SAMSUNG

White paper:

The ultimate law enforcement agency guide to going mobile

Table of contents

About the Author

Dale Stockton is a 32-year veteran of law enforcement, having worked in all areas of police operations and investigations and retired as a police captain from Carlsbad, California. He is a graduate of the 201st FBI National Academy and holds a master's degree in criminology from the University of California, Irvine. He has presented best practice classes in the use of technology on behalf of both the International Association of Chiefs of Police (IACP) and the National Institute of Justice. Stockton has served on advisory committees for both organizations, including the IACP Criminal Justice Information Systems (CJIS) Committee for more than five years. He also founded Below100, a nonprofit national training program dedicated to driving down line-of-duty police deaths.

Introduction

Today's police officers increasingly rely on technology to ensure their effectiveness and safety in the field. In-vehicle computers not only provide access to regional and national databases, they also support mission-critical functions like computer-aided dispatch (CAD), control of video units and automated license plate reader systems.

This level of computing power used to only be available on desktop computers inside a secure police facility. But today, fully equipped patrol vehicles give officers access to more powerful technology than they get at the station. Many of the newer, more powerful data systems provide officers with actionable data — in real time or near-real time — which can improve situational awareness and, by extension, officer safety.

But by the nature of law enforcement, the most effective officers tend to be those who spend less time in their vehicles. Many agencies are investing in community policing, encouraging officers to leave their cars and interact with the public as way to reengage with the community. In-vehicle computers offer incredible information platforms, but these platforms' benefits effectively end when the officer steps out of their vehicle, left with only the most basic information sources. Therein lies the challenge: Officers who need information while they're away from their vehicle must rely on their radio. Keep in mind, mobile computers' original purpose in law enforcement was to lighten the burden on radio dispatch, which was often overtaxed and required two people to conduct even the most basic queries.

Thanks to their versatility, smartphones have become an essential tool for today's police officers. Progressive law enforcement agencies have recognized smartphones' utility and their potential to supplement traditional vehicle-mounted laptops — or even replace them with handheld computing devices that double as push-to-talk (PTT) alternatives to traditional land mobile radio (LMR) communications. And as more technology solutions emerge, combining them with a smartphone platform will provide more innovative capabilities for public safety.

This white paper will inform forward-thinking public safety administrators about mobile technology's potential and provide an informed, thoughtful overview of best practices for implementing a mobile device program within their agency.

Today's opportunities

Most agencies already utilize smartphones to some extent, but these phones often belong to administrators or investigators who primarily use them for calls and emails. That's changing rapidly as more departments realize the significant benefits of providing smartphones to field officers.

Smartphones provide officers with practical communication benefits and extend their resources beyond the patrol car. For example, officers can follow up with witnesses over the phone or check the space availability at local mental health facilities, saving time and achieving quick return on investment (ROI). Smartphones can also be employed alongside other technologies in a wide range of more sophisticated applications.

Beyond the communication benefits, smartphone utility offers additional advantages, well beyond the capabilities of an in-vehicle computer. The Android OS serves as a platform for custom apps and peripherals, which can improve decision-making and save lives.

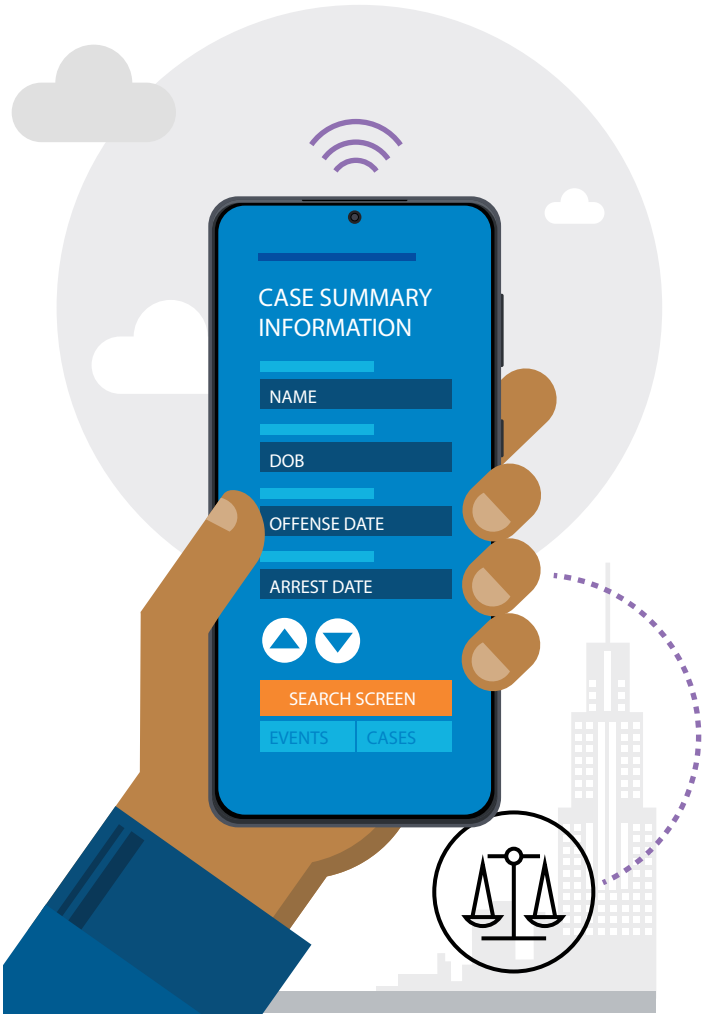
Here's a partial list of the resources available today, combining baseline features, apps and peripherals (attached or wireless):

- Camera for still image and video capture
- Voice recording
- Easy access to policy documents, case law notes and training videos
- Location services for situational awareness
- Officer under duress alerts (SOS)
- Electronic citations
- Officer wellness and health metrics
- Biometric authentication
- Forward-looking infrared (FLIR) imaging
- Report dictation
- Language translation
- Pill identification
- Connected sensors for transmitting real-time data
- CAD via smartphone
- License plate recognition
- Criminal justice database queries
- Secure push-to-talk (PTT), supplementing LMR
- In-field fingerprint ID
- Driver's license scan and ID card verification/validation
- Body-worn cameras or camera controllers
- Live video feed from CCTV or aerial cameras, e.g., Unmanned Aircraft Systems (UAS)

Planning for success

When public safety organizations decide to implement a mobile strategy to transform their operations, they're making a significant commitment, both in terms of budget and personnel resources.

The good news is there's proven ROI. Properly planned and managed, a smartphone rollout comes with minimal risk or disruption to your daily operations. As far as scale goes, a larger deployment that's well planned and utilizes effective mobile management tools will likely require less IT resources than a smaller deployment that's poorly planned and managed. The following approach has proven effective for many agencies:



Determine the desired outcome

What capabilities do you want your personnel to have? This will drive many of your mobility decisions. When you leverage smartphones, you don't have to do everything at once. You can start with basic capabilities and build on them over time. Once the foundation is established across the agency, you can progressively add more apps and access to relevant data sources. If you want your smartphones to have full capability for criminal justice information (CJI) queries, you should plan on having a higher level of security to safeguard data transactions, in accordance with Criminal Justice Information Services (CJIS) policy. A good way to start is to have a comprehensive mobile device management (MDM) or enterprise mobility management (EMM) solution in place as you deploy your phones. This step will make it much easier to manage your fleet, especially in a 24/7 work environment where personnel are often in the field. MDM/EMM is also a key component of gaining CJIS compliance. (See the MDM and CJIS sections of this guide for more information.)

Assess your current systems

If you want your smartphones to replicate or replace existing query devices, you'll need to assess your existing software components and determine whether they each have an effective mobile interface. If not, you'll need to determine what it will take to get the software operating smoothly on your mobile devices.

Vendors of key operational software, like CAD and records management systems (RMS), are increasingly updating their product offerings, recognizing agencies' interest in going mobile. However, a full-featured mobile or web version is not a given; you'll still want to have full awareness of your software's mobile capabilities. Start by talking to the relevant vendors of the programs you want to use on your smartphones. Then you can plan your deployment, training and expectations accordingly.

Issued devices vs. Bring Your Own Device (BYOD)

Some agencies have programs that allow officers to receive a stipend for using their personal smartphone for department business (under a BYOD policy). This approach may work for basic phone functions, but when officers are using smartphones to access, gather and share CJI, a BYOD policy lacks the necessary security. There's also a potential security issue if evidence documented or stored on an employee's personal smartphone is presented in court.

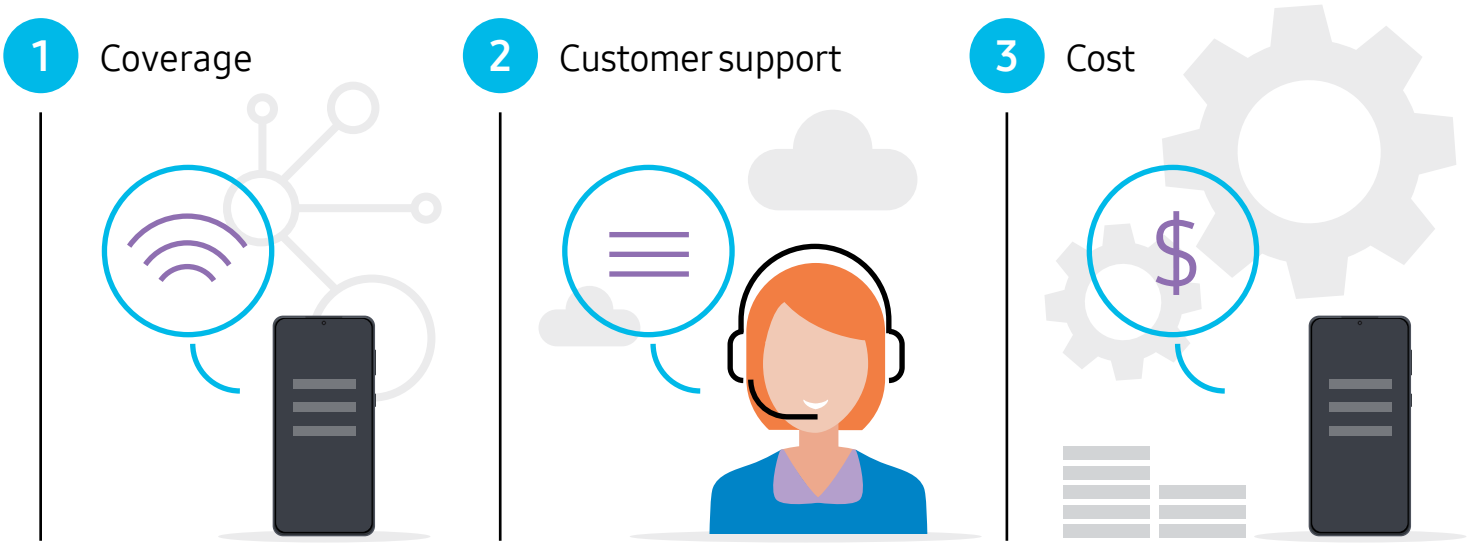
Agencies have to make sure they can manage and control their mobile devices effectively, and that becomes difficult — or impossible — when CJIS policy requirements need to be applied in a BYOD environment. Agency-issued phones and a strong EMM solution form the most secure approach, and will likely save you both time and money in the long run.

Identify and engage your stakeholders

A successful mobile deployment will depend on the committed support and engagement of your key stakeholders. This will vary somewhat based on your agency, labor environment and project scope, but you should be overly inclusive to avoid unexpected roadblocks. This will be a tech-intensive project, and you'll need ongoing support from the IT staff that currently supports your agency's technology; they'll be key to your project's success.

If you want to extend CAD and RMS access to your smartphones, you'll want to include your dispatch and record supervisors in the discussion. And if your agency has a labor bargaining unit, you should bring them into the planning process as well — especially if you'll be leveraging your smartphones' geolocation or sensor capabilities. These may be sensitive discussions, but successful engagement often begins by emphasizing the safety benefits and transparency regarding personnel expectations. You may seek input from experienced field training officers, as they're often key to implementing change within an organization and will be able to provide meaningful feedback on mobility features and operational expectations.

Carrier selection considerations



Choose a cellular carrier that makes sense for your area and agency

Phone hardware is important, but if you can't access your data or run your desired apps, your phone becomes an expensive paperweight. As for carriers, remember the three C's: coverage, customer support and cost — prioritized in that order.

Coverage should be your top determining factor. Conventional wisdom in government purchasing is to go after the lowest bid, but this is a time when the best-value service quality is worth the investment. A low-cost data plan isn't an effective bargain if the coverage is spotty or upload/download speeds don't meet your operational needs.

You should also check that your carrier's operational protocol and network design prioritizes public safety operations. In other words, will your mission-critical call or data get through during an emergency when the network is at capacity?

After coverage, consider the quality and availability of support. Law enforcement agencies know the importance of a trusted partner, and this should be your benchmark for customer service. You should have a single point of contact who provides timely information in a user-friendly manner. This will be an ongoing relationship, so make sure you find the carrier that provides the best customer service. You can also look into the options provided by fully unlocked devices.

Now it's time to consider the cost. If you're rolling out a new department-wide program, inquire about incentives for large-quantity hardware purchases. Most agencies that use smartphones as their primary query devices sign up for unlimited data. Carriers usually offer an overarching package deal for government agencies. Ask about their definition of "unlimited" and what you can expect in terms of download and upload speeds. Remember that advertised speeds generally reflect the upper limit and may vary depending on factors like coverage and bandwidth.

Make sure to ask your carrier whether your data speeds will be slowed after a certain level of usage. You may encounter prolonged operations, such as a major wildfire, and your bandwidth speeds shouldn't be compromised by a predetermined limit. These are relatively basic questions that your carrier should be able to answer. If possible, do your own speed and coverage testing. Also check with other agencies in your region to see what their experience has been with the carrier you're considering.

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

MDM and EMM solutions

Smartphones or tablets that police officers use for CJI exchange need to be as secure as possible. Regardless of your agency's size, you'll benefit from a comprehensive approach to managing your mobile devices, and the best way to achieve that is with an effective MDM solution. When device management is expanded to include app and content management, as well as containerization, it's often referred to as EMM.

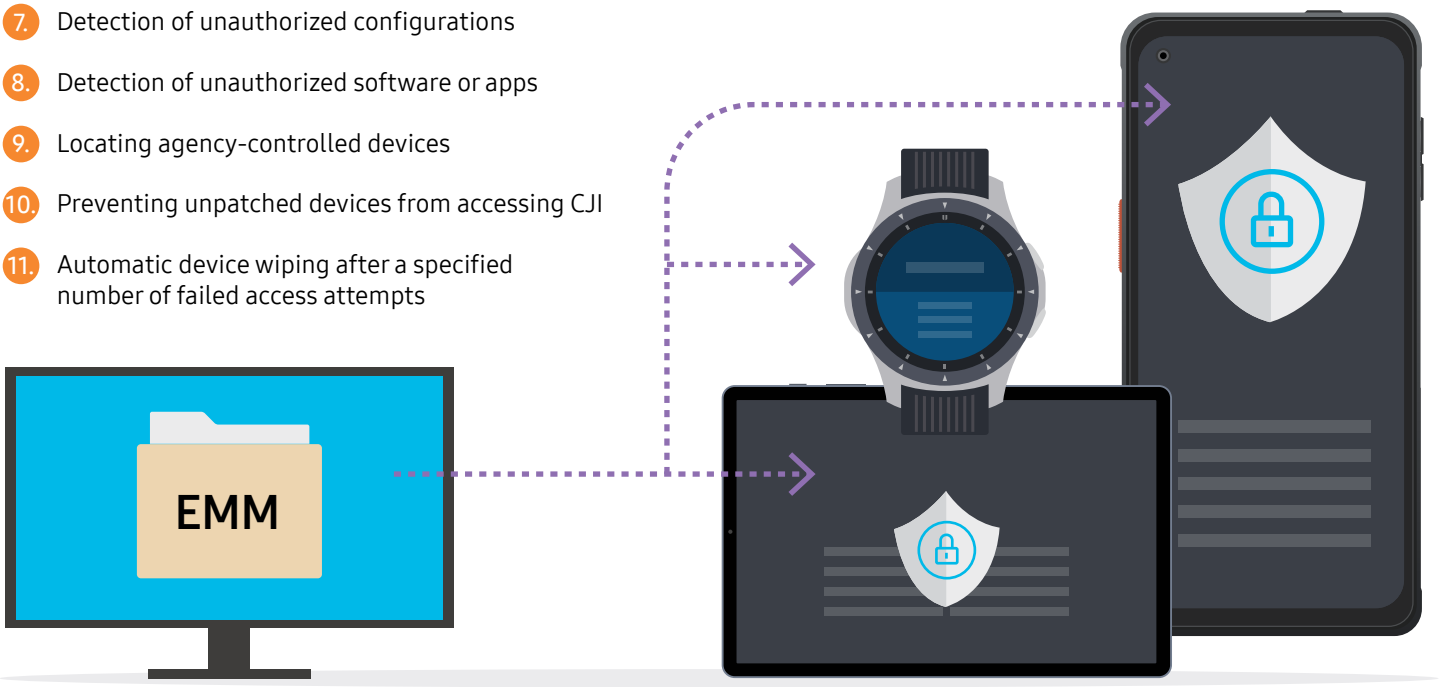
When it comes to mobile devices that are accessing or storing CJI, an MDM or EMM isn't just good practice, it's a requirement for CJIS compliance. It's also important that agencies ensure their MDM or EMM is capable of performing the following tasks as a minimum standard (CJIS Policy Section 5.13.2):

1. Remote locking of device
2. Remote wiping of device
3. Setting and locking device configuration
4. Detection of "rooted" and "jailbroken" devices
5. Enforcement of folder or disk-level encryption
6. Application of mandatory policy settings on the device
7. Detection of unauthorized configurations
8. Detection of unauthorized software or apps
9. Locating agency-controlled devices
10. Preventing unpatched devices from accessing CJI
11. Automatic device wiping after a specified number of failed access attempts

Using an EMM can significantly reduce your IT team's workload in managing a mobile initiative by streamlining everything from inventory management to device policies and real-time monitoring. The EMM will aid in efficient device deployment and assignment because phones can be preconfigured with core apps, password protocols and data access controls, such as prohibited internet connections or restrictions on Wi-Fi access. Mobility managers can also use these tools to limit which apps can access information, which is particularly important when dealing with CJI.

Most EMM solutions can be used to track a smartphone's location, which can help you recover a lost or stolen device. Although not mandatory for CJIS compliance, this tracking capability is recommended in the policy, as noted in the CJIS Mobile Appendix G-4: "Device tracking is not currently required in the CJIS Security Policy but should be applied to agency owned devices where possible as a risk mitigation factor."

Implementing an effective EMM requires a thoughtful and comprehensive approach. Working with experts who specialize in mobile device security and have a deep understanding of CJIS requirements will help ensure successful implementation. You may also benefit from consulting other law enforcement agencies that have significant experience using mobile devices.



CJIS compliance on mobile devices

What you need to know and consider

For most law enforcement agencies, full utilization of smartphone capabilities includes routinely reviewing CJI and accessing CJI databases. Agencies need to comply with the requirements established by the CJIS Division of the FBI and follow the policy set forth by their state's CJIS oversight and auditing entity, known as the CJIS Systems Agency (CSA). The person responsible for administration of CJIS policy within the CSA is known as the CJIS Systems Officer. Note that CJIS compliance is not an option if you're accessing CJIS-controlled databases.

The rules for CJIS compliance are somewhat complex and subject to a degree of interpretation by the state-level CJIS Security Officers. The intent is to safeguard both the criminal justice database systems and the sensitive data associated with personal information, especially when it comes to records such as an individual's criminal history. It also includes biometric data, which is quickly becoming more important to law enforcement operations. By definition, CJI that's subject to CJIS compliance includes, but is not limited to, biometric, identity history, biographical, property and case/incident history data (CJIS Policy Section 4.1).

Smartphones that run on 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 OS. However, the limited-feature OS also means user control of the device is more restricted, so an MDM solution is required (CJIS Policy, Appendix A, Definition: Limited-feature Operating System). See the MDM/EMM section of this guide for more information.

Agency administrators should closely review CJIS Policy Section 5.13, which specifically covers mobile cellular devices. They should also review CJIS Policy Sections 5.5 and 5.6, which definitively address access and authentication requirements, respectively. As you work to establish CJIS compliance, be wary of any vendor who claims to be "CJIS-certified"; FBI CJIS does not issue such certifications. If a vendor makes such a claim, ask who issued their certification.

All agencies that use CJIS systems are subject to periodic audits. Failure to maintain compliance can result in denied access to essential databases. This is an area of specialization, and each agency should have a specific person responsible for CJIS compliance, generally designated as the Terminal Agency Coordinator (TAC) (CJIS Policy Section 3.2.3).

The power of Knox

More public safety agencies are recognizing how mobile technology can empower officers and improve organizational efficiency, but they face two big challenges in harnessing the full potential of going mobile:

First, as the use cases for mobile devices continue to expand, so do the requirements for configuring, managing and supporting these devices. And secondly, with smartphones and tablets that access sensitive data or information subject to CJIS compliance, mobile security becomes an absolute requirement.

The Samsung Knox platform consists of overlapping defense and security mechanisms, such as encryption and hardware root of trust, which protect against intrusion, malware and other 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. Data inside a Galaxy device's work profile is double-encrypted, using two independent crypto modules. Knox Dual Data-at-Rest (DualDAR) also allows third-party crypto modules for inner-layer encryption. For double-layered encryption of data in transit, Knox supports VPN chaining.

The Knox platform does not replace the need for EMM tools, but it does provide a secure foundation. Samsung has collaborated closely with many of the leading MDM software providers to ensure close integration between the Knox platform and these providers' management tools.

At the same time, Samsung has developed its own set of cloud-based software solutions to meet specific enterprise needs. This Knox solution portfolio, which can be licensed and accessed through the Knox portal, is designed to assist mobility managers throughout a mobile device's life cycle. If you're using a Samsung device, some of these Knox features are already built in, and they're designed to work seamlessly with other Knox solutions.

Here are key offerings in the Knox solution portfolio:

Knox Configure allows you to customize devices before they're even out of the box, bypassing time-consuming setup wizards. Your Samsung smartphones and tablets are ready to roll in minutes, all configured with the same settings. You can turn mobile devices into purpose-built appliances with one specific use or include limited multipurpose capabilities. You can also create profiles to automatically provision apps and content, remove unnecessary preloaded apps, enroll in an MDM solution and remotely configure virtually any setting at a granular level. For instance, settings like Wi-Fi connectivity, Bluetooth, GPS, near-field communication (NFC) and Flight Mode can all be restricted as needed. Additionally, updates can be made via push notifications to ensure security compliance.

Knox Mobile Enrollment (KME) provides zero-touch deployment, automatically adding each device to your EMM solution once your IT team has pre-populated its user credentials. End users can skip setup wizards and account registration, so they get up and running faster. With KME, you can ensure all your devices stay enrolled in your EMM system. If an end user or an outside threat performs a factory reset or uninstalls the EMM agent, KME will automatically reinitiate the enrollment process. Your IT team can also enable Android factory reset protection, allowing a device to be recovered even if the user credentials are lost.

Knox Manage is a cloud-based EMM solution that functions like a command-and-control center. Hundreds of devices can be configured or modified at once, saving hundreds of hours of personnel time and ensuring stronger confidence in agency-wide security for mobile devices. Knox Manage allows for remote IT support, so an employee can allow IT direct access to their device for quick troubleshooting. Perhaps more importantly, a lost or stolen device can be located, locked and rebooted or wiped. Knox Manage also allows you to set an allowlist and blocklist of apps and limit certain phone functions, such as screen capture or use of an external SD card.

Knox E-FOTA gives your agency control over software and OS updates, allowing you to validate, approve and deploy updates across all devices, without any end-user interaction. You can test and validate firmware updates in advance to uncover potential compatibility issues, and then schedule updates to be deployed by device group and time of day, minimizing workflow disruption. You can even factor in other criteria like battery life. Knox E-FOTA is integrated with leading EMM solutions, so you can pull existing device and group information from your EMM to streamline your firmware management processes.

Knox Suite combines these mobile enterprise solutions into a single package with one license key, providing end-to-end security and the flexibility to secure, deploy and manage devices throughout their life cycle.

Samsung DeX is revolutionizing police computing

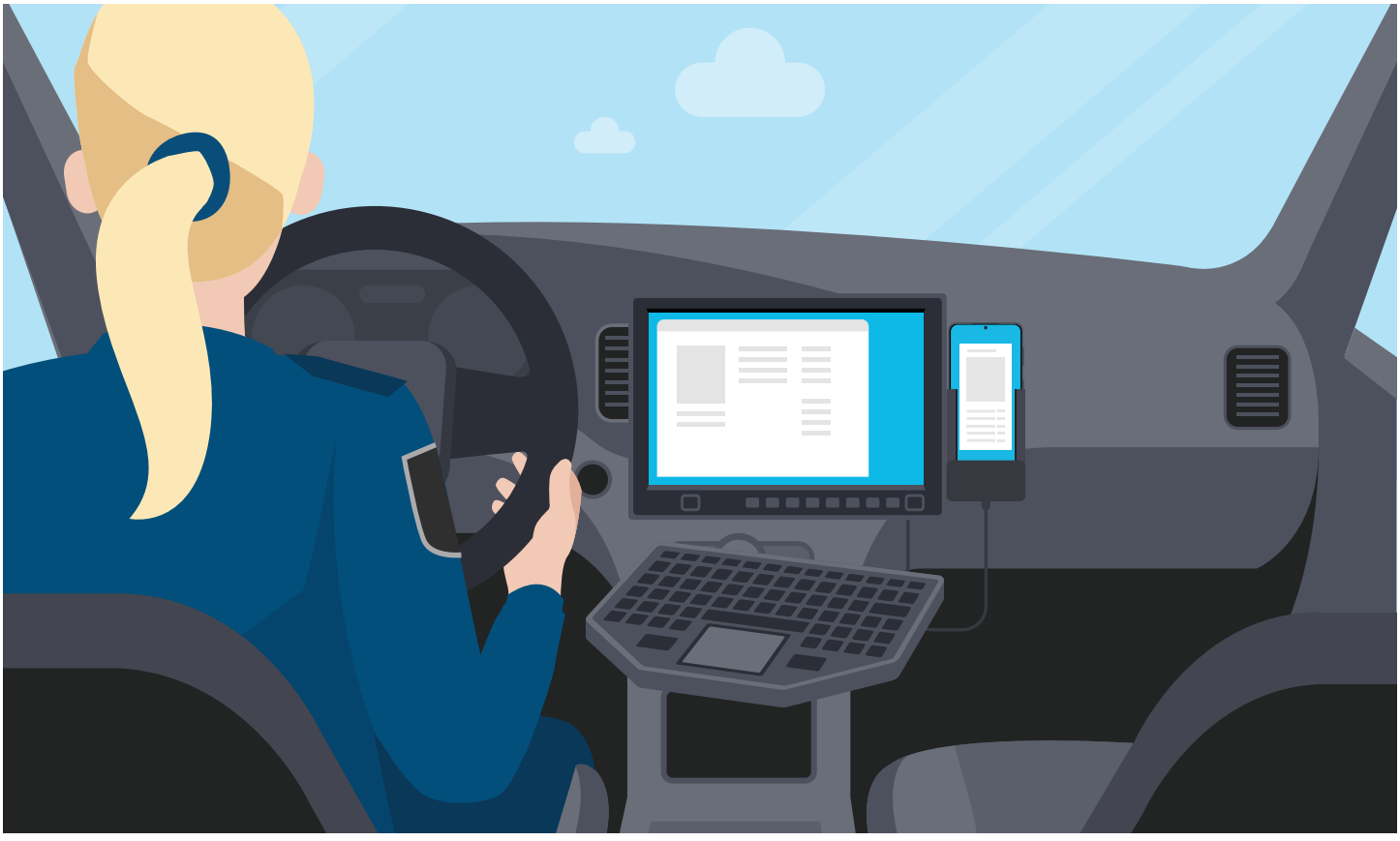
One device supports in-field, in-vehicle and in-station use

Current in-vehicle computers are relatively expensive and lose their value once an officer leaves the vehicle. Forward-thinking law enforcement leaders have found that today's smartphones negate the need for a dedicated in-vehicle computer, as officers can take their computing device with them.

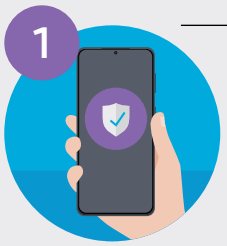
Samsung DeX was designed to link a smartphone with peripherals to provide a full-featured, desktop-like experience for users working from an office or at home. In law enforcement agencies, DeX makes it possible to replace an expensive, limited in-vehicle computer with a smartphone that links seamlessly to a dedicated display and keyboard designed to operate in a patrol vehicle.

Using DeX in a patrol vehicle centers an officer's workflow on one smartphone, which they can use for query and geolocation services both in and out of the vehicle. The benefits of Samsung DeX are not limited to replacing the in-vehicle computer. An officer can use their smartphone in the field for query or evidence collection, and then dock the device in their patrol vehicle to support CAD and geolocation functions. When the officer returns to the station, the same smartphone can be dropped into a DeX docking station, and the officer can write an incident report or transfer evidence, such as photos or videos, over the department's secure network.

The technology is still evolving, but the solutions coming to market bring incredible cost savings and productivity. If your department's IT infrastructure is adequate, your officers' smartphones are securely protected inside an architecture that supports full interaction with criminal justice systems. And 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 for maximum benefit.



Best practices for mobile deployments

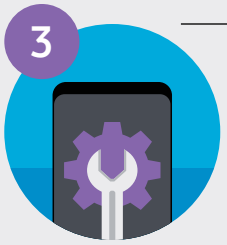


Assess your current IT infrastructure

If you're planning to integrate your smartphones with your existing CAD, RMS or other departmental apps, such as email or scheduling, it will serve you well to have a solid awareness of these systems, their supporting hardware and how they operate on your network, or in conjunction with it. It's generally better to work from the perspective of adding a new capability (e.g., mobile access to CJI) and leverage processes that are already proven and trusted. That said, use this opportunity to look for potentially vulnerable points and ways to improve security.

Phase your rollout

Start with a pilot group of selected participants who agree to provide feedback. Stress the importance of the project and that their input is valuable to you. Using a pilot group allows you to address unexpected challenges on a smaller scale and make course corrections without major expense. If you've selected your pilot participants carefully, they can serve as champions of your program and help other officers get up to speed. Once your pilot is completed to your satisfaction, you can begin deploying devices across your organization. Depending on your agency's size and organizational structure, consider deploying devices to one group or division at a time.



Configure your devices before issue

For a smoother deployment, agencies should configure device settings and controls before devices are issued to officers. This can be accomplished with an EMM tool (see pages 5 and 8), which you can use to establish security settings that ensure PINs and passwords are strong enough for a public safety environment. As part of your initial configuration, you can include biometric authentication for unlocking certain functions, providing a powerful — and user-friendly — additional level of security. Agencies can invoke protocols such as blocking access to public Wi-Fi, preventing unapproved app downloads or restricting access to specific types of web content or URLs. Key apps can be preloaded, and undesirable apps like "bloatware" can be disabled. This pre-issue configuration process is akin to creating a master image for your devices. It will save a tremendous amount of time for your IT team, as your agency's devices will have all the applicable settings and limitations configured over the air, ready to go when the device is turned on. Your devices can be custom-configured to the needs of different groups. For instance, you might allow a higher or broader level of access to a certain group of officers or investigators who have a specific need for it.

Establish a written policy

Your agency's written policy should provide an overview of the purpose of your mobile program and outline the expectations for secure device usage. If your agency intends to issue individual smartphones and allow some degree of personal use, then your policy should clearly state which uses are permitted and which aren't. Policy should also underscore security protocols and expectations, as well as CJIS-related requirements, at both the federal and state level.

Conduct regular training

If possible, ask some of the personnel from your pilot effort to train other officers, championing the benefits of having a smartphone in the field. Share success stories widely; what gets recognized will be repeated. Training should include a candid, positive discussion of the security protocols that will safeguard your devices.

This information will be better received if you provide an explanation as to why it's so important to protect private data and maintain system integrity. Draw a parallel with officer safety: If officers are negligent with their passwords or data access methods, they'll be taking on significant unnecessary risk. They could become the victim of a data breach, or potentially expose sensitive information to suspects.

Make sure you warn officers of the potential danger of being distracted by their smartphone while dealing with a suspect. Point out the benefits of maintaining a safe distance and holding/viewing the phone in such a way that officers are continually aware of a suspect's movements.

Push-to-talk (PTT): What you need to know

Public safety agencies have long depended on two-way radio communications, using very high frequency (VHF) and ultra-high frequency (UHF), to support operations from routine information exchange to life-or-death tactical response. Millions of times a day, officers use the PTT capability on an LMR handset to talk to another party.

Cellular handsets and smartphones use LTE connectivity as their broadband communication system. Unlike LMRs, cellular devices generally don't have a physical button to push. But as more agencies issue smartphones for their personnel, there has been growing interest in using these mobile devices to replace LMR radios by adding a PTT capability that could, ultimately, support mission-critical operations.

Major carriers — including AT&T through FirstNet, and Verizon with Frontline — are now offering PTT capability based on 3rd Generation Partnership Project (3GPP) standards. 3GPP was formed more than 20 years ago to unite seven different telecommunication standards organizations and ensure their compatibility as LTE evolved. Standards for mission-critical PTT (MCPTT) were first addressed by 3GPP in 2016, covering key functions like broadcast calling, location services, emergency alerting and device-to-device communication. The latest release of 3GPP standards addresses 5G connectivity.

Even without a major carrier, PTT capability can be achieved with apps such as ESChat or Orion. These over-the-top (OTT) solutions provide encrypted communication that can support routine day-to-day operations, or they can be configured to support an evolving situation, even if it involves multiple organizations. These apps can also provide two-way communication without the geographical limitations of an LMR system. A commander at an out-of-state conference, for example, could be reached via an OTT solution as easily as if they were in their own jurisdiction.

MCPTT and PTT on an OTT app can effectively augment an existing LMR system by increasing the number of users, expanding the effective range and improving overall interoperability. Because PTT functionality uses LTE, users can easily combine two-way voice communications with sharing texts, photos and even live video, all from a single device.

LMRs have a long history in public safety, where communications are mission-critical, so the adoption of LTE-based PTT systems is likely to be an evolution as opposed to a singular event.

Here are some of the primary reasons for a gradual transition:

- Most smartphones are designed for everyday consumers, so they need a protective case to withstand the rigors of a public safety environment. Also, most smartphones don't have a physical button dedicated to PTT, so users generally need to adjust some settings to activate the PTT capability. However, the Samsung Galaxy XCover Pro features a physical button that can provide instant PTT engagement, and the device is built to MIL-STD-810G standards. (See the following section for more on rugged device considerations and the XCover Pro.)
- To integrate MCPTT with legacy LMR systems, there are some interoperability challenges, as well as remaining questions about PTT interoperability between different carriers.
- Device-to-device PTT operations, which is routine for LMR handsets, is not as streamlined on LTE devices that transmit at much lower power with internal antennas. In other words, LTE offers a smaller range of reliable direct communication (that isn't cellular) compared to LMRs.

PTT via LTE is already benefitting public safety operations by supplementing existing radio systems, providing coverage where radio signals are lacking and empowering personnel who either don't have a radio or are outside the range of the agency's LMR system. As another powerful tool in the public safety communication toolbox, PTT's added utility and potential for cost savings will likely motivate many more agencies to make the shift.

Making the case for rugged: The Galaxy XCover Pro is ready to serve

Public safety operations typically need devices that can withstand unusually tough environments. From dust and rain to drops and extreme temperatures, police officers' mobile devices have to put up with a lot.

Recognizing the rapidly growing interest from public safety agencies, as well as other physically demanding industries, Samsung recently introduced the Galaxy XCover Pro. The full-featured, cost-effective rugged mobile device is purpose-built for first responders. And it has earned FirstNet Ready status, meaning FirstNet subscribers can use their XCover Pro to access the Band 14 spectrum for public safety connectivity.

The XCover Pro has proven itself ready for field operations by passing 21 environmental tests under the Defense Department's MIL-STD-810 standard, including repeated drops from 5 feet up. The device has a 6.3-inch edge-to-edge display built with Gorilla Glass 5, designed for high durability. A 4050mAh battery keeps the XCover Pro going through an entire shift, and heavy-duty pogo pin connectors make it easy to quickly drop the device into a multi-unit charger. Unlike most consumer smartphones, the XCover Pro's battery is easy to swap out when duty calls.

The other most notable feature of the XCover Pro is its programmable physical button, which can be set to open a specific app — so you can skip the menus. This physical button can be used with a variety of PTT applications including those offered by FirstNet, Verizon and even Microsoft Teams. (See the Push-to-talk section on page 14.)

The fingerprint sensor is built into the power key, so an officer's phone is unlocked in user mode as soon as it's drawn from their belt. The XCover Pro even has a Glove Mode that improves responsiveness when the user is wearing gloves.

Is the XCover Pro well suited for uniformed law enforcement? That question was recently answered by an IT manager supporting a large sheriff's department in the Pacific Northwest:

"The rugged case is part of the phone's design, and that cuts peripheral costs. The biometric reader is on the side, and that makes the phone quick to put into operation. We've configured the flashlight to come on with a push of the top right button, so there's no pull-down menu required. With PTT, we're exploring how it can integrate to the radio system, as well as supporting specialty units with [an EMM solution]. We plan to use it [the XCover Pro] to scan transit cards, and this will eliminate a heavy single-purpose device. Overall, it's a great tool for law enforcement."

Like other Galaxy smartphones, the XCover Pro is protected by Knox, Samsung's defense-grade mobile security platform (see the Knox section on page 10). Purpose-built for field officers, the XCoverPro combines powerful smartphone features with a rugged design — serving as a great partner for any public safety officer.

Tablets: Important use case considerations

As more police departments move toward mobile technology, they have to consider which form factor will best support the officers. Most field officers prefer to work with a smartphone because it's easy to carry in their pocket, allowing them to keep both hands free. But for many public safety assignments, tablets can expand operational capabilities better than smartphones.

In some situations, public safety personnel may prefer the user experience of a tablet rather than a smartphone. Officers investigating a crime scene or traffic accident, for example, are often tasked with evaluating a prolonged incident that requires extensive, detailed documentation. With a tablet, the officer can see their work on a larger scale and with greater context. The larger display also allows officers to complete complex forms in less time — and with less chance of error.

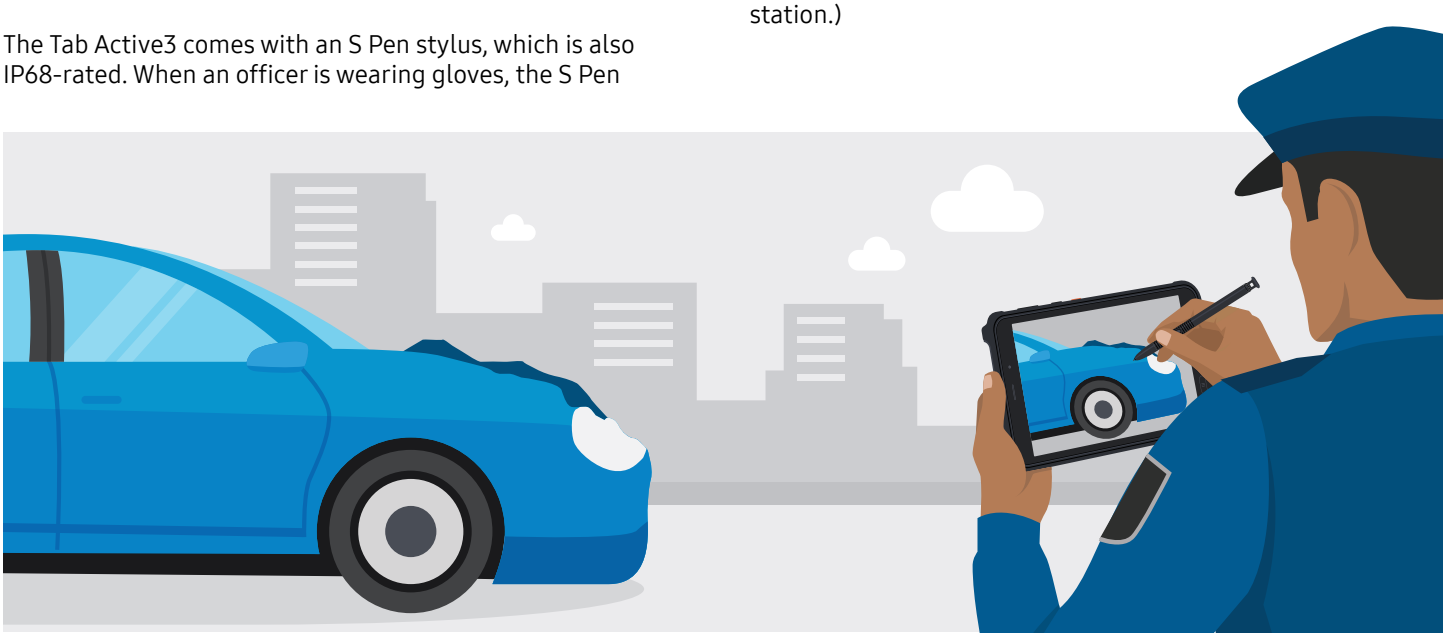
For public safety officers, working a scene in a dust storm, blowing rain or salt spray is part of the job. The key is to select a tablet that's designed to survive the volatile environment of public safety operations. In tough working conditions, rugged tablets provide a large mobile work surface. The Samsung Galaxy Tab Active3, for instance, has an 8-inch touchscreen. The Tab Active3 is IP68-rated for resistance to dust, dirt, sand and moisture, and it has passed a series of MIL-STD-810 environmental durability tests, proving its resilience in unpredictable conditions.

The Tab Active3 comes with an S Pen stylus, which is also IP68-rated. When an officer is wearing gloves, the S Pen makes it easier to write on the tablet, so they can take notes or draw sketches without pulling their gloves off. Officers can also use the S Pen's button to communicate with their tablet remotely, controlling the camera or advancing presentation slides during a debrief.

In a paperless workflow, officers' tablets store digital information that can be shared instantly with other units, no printer required. The Tab Active3 even supports LTE connectivity, providing uninterrupted access to department databases and other online resources. It also features a 13MP camera that captures high-resolution photos and video, which are easy to integrate into a report. And it comes with plenty of onboard storage, plus a microSD slot to increase your capacity if you need it.

Users can rest assured their tablet will make it through a full shift, with up to 11 hours' battery life on the Tab Active3. When the battery does run out, it's easy to swap out for a charged one. But if an officer doesn't have a fresh battery on hand, their tablet can still operate using an external power supply when it's mounted in a vehicle.

When a desktop computer would be more comfortable, an officer can connect their Tab Active3 to a monitor, keyboard and mouse using Samsung DeX. (See page 11 to learn more about DeX and how one mobile device can support public safety operations in the field, in the patrol car and in the station.)



Experiences from agencies that have gone mobile

Mobility helps Chula Vista PD connect officers to more apps

The Chula Vista Police Department (CVPD) in Southern California serves a population of 275,000 people, with authorization for 255 sworn positions. That's a staffing ratio of less than 1 officer per 1,000 civilians, one of the lowest ratios in the entire country — and significantly less than the nation's average of 2.4 officers per 1,000 civilians, as reported by the FBI. CVPD has managed to keep serving its residents by strategically leveraging technology as a force multiplier. Their response times have improved, and public satisfaction has increased.

A key factor in CVPD's success has been their deployment of smartphones to all personnel. This connected officer approach has served as a foundation for layering additional technologies. CVPD's smartphones are CAD-enabled and CJIS-compliant, and they provide real-time geolocation for each officer, rather than each patrol vehicle. What's more, the devices can receive live video feeds from CVPD's nationally recognized Drone as a First Responder program, as well as an extensive city-controlled CCTV system.

Beyond that, CVPD officers use their smartphones to gather evidence, dictate reports, manage body-worn cameras and conduct in-field fingerprint checks. The agency conducted a pilot effort to evaluate the effectiveness of replacing conventional patrol car computers with smartphones using Samsung DeX, and the department is now expanding the concept to more vehicles. By this model, a single smartphone could support all the computing needs of an on-duty officer while they're in the field, in their vehicle and at the station.

The importance of leadership

Technology endeavors like these don't just happen; they take committed leadership. "We will never have the funding available to provide us with all the officers we need," explains CVPD Chief Roxana Kennedy. "So we have to look at ways to make them as effective as possible. And we have to be creative."

Kennedy stresses the importance of balancing the community's expectations with the realities of policing. This means assuring the public that policing technology will be used responsibly, citing the drone program as an example. "We've been very transparent," says Kennedy, "and everything we do is documented on our website. The thing I balance is that our technology often helps us to deescalate situations because real-time information is available to officers, and this allows them to make the best decisions."

Eric Wood, CVPD's IT manager, has overseen the agency's connected officer effort since its inception and participated in a webinar entitled "Paradigm Shift: A Mobility-First Approach Provides Powerful New Capabilities." During the webinar, Wood shared 20 unique apps that are now accessible to officers through their smartphone.

CVPD's use of smartphones to untether officers has given field personnel greater flexibility and full access to mission-critical information, resulting in improved officer safety and increased efficiency.

Bernalillo Count Sheriff's Department deploys ATAK on smartphones

Smartphone apps are providing new, powerful capabilities for public safety agencies. One great example is the Android Team Awareness Kit (ATAK) and the way it's being used on Samsung smartphones by the Bernalillo County Sheriff's Department (BCSD) in New Mexico. Originally developed for military special operations by the U.S. Air Force Research Lab, ATAK is a collaborative mobile app that tracks team members' locations in real time and facilitates data sharing for photos, videos and secure texts. The app allows data to be layered, so users can share mission-essential information, including real-time camera feeds.

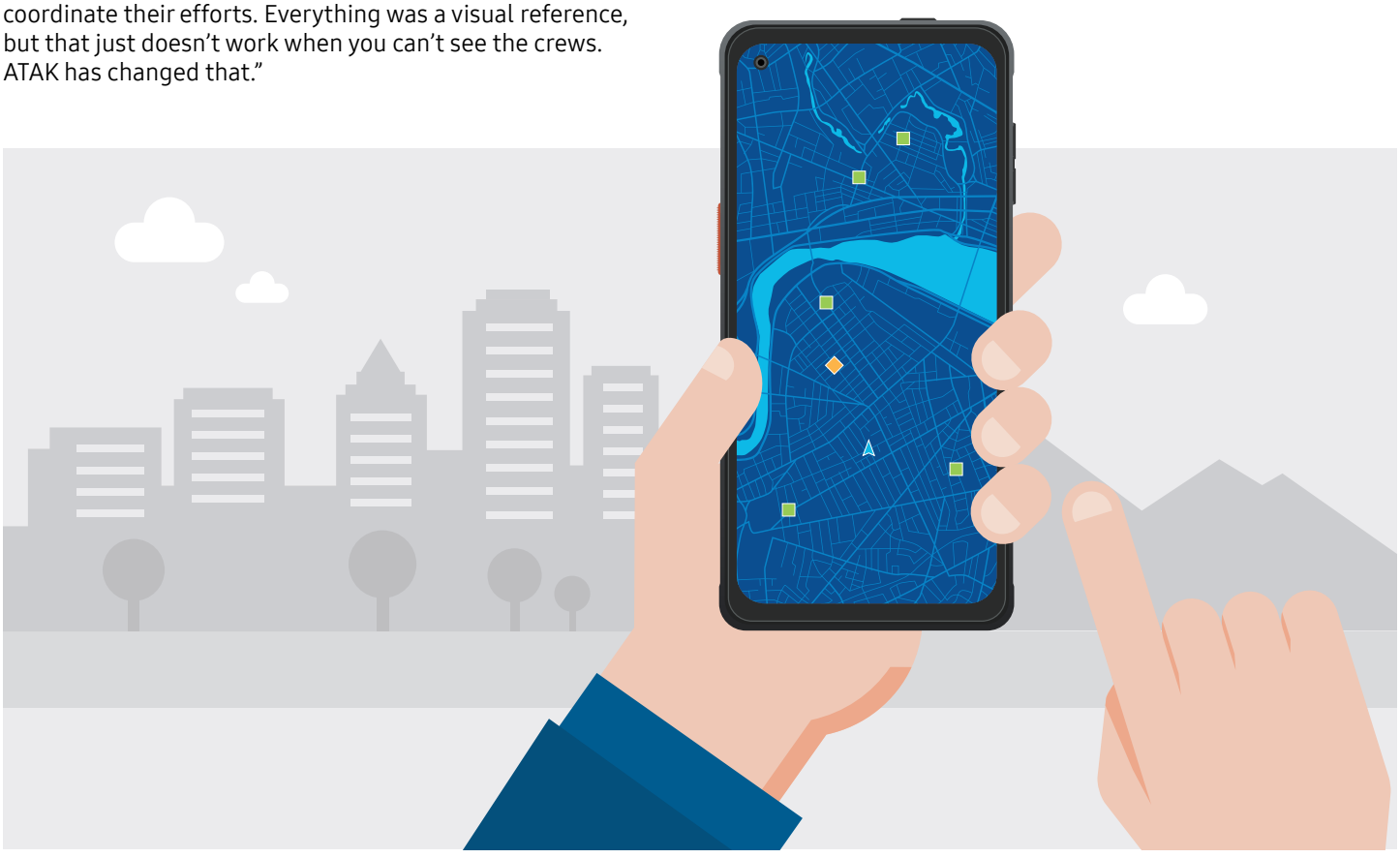
BCSD Undersheriff Larry Koren serves as the agency's senior pilot and has participated in more than 500 search and rescue missions. Koren says his agency's use of ATAK on their Galaxy smartphones has dramatically increased the success rate of their rescue missions by improving information sharing and situational awareness.

"We were having an issue with ground crews during both wildland fires and search and rescue missions," Koren explains. "We would be flying over an area and there would be personnel that we couldn't see under a canopy of ponderosa pines. Sometimes we would have three separate crews looking for an injured hiker, and it was really difficult to coordinate their efforts. Everything was a visual reference, but that just doesn't work when you can't see the crews. ATAK has changed that."

Before ATAK, BCSD's rescue mission communications were subject to significant lag time and errors, as crew members exchanged information with a series of phone calls. "With ATAK, communication is streamlined," says Koren. "Everyone can see key information, like the designated LZ [landing zone] or the staging area for the ambulance. It keeps everyone on the same page. Air crews can fly over an area and transmit an aerial view of terrain to their counterparts on the ground. This helps them prepare in terms of equipment and the approach that will be needed."

When an experienced rock climber sustained serious injuries after a fall in the Sandia Mountains, ATAK played a critical role in coordinating air and ground rescue efforts. "It was very treacherous terrain at an elevation of 9,000 feet, but we were able to quickly get ground personnel to the patient, then insert a paramedic who packaged the patient in a litter basket," says Koren. "He attached the helicopter's rope, and we moved her to the staging area where the ambulance was waiting."

Search and rescue efforts in Bernalillo County often involve other agencies, which may be operating on a different radio frequency — or may not even have a radio available. ATAK leverages cellular technology as a common denominator. "It gives me peace of mind that the other personnel involved in this rescue network have the same level of awareness," says Koren.



Looking to the future

Smartphones have rapidly become a cost-effective force multiplier for public safety, and the Android platform is an ideal foundation for building new mobile capabilities. The phone can even power specialized peripherals via the USB port, and time will continue to bring new capabilities, like in-field fingerprint submission and advanced sensor utilization.

Emerging apps are increasing officers' effectiveness in the field and allowing their smartphones to communicate important situational awareness information both horizontally and vertically. In other words, relevant information can be shared instantly with other officers, while specific sensor data such as radiation detection can be continually relayed to a command center.

With unmatched utility, smartphones are quickly becoming a must-have for officers in the field. Smartphones have the potential to serve as a cost-effective in-vehicle computer, and can supplement or even replace traditional LMR systems, offering high ROI for departments and officers alike. With a well-structured rollout plan that covers operations, security and functionality concerns, departments can make a smooth transition into the next era of mobile police work.

Increasingly, police leaders are recognizing that it is only a matter of time until the concept of fielding connected officers is fully realized, dramatically improving both officer safety and officer efficiency. This will be the result of powerful mobile devices and apps that provide a level of utility equivalent to several single-purpose tools — far surpassing the capabilities of traditional in-vehicle computing.

Click here for more info: Samsung Solutions for Public Safety

Learn more: samsung.com/publicsafety | insights.samsung.com | 1-866-SAM4BIZ

Follow us: youtube.com/samsungbizusa | @samsungbizusa

SAMSUNG

WHP-HHP-LAW-ENFORCEMENT-JUL21