal foundation to expand functionality and management capabilities. The fact that the phone can provide power (via the USB port) to peripherals for specialized functions means organizations will continue to see new capabilities, like in-field fingerprint submission and advanced sensor utilization.

Emerging applications are advancing officer effectiveness in the field, and allowing smartphones to communicate important situational awareness information to all necessary parties. With this technology, relevant information can be instantly shared with other officers, while specific sensor data such as radiation detection can be continually sent to a command center.

Smartphones are becoming so utilitarian that they are quickly becoming a must-have for officers in the field. Combining usefulness with the potential of serving as a very cost-effective in-car computer, it creates an increased return on investment for departments and officers alike. With a well-structured roll-out plan that includes operational, security and functionality concerns, departments can make a smooth transition into the next era of digital police work.

Click here for more info: Samsung Solutions for Public Safety

Footnotes

1. https://www.fbi.gov/services/cjis
2. Criminal Justice Information Services (CJIS) Security Policy. June 1, 2016.
3. ibid.
4. ibid.