SAMSUNG

White paper:

A comprehensive guide to CJIS compliance in a mobilized agency

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 retiring 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 Below 100, a nonprofit national training program dedicated to driving down line-of-duty police deaths. Stockton currently serves as the Chairman of the Spirit of Blue Foundation.

Introduction

Smartphones: A powerful force multiplier for law enforcement

Across the country, public safety agencies are recognizing that smartphones can play a significant role in helping officers be safer and more efficient as they perform their law enforcement duties. Combined with powerful new apps and peripheral technologies, smartphones are truly a game changer for first responders, allowing officers to stay connected and informed, regardless of their assignment or proximity to a patrol vehicle.

Traditional in-vehicle computers have long provided a valuable information platform, but their utility disappears when an officer steps outside the vehicle. Being an effective officer means engaging with the public, and an in-vehicle computer limits an officer's ability to operate efficiently when away from the patrol vehicle.

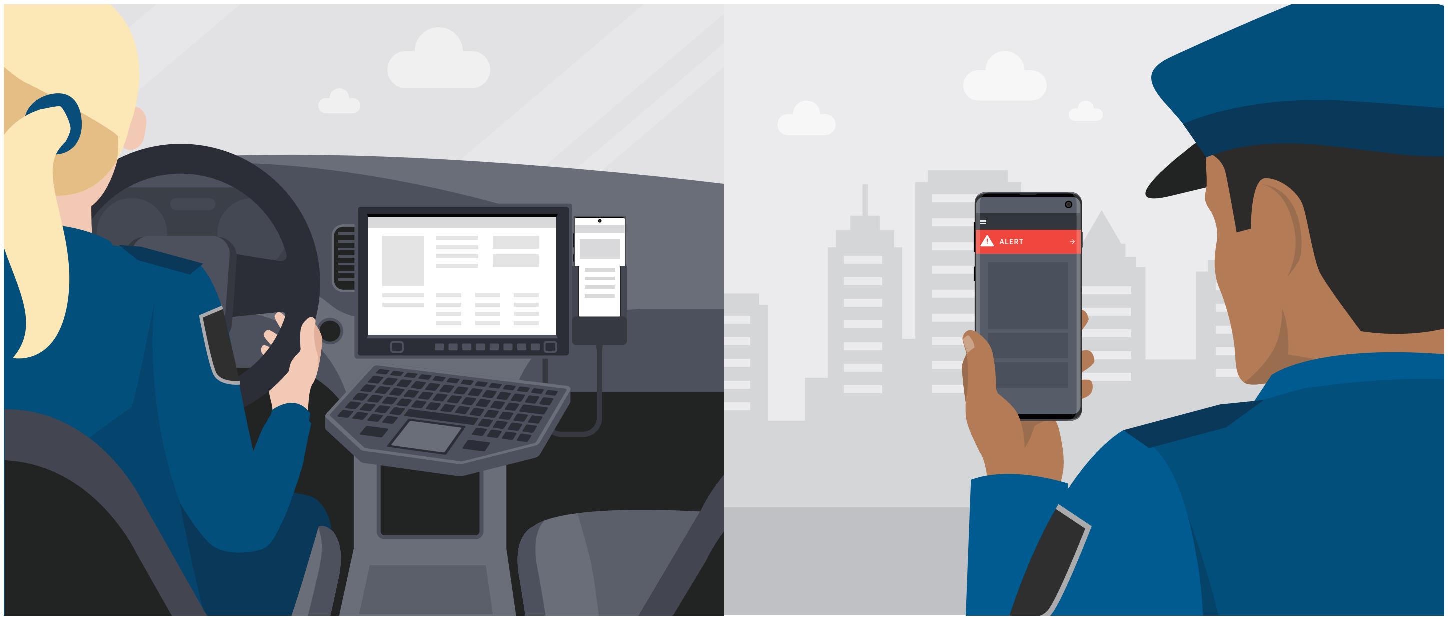
Smartphones overcome this limitation by delivering the same level of information access when an officer is away from the car or assigned to a nonvehicle responsibility, such as bike or foot patrol. The sheer utility and flexibility of a smartphone offer significant operational advantage.

Although many agencies already have some degree of smartphone use, many issue the devices only to administrators and investigators for relatively limited uses like basic calling, texting and emailing. That's rapidly changing, as progressive agency leaders realize the benefits of a connected officer who has full information access whether they're at the station, in their vehicle or in the field.

To realize the full potential of smartphone utilization, officers need to be able to access the full range of databases available to law enforcement professionals. These databases contain criminal justice information (CJI), so agencies must ensure compliance with the requirements established by the FBI Criminal Justice Information Services Advisory Policy Board (CJIS APB).

Virtually all police agencies have data systems that routinely access criminal justice systems subject to CJIS security policies. Many agencies also have patrol cars with in-vehicle computers that currently operate in a secure, CJIS-compliant environment. In effect, these agencies already have a foundational level of CJIS security processes that may be leveraged to support a robust and reliable smartphone program, providing personnel with greater operational flexibility and efficiency.

> This paper will provide an in-depth overview of CJIS Policy requirements, as well as practical steps and considerations for implementing a smartphone-centric program that will support full connected-officer capability and comply with CJIS security requirements.



CJIS: Composition, purpose and process

To fully benefit from a smartphone deployment, law enforcement agencies need access to CJI databases and the ability to review the information therein — which requires agencies to comply with CJIS Policy, set by the FBI CJIS APB. The primary purpose of CJIS Policy is to establish the minimum baseline of controls necessary to protect the full life cycle of CJI, whether it's at rest or in transit. The policy applies to every individual who has unescorted access to unencrypted CJI, regardless of their role or employer.

Although CJIS Policy is the primary document setting forth security requirements, agencies must also comply with the protocol set by their respective state's CJIS oversight entity, commonly referred to as the CJIS Systems Agency (CSA). CJIS Policy is comprehensive and subject to a degree of interpretation by each state's CSA. CSA-designated entities vary from state to state and include agencies such as state police and state justice departments. All CSAs have a designated CJIS Systems Officer (CSO), who is responsible for the statewide administration of CJIS oversight on behalf of the CSA. The intent is to safeguard the criminal justice database systems and any sensitive personal information, such as an individual's criminal history. The collaborative work of FBI CJIS and the state-level CSAs — the CJIS Advisory Process — is designed to provide a management approach that includes the FBI, local, state, tribal and federal data providers and system users.[1]

The work of the CJIS Advisory Process is carried out by five working groups that comprise the CJIS APB — four groups that regionally represent the states, and a fifth that covers federal agencies. Regional APB working groups have state-level and local-level representatives, as well as a tribal representative. State-level representatives are assigned by the CSA, and local-level reps are assigned by either the International Association of Chiefs of Police or the National Sheriffs' Association. The purpose of the APB is to review policy, technical and operational issues. This approach ensures that CJIS policy is capable of evolving to address new technologies and security threats.

The complementary role of the National Institute of Standards and Technology

CJIS Policy is largely based on standards established by the National Institute of Standards and Technology (NIST), whose mission is to advance measurement science, standards and technology to enhance economic and national security. Many of the technical facets of CJIS Policy involve complex technological processes that are based on testing done by NIST and vetted by the FBI CJIS APB. Although there isn't an official and codified relationship regarding CJIS Policy and NIST, there is ongoing collaboration on best practices and evolving processes.

For example, recent changes in CJIS password requirements are a direct reflection of the extensive work done by NIST regarding digital identity services and the related publication, NIST Special Policy 800-63-3. NIST is also a key participant in the Fast ID Online (FIDO) Alliance — which is actively working toward stronger, more practical methods of ensuring authenticated and secure online transactions.

Recommendations from FIDO's work will likely be incorporated in future revisions of CJIS Policy. IT professionals supporting a department smartphone program would be well served to review FIDO's processes and recommendations. Devices running Android 7.0+ are FIDO2 certified right out of the box.

Smartphones and CJIS: The basics

A full transition to a smartphone-centric computing environment for public safety will require that officers continue to have access to the criminal justice databases they depend on. Mobile devices used to access that information are subject to CJIS Policy, as well as any additional information assurance requirement(s) imposed by the state-level CSA. The use of smartphones to conduct CJI queries is a relatively new capability, and the specifics of achieving and maintaining CJIS compliance are still evolving, particularly for agencies using compensating controls (see page 14, Compensating controls).

This white paper will address the CJIS Policy sections with substantial relevance to mobile implementation. However, current CJIS Policy is over 250 pages long, and there's a degree of subjectivity in how state-level CSOs interpret the policy. The CJIS Policy G.4 Mobile Appendix provides an overview of requirements and issues related to CJIS mobile compliance, explaining why CJIS requires specific steps to safeguard CJI on mobile devices.

The Mobile Appendix notes that a mobile OS is "inherently more resistant than a full-feature operating system to certain types of network-based technical attacks due to the limited feature sets."[1] Even so, CJIS policy also notes that "threats to cellular handheld devices stem mainly from their size, portability and available wireless interfaces and associated services." The policy cites examples of potential threats including loss, theft, unauthorized access, malware and electronic eavesdropping.

Although CJIS Policy (current version is 5.9) is more than 250 pages long, the separate Requirements Companion Document drills down the longer-form policy into just 35 pages. For people deeply involved in CJIS processes, this document is commonly referred to as the "stuff without the fluff," primarily created to help those responsible for actual policy implementation.

The Requirements document can be used to quickly identify mandated processes or actions and ensure contextual understanding.

Bring Your Own Device (BYOD) and CJIS: Not Recommended

Some agencies have programs that give officers a stipend for using their personal smartphone for department business as part of a Bring Your Own Device (BYOD) policy. This policy may be acceptable for basic tasks, but if you're using smartphones to access, gather and send CJI in a BYOD environment, it becomes difficult to comply with CJIS requirements. Note these two excerpts from CJIS Policy Appendix G.4:

"... the technical methods and compensating controls required for CJIS Policy compliance are likely to exceed any potential cost savings for implementing BYOD."

"BYOD environments pose significant challenges to the management of secure device configurations. In many cases it may be impossible to apply effective security that is acceptable to the device owner, or it may require extremely costly compensating controls to allow access to CJI on personally owned devices."

Agency-issued smartphones, combined with a strong mobile device management (MDM) infrastructure, facilitate the best and most secure mobile strategy — and will save your agency both time and money in the long run.

CJIS Required: Mobile Device Management (MDM)

Although a smartphone OS is resistant to network-based technical attacks, the limited-feature OS comes with more restricted user control of the device. An MDM solution is not only good practice, it's required by CJIS Policy for direct access to CJI. With an MDM in place, an agency can exercise a high level of control over deployed mobile devices. CJIS Policy Section 5.13.2 requires that, as a minimum standard, agencies use an MDM capable of performing the following tasks:

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

Agencies of any size can benefit from a robust and comprehensive management strategy, and the most reliable way to do that is with an effective MDM solution. When device management includes app and content management as well as containerization, it's often referred to as enterprise mobility management (EMM).

An effective MDM or EMM solution is key to managing a mobile initiative, streamlining everything from inventory management to device policy setup and real-time monitoring.

Risk Mitigation

In addition to using an MDM, organizations must take the following steps — at a minimum — to mitigate the security risk associated with wireless devices (CJIS Policy Section 5.13.3):

- ✓ Apply OS patches and upgrades as soon as they become available, after necessary testing.
- ✓ Configure for local device authentication.
- ✓ Use Advanced Authentication or approved compensating control.
- ✓ Encrypt all CJI data that resides on the device.
- ✓ Erase cached information — including app authenticators — when a session is terminated.
- ✓ Implement firewalls on full-featured OS devices or run an MDM system that provides such services from the agency level.
- ✓ Employ malicious code protection on full-featured OS devices or run an MDM system that facilitates the ability to provide antimalware services from the agency level.

(The last two steps don't apply to most smartphones, as they're not full-featured OS devices.)

EMM can be a tremendous timesaver for IT personnel responsible for a large project, particularly during device deployment and assignment, because phones can be preconfigured with desired app access, password protocols and data access controls. Limitations can also be placed on which apps can access information under certain conditions, something that's particularly important when dealing with CJI.

Ensuring Authorized Access

Due to the potential for mobile devices to be lost, misplaced or stolen, user and device authentication are key to preventing unauthorized access to these devices and maintaining the integrity of CJI. Rigorous security ensures only authorized users have device access, thanks to a multilayered security strategy. User PINs and passwords, for instance, have significant potential for compromise, but they can be combined with additional security features. The challenge comes in establishing security protocols that ensure sensitive data stays secure while still being user-friendly.

Examples of standard authenticators include passwords, hard or soft tokens, biometrics, one-time passwords (OTPs) and PINs. CJIS has recently modified its password requirements to align with NIST Special Publication 800-63B and now provides two categories of password methodology: Basic and Advanced. The primary differences are password length (minimum of 8 characters for Basic versus 20 characters for Advanced) and the length of time between required password changes (maximum of 90 days with Basic versus one year with Advanced). The Advanced standard's less frequent update requirement is a result of the increased password length. Additional requirements under the Basic and Advanced categories can be found in CJIS Policy Sections 5.6.2.1.1.1 and 5.6.2.1.1.2, respectively.

Note: The 20-character requirement for a password under the Advanced criteria may not be practical for many smartphone users in law enforcement. Not only are they working on a relatively small display/keyboard, but for their safety officers should spend a minimal amount of time looking down at their mobile device.

Key Steps for Implementing a CJIS-Compliant Smartphone Program

1. Determine your desired outcome

If you intend for your agency smartphones to have full CJI query capability, you'll need to build your system with an eye on CJIS compliance. This is much more effective before phones are deployed, because you can preconfigure the devices to prevent unauthorized operations and ensure they'll receive security patches as needed. An MDM/EMM solution will also allow you to lock or wipe a lost or stolen device. In addition, each agency needs to assess its unique needs to determine the best method of ensuring successful compliance (see next step).

2. Assess your current CJIS utilization and app utilization

Determine your agency's current use of CJI and identify your Terminal Agency Coordinator (TAC) or Local Agency Security Officer (LASO), who will work with your state's CSA. This person is often responsible for your connection to the National Crime Information Center (NCIC) and/or the periodically required CJI access training. If your agency is already conducting CJIS queries from devices outside the building, such as in-vehicle computers, there's likely already a secure and encrypted "backhaul" to be utilized by mobile devices.

›

There's more to do, but this is a significant start. You'll need to evaluate your existing software components and determine whether they have an effective mobile interface. This basic step should be done early in the process to see whether your existing software vendors will effectively support field operations with a smartphone. If not, inquire with your vendors as to what it will take to get the software operating on your mobile devices.

Author's Note: Increasingly, vendors of key operational software, like computer-aided dispatch (CAD) and records management systems (RMS), recognize the interest in mobile devices and are updating their product offerings accordingly. However, a mobile capability is not a given, and you'll want to be fully aware of any limitations. Start by talking to vendors of the software you want to use on your smartphones. If the capability isn't already there, ask when it will be available. If you have legacy systems or department-developed apps that aren't currently usable on your smartphone, you may want to consider using a virtual desktop infrastructure (VDI). VDI is designed to store and run desktop workloads including a Windows client OS, apps and data in a server-based virtual machine, allowing interaction with a desktop that's presented to the user via Remote Desktop Protocol (RDP). While VDI requires a degree of IT management, it can be effective at bringing greater functionality to your smartphones.

3. Check with other agencies, approval authorities and your vendors

All agencies that access CJI with mobile devices must comply with CJIS Policy. Ask around to determine who in your region has a robust and successful smartphone program. Meet with the person responsible for that project and inquire about the specifics of the technical processes that were used to achieve CJIS compliance. Ask if they have documentation of their system and whether they've submitted an application to the state's CSA that they'll share with you. You're unlikely to find this information on the internet because posting a specific method of CJIS compliance could undermine the security of the program. Nonetheless, the agency will likely be willing to work with you directly to help get you started and share lessons learned. If the program is successful and has withstood a CJIS review process, consider a similar approach with your project. This can save you a lot of time and give you a higher likelihood of approval and success.

If you're unaware of an agency in your area that's currently using smartphones for CJIS queries, check with the approving authorities involved in the CJIS process. Start with your own agency's NCIC representative and work from there. Depending on the size of the state and number of agencies involved, there's likely a regional or county "switch" that channels queries to the state and then to NCIC. Check with each of these levels and ask about agencies who have successfully introduced smartphones to the process. Once again, do your inquiries and determine if you can use an existing process as a model for your program. Finally, ask your current vendors (software, hardware and cellular carrier) for referrals to successful smartphone deployments. You may also consider attending a relevant conference, such as the International Association of Chiefs of Police (IACP) Technology Conference, to gather information and participate in relevant workshops.

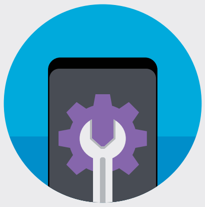
Author's Note: Be wary of any vendor who claims to be CJIS certified. There is no such certification. At best, vendors may have clients who have used their products to successfully comply with CJIS requirements, but this doesn't extend to a certification for the vendor. While successful deployments may serve as a road map for your effort, remember that CJIS approval and auditing happen primarily at the state level. This means that programs that have been approved in one state may not necessarily meet the expectations of reviewers in your state, especially in areas that fall within compensating controls for Advanced Authentication.

4. Establish a written policy

Agencies should have policies that define the purpose of their mobile program and outline expectations for device usage. Agency policy should also underscore security protocols and expectations and include applicable CJIS-related requirements. Ensure there's a warning banner that appears on the screen at the time of device startup, reminding personnel that they're subject to departmental policy regarding the use of the device.

5. 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 allows for course correction without major expense. If you've selected your pilot participants carefully, they may serve as program liaisons and assist in onboarding other officers. Once your pilot is completed to your satisfaction, you can begin deploying devices across your entire organization. Depending on the size and structure of your agency, consider deploying devices to one group or division at a time, instead of all at once.



6. Configure your devices

Agencies will be well served to configure device settings and controls before they issue smartphones to officers. Security settings can be established beforehand to ensure PINs and passwords meet CJIS requirements. Agencies can invoke protocols such as blocking access to public Wi-Fi, preventing unapproved apps or blocking specific types of web content or URLs. Key apps can be preloaded, while undesirable apps such as "bloatware" can be disabled.

Think of this pre-issue configuration process like 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 devices are turned on). Configurations may be customized to address the needs of different groups. For instance, you may allow a higher level of access to a certain group of officers or investigators who have a specific need.

7. 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, positive discussion of the security protocols that will safeguard devices. Emphasize the responsibility that comes with being assigned a device capable of accessing CJI. Equate the issuance of this device (and the accompanying responsibility) to other high-value or controlled equipment.

The above information will be best received if it comes with context about device security and system integrity. Draw a parallel to officer safety: If officers are complacent with their passwords or access methods, they'll 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 apps are properly addressed. These training sessions are also a great opportunity to share success stories made possible by the use of mobile devices. Recognizing new capabilities and their results is a good way to encourage further engagement and use.

8. Measure ROI holistically

Establishing a robust and effective CJIS-compliant smartphone program requires substantial investment. However, once in place, the return on investment (ROI) is significant. Smartphones continue to introduce new paradigms to policing, allowing officers to work much more efficiently in the field, regardless of their assignment. Notwithstanding CJIS query capability, they also provide an unrivaled level of sheer utility that will increase officers' situational awareness and improve their overall effectiveness.

Passwords and PINs: The specifics

CJIS Policy has specific requirements for passwords and PINs that are used in the authentication process for accessing CJI.

Password requirements:

- Be a minimum length of 8 characters on all systems
- Not be a dictionary word or proper name
- Not be the same as the user ID
- Expire within a maximum of 90 calendar days
- Not be identical to any of the previous 10 passwords
- Not be transmitted in the clear outside the secure location
- Not be displayed when entered

PIN requirements

- Be a minimum of 6 digits
- Have no repeating digits (e.g., 112233)
- Have no sequential patterns (e.g., 123456)
- Not be the same as the user ID
- Expire within a maximum of 365 calendar days

Author's Note: Under the provisions of CJIS Policy Section 5.6.2.1.2, if a PIN is used to access a soft certificate that's the second factor of authentication, and the first factor is a password that complies with the requirements in Section 5.6.2.1.1, then the 365-day expiration requirement can be waived by the CSO.

- Not be identical to the previous three PINs
- Not be transmitted in the clear outside the secure location
- Not be displayed when entered

Exception: When a PIN is used for local device authentication, the only requirement is that it be a minimum of 6 digits.

Author's Note: CJIS Policy acknowledges that the minimum password/PIN requirements above may not be practical for a mobile device password/PIN due to the need for immediate access for some device functions (such as phone calls) and the inherent difficulty of entering information on a small screen during an emergency. CJIS Mobile Appendix G-4 includes discussion of using a layered authentication approach in which the initial device password is simplified. CJI access is still protected by additional layers of access control, and the CJI or access to CJI is cryptographically separated from apps that can be operated at the device level. Appendix G-4 indicates that this approach "may satisfy the CJIS Security Policy requirements if fully compliant as a standalone application."

CJIS required: Advanced Authentication

The intent of Advanced Authentication (AA) is to meet the standards of multifactor authentication, which employs the use of two of the following three factors of authentication: something you know (e.g., a password), something you have (e.g., a hard token) and something you are (i.e., a biometric). The two authentication factors must be unique. AA is required when CJI is accessed from a mobile device, unless the access is indirect. Indirect access is defined as having the authority to access systems containing CJI without being able to conduct transactional activities on state and national systems. Under CJIS Policy 5.6.2.2.1, the relevant CSO will make the final determination as to whether access is considered indirect.

The primary purpose of AA is adding a layer of security to ensure only authorized users gain access. If the initial authentication step is compromised, a threat will be thwarted by the additional step. This is why it's so important the secondary factor be different from the first, not simply an additional step.

CJIS Policy also emphasizes the need for robust identity and authentication processes that are properly utilized, and it cautions against overreliance on product claims: "Many identity and authentication schemes used by existing commercial applications may make claims that appear to be consistent with CJIS Security Policy Advanced Authentication requirements, however, extreme care must be taken to ensure the actual technical implementation is compliant with policy."[1]

Advanced Authentication: Evolving areas of interest

Author's Note: The information contained in this section is the result of input from several tech practitioners and IT professionals who are exploring ways to effectively meet AA requirements while providing a degree of user convenience. The National Cybersecurity Center of Excellence and the NIST Public Safety Communications Research Division (PSCR) have been identifying viable AA options that support the Fast Identity Online (FIDO) Universal Second Factor and Universal Authentication Framework standards. This work is documented in NIST Special Publication 1800-13, Mobile Application Single Sign-On: Improving Authentication for Public Safety First Responders,[2] which is recommended reading for IT professionals who are currently evaluating AA options. This is an evolving area, and any process not expressly authorized and documented in CJIS policy should be submitted to the appropriate CJIS authority (usually a state-level CSO or designate) before being purchased or implemented.

AA is one of the areas of greatest challenge when establishing CJIS compliance for smartphone use. There are already multiple ways to meet the AA requirements of CJIS, but all have pros, cons and some degree of complexity or challenge for the user, especially given the diverse range of law enforcement operations. Fortunately, CJIS Policy continues to evolve, and there is some flexibility in the form of compensating controls that permit alternative security processes. (Note: Compensating controls are considered temporary and must be approved by the relevant CSO.)

One proven approach to AA is for an officer to use their user ID, followed by a CJIS-compliant password and then, for the second factor, a hard token to generate a random 6-digit number to initiate a CJI inquiry session. However, use of a hard token in conjunction with a smartphone generally requires an officer to use both hands and pay close attention to the authentication steps. This is not an ideal situation in a patrol environment, where officers need to stay situationally aware and must always be capable of accessing the necessary tools they carry on their duty belt.

Another option would be to issue a one-time password (OTP) that's sent to the mobile device during the authentication process. CJIS requires that the OTP be transmitted out of band, meaning the communication service channel (network connection, email, SMS text, phone call, etc.) that's used to obtain an authenticator is separate from the channel used for login (CJIS Policy 5.6.2.2). For many agencies, this approach may be preferable to requiring an officer to use and maintain a hard token.

A more complex AA method would be to meet the second factor with a device certificate that's stored in a secure container and invoked only when the user provides authorization in the form of a password (which must be different than the login password). This allows the authorized user to meet the second factor of authentication by "having" the certificate and producing it on demand. The CJIS Security Policy discusses this process and requires a password to invoke the certificate. However, it may be equally viable to use a phone-based biometric (like a fingerprint) in place of the required password. This is an area that has not been specifically discussed in CJIS Policy, but could be submitted for review by the relevant CSO.

Agencies may also want to consider submitting an application asking for authorization to use other forms of technology to meet the "have" requirement. For instance, many agencies use a proximity access card (often called a prox card), which is uniquely issued to an individual. These devices generally use near-field communication (NFC) technology, which is available on many smartphones. Although it would probably require some development, the second factor could be accomplished by the officer touching the phone to the pocket holding an issued prox card. This approach is user-friendly, quick to complete and doesn't require two hands. If desired, a smart card with additional identification factors could be used in lieu of a standard prox card. Both approaches would be subject to CSO review and approval.

A paired smartwatch, uniquely issued to an individual and worn on the wrist, could also serve as the "have" requirement of the login sequence. This solution would provide both convenience and higher security, as individually issued watches would be strapped to an officer's wrist, lowering the risk of it getting lost or left unattended with the smartphone. The officer would initiate the authentication process as normal, including entering their password (something they know). The second authentication step could leverage NFC with the smartwatch, with an officer simply touching the phone to the area of the watch, similar to the prox card scenario previously described. Note: Consistent with NIST Special Publication 800-63B, authentication must be intentional; therefore, the second method of authentication must require action on the part of the officer, e.g., touching the area of the watch. If deemed CJIS compliant, this process would provide a quick and secure method of AA, allowing an officer to reliably log on while meeting security requirements and supporting officer safety protocols. Again, this process would be subject to CSO approval.

Although many smartphones now have fingerprint readers, these cannot be used to meet the "have" component of AA because the user's fingerprint isn't centrally validated by the agency. However, an agency could design a process that would call on an agency Registering Authority (RA) to meet with an officer at the time of device issuance to register their fingerprint. After verifying the officer's identity, the RA would assign strong authentication policy to the device, retrieve the policy and, when prompted, observe the enrollment of the fingerprint to validate its authenticity. The RA would then provide the user an authorization code to enter in the relevant CJI app. Once this process is complete, future login sequencing will consist of a username followed by a CJIS-compliant password (the "know" factor) and then, when challenged, the user-provided (and agency-validated) fingerprint. Alternatively, an agency could use the smartphone fingerprint reader to unlock a Trusted Platform Module and produce a device certificate, thereby meeting the "have" requirement. Both of the AA processes outlined are expedient and conducive to officer safety. As with the other processes described in this section, they would need to be reviewed and approved by the relevant CSO.

Compensating controls

As technology continues to evolve, new options that may be more effective or appropriate may not yet be approved. Fortunately, a degree of flexibility is built into the CJIS policy for dealing with these situations. CJIS includes a provision known as "compensating controls," which permits temporary alternative security processes that provide the same level of protection as AA, or greater, in circumstances involving legitimate business or technical constraints. The concept of compensating controls may be particularly relevant to agencies that are integrating an expanded smartphone program with legacy infrastructure. CJIS Policy designates the CSO as the determiner of whether a process will be deemed an acceptable compensating control and for what period of time the compensating control will be allowed. The reviewing CSO is an appointed administrator within the respective CSA, and they'll be from the same state as the agency.

Author's Note: Compensating controls are considered to be temporary and the period for which an alternative process may be utilized is subject to the determination of the state's CSO. It is recommended that an agency seek guidance as to what the expectations may be in terms of replacing compensating controls, particularly if the processes involved are expensive or difficult to implement.

Before a CSO can consider approval, an MDM policy must be implemented that satisfies CJIS requirements. The compensating controls shall:

1. Meet the intent of the AA requirements
2. Provide a similar level of protection as the original AA requirement
3. Not rely upon existing AA requirements
4. Expire upon the CSO approval date or when a compliant AA solution is implemented

In addition, the following minimum controls shall be implemented:

1. Possession and registration of an agency-issued smartphone or tablet as an indication it is the authorized user
2. Use of device certificates (see page 16)
3. CJIS-compliant standard authenticator protection of the secure location where CJI is stored

Understanding the concept of compensating controls

Law enforcement agencies around the country use a variety of technological and procedural methods to meet the requirements set forth by CJIS Policy. Although the document is comprehensive (more than 250 pages, mostly single spaced), there is allowance built in for agencies that find they are unable to meet the specified requirements. Compensating controls (addressed in CJIS Security Policy Section 5.13.7.2.1) are designed to permit alternative security processes that provide the same protection — or greater — in circumstances involving "legitimate business or technical constraints."

It's important to understand that temporary compensating controls are subject to approval at a state level and require the approval of the CSO who operates in conjunction with the respective state's CSA. While this allows for a degree of flexibility, it also introduces subjectivity due to two primary factors:

1. To be considered, the temporary alternative solution requested by the agency must be deemed to "meet the intent of the CJIS Security Policy AA requirement" and "provide a similar level of protection or security as the original AA requirement."
2. Compensating controls are "temporary control measures" and "expire upon the CSO approved date or when a compliant AA solution is implemented."

The above quoted excerpts are taken from CJIS Policy Section 5.13.7.2.1. The CSO has a great deal of authority in determining whether or not to approve a request for compensating controls and how long to allow it to remain in effect. More so than any other section of CJIS Policy, the compensating controls section intentionally allows agencies to propose alternative methods of authentication verification. Clearly, this may result in a degree of inconsistency. And some of the underlying policy wording may not be entirely clear to practitioners. The definition section of CJIS Policy includes this statement, for example, which may confound readers: "Additionally, compensating controls may rely upon other, non-AA, existing requirements as compensating controls and/or be combined with new controls to create compensating controls."[1]

As a result, determining which processes will be deemed acceptable compensating controls may be less than clear to tech practitioners. And because approval lies with a state-level CSO, what's permitted in another state may not be permitted elsewhere. In other words, if a vendor proposes a solution that's not clearly outlined in CJIS Policy but has been deemed acceptable in another state under the concept of compensating controls, your agency should do a good degree of due diligence. At a minimum, try to obtain a written description and justification of the specific compensating controls — and, if possible, contact the CSO who oversees your state (or write to your state's CSA) and ask for an opinion regarding acceptability and how long it would be allowed (remember, by policy, compensating controls are considered temporary).

A good example of compensating controls regarding smartphones use can be found in the CJIS Policy immediately following Section 5.6.4 Assertions. Review Figure 8 and specifically Use Case 7, "Advanced Authentication Compensating Controls on Agency-Issued Smartphones."

Device certificates

Device certificates uniquely identify a device and can be an effective method of authenticating the device to a system supplying CJI. However, the certificate alone isn't considered proof that the device is being operated by an authorized user. For certificates to be used as a compensating control, they must be:

1. Protected against extraction from the device
2. Configured for remote wipe on demand or self-deletion based on a set number of unsuccessful login or access attempts
3. Set up to use a secure authenticator such as a password or PIN to unlock the key and invoke its use for authentication

The third requirement is of particular relevance because it ensures the certificate is used to authenticate the device only after the user has allowed the certificate to be accessed. This prevents an unauthorized user from presenting the secondary level of authentication simply by having the device in their possession.

Author's Note: There's helpful and relevant discussion of certificate use in the G.4 Mobile Appendix of the CJIS Security Policy (see page G-46 of the policy).

Encryption requirements

Encryption isn't required for CJI that's "within a physically secure facility," which CJIS defines as generally consistent with the 24/7 operation within controlled access areas of a police building. However, whenever CJI is transmitted or stored (at rest) outside the boundaries of a physically secure location, encryption is required.

The exact standards that the data would be required to meet are detailed in CJIS Policy Section 5.10.1.2. At a minimum, the level of encryption for transmitted data must meet Federal Information Processing Standard (FIPS) 140-2 level, using a symmetric cipher key of at least 128-bit strength to protect the CJI. For data at rest, encryption must be compliant with FIPS 140-2 or FIPS 197, with a 256-bit strength cipher key. Products used to meet the FIPS standard must be certified and listed on the NIST Cryptographic Module Validation website.[3] Note that a claim of FIPS compliance by a vendor isn't sufficient. CJIS requires that a certification number be assigned.

Police agencies commonly use a virtual private network (VPN) to meet the encryption requirements of CJIS policy. A VPN functions as a secure tunnel that provides an end-to-end encrypted path between sender and recipient, thereby preventing interception of the data by unauthorized users.

Agencies may also utilize a technology known as Transport Layer Security (TLS), which is commonly used to provide secure transmission of financial transactions and other sensitive information.

One agency's path to CJIS compliance

There are different methods and technologies associated with CJIS compliance, but it can be helpful to consider what other organizations have done that has been approved by a CSA.

For gaining CJIS compliance with smartphones, there are three primary requirements: encryption, Advanced Authentication and MDM (see pages 16, 12 and 6, respectively). To be successful, an agency needs to integrate different products and processes in such a way that security requirements are met and the user experience isn't burdensome for the officers in the field. Below are the actual components and processes in place at a mid-sized California agency with a robust smartphone program. The methods used were deemed CJIS compliant. This information is provided only as an example, and it's important to remember that approval is granted at a state level. States may differ on their interpretation of CJIS Policy. Readers are strongly encouraged to submit their planned course of action to the appropriate CJIS authority before initiating procurement.

Summary of one agency's CJIS processes for smartphones

Officers are issued individual smartphones. At the time of assignment, the officer is asked to choose a six-digit PIN that meets CJIS requirements (see page 11). The officer is assigned a hard token that's used to obtain an OTP for the login sequence (described below). The security token and the supporting security service are products of Thales. The agency's active directory, which contains the officer's network username, is linked to the Thales security system. This ensures the multifactor authentication information is synced and updates are automatic, allowing for a seamless user experience and less IT maintenance. Once the security tokens are linked to the system, the agency IT administrator can assign and enroll the tokens.

When a smartphone is issued, it's also enrolled in the agency's MDM solution (Samsung's Knox Platform for Enterprise, or KPE), which downloads all relevant security policies and configurations, such as the device PIN requirement and idle lock. KPE exceeds the minimum CJIS requirements for MDM that are outlined on page 6.

Encryption of data in-transit is accomplished by using a VPN product from NetMotion that meets CJIS encryption requirements. NetMotion has the added benefit of session persistence, meaning the user stays logged on even when there's a drop in network connectivity, e.g., loss of cell signal. Encryption of data at rest is achieved with Samsung Knox Workspace, which encrypts work data on agency-managed devices whether a device is powered up or turned off. See page 16 regarding encryption requirements for data in transit and data at rest. More information on Knox solutions may be found on page 21.

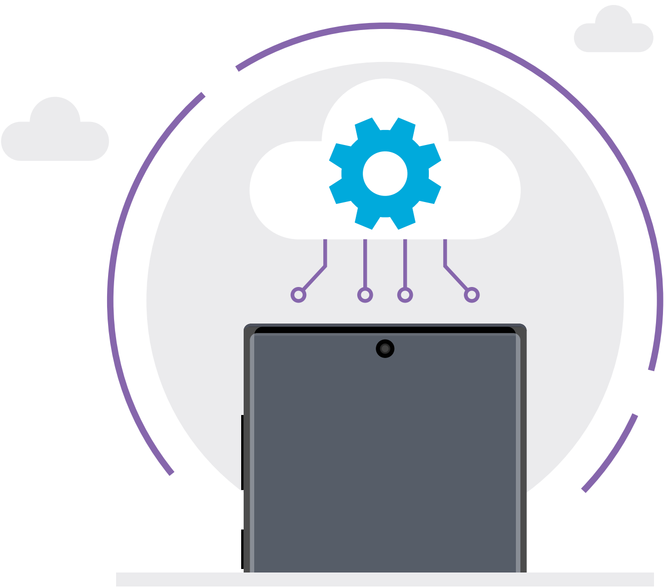
The agency's method of meeting Advanced Authentication requirements is best explained by the user experience when they log on. After unlocking the mobile device, the officer launches the NetMotion VPN client and is challenged for a username (same as contained in the agency's active directory) and a password. The officer enters their username and the six digits of their PIN. They then use the security token to obtain a six-digit OTP issued by the Thales security system. The officer enters this number after their PIN, resulting in a 12-digit number that completes the password field. When the Thales security program receives the user credentials at login, it ensures the first six numbers match the officer's PIN (something known) and the following six numbers match the numbers issued to the token (something the officer has), thus complying with the multifactor authentication requirement.

Important considerations

The agency in the above example found that the security token approach comes with some challenges. Tokens can be lost or damaged, and the supporting battery has a lifespan of about 3 years, depending on the frequency of use. The agency is now considering moving to a "soft" token approach, which would require officers to obtain an OTP via a smartphone app separate from the login process. Parallel to the multifactor authentication outlined above, after the officer enters their PIN, they enter this randomly generated six-digit number. This soft token approach may be considered compliant with the CJIS requirement for a code to be sent through a "separate communication service channel" as described in CJIS policy section 5.6.2.2.

The integration and coordination of the components outlined above require a skilled IT person. Most midsize and larger agencies will likely have a capable resource within their city or county IT staff. Agencies that don't have such a resource should consider working with a larger or regional agency that may be able to handle some or all of the security-related IT tasks. An appropriate place to make an initial query is with the agency that handles the county or regional switch for NCIC data. An alternative approach is to work with an IT integrator that specializes in helping agencies achieve CJIS compliance.

Cloud services



Forward-thinking agencies are quickly recognizing the value of cloud services in increasing the effectiveness of their smartphone programs. Although independently beneficial, a smartphone program paired with cloud services allows officers wider access to a greater level of mission-critical and mission-essential information — whenever and wherever they need it.

Law enforcement commonly uses a variety of technology-driven force multipliers, including license plate readers, in-vehicle video systems and body-worn cameras, all of which generate large amounts of data and place huge demands on even the most robust department-maintained servers. Archived records and photos can also provide significant benefit — but only if they can be readily accessed from the field.

Cloud services can be a cost-effective way to ensure personnel have maximum capability with their smartphones in the field. The evergreen cloud platform allows agencies to utilize a variety of mobile capabilities in a modern and secure framework. Mobile apps designed to support public safety operations are rapidly evolving. And these apps are increasingly being paired with cloud services that perform data processing and storage outside the mobile device, enabling greater capabilities and efficiency. These apps also have the advantage of regular updates and less vulnerability to cyber threats.

Cloud-based storage is easily scalable, continually updated and maintained 24/7 by cyber professionals. With cloud storage, complex responsibilities like maintaining a disaster recovery solution no longer rest with the agency. Cloud storage also makes it possible to provide resources like detailed building diagrams during a rapidly unfolding tactical incident.

CJIS considerations for cloud computing

CJIS has specific rules regarding the use of cloud computing for CJI. CJIS Security Policy Section 5.10.1.5 covers the core requirements with extensive guidance provided in Appendix G.3, pages G-15 through G-31. CJIS Policy recommends that agencies also review NIST Special Publications 800-144, 800-145 and 800-146. Agencies interested in utilizing cloud services to access, store or transmit CJI must be prepared for due diligence, including these important considerations:

1. Although there are numerous cloud-based services and cloud computing vendors, only a small percentage meet CJIS requirements. Be cautious of providers who claim "CJIS certification"; there is no central CJIS certification or accreditation authority. Ensuring compliance with CJIS Policy is the shared responsibility of FBI CJIS, CJIS Systems Agencies and the State Identification Bureaus. Accordingly, each CJIS review is unique, and an authorized solution in one state may not be acceptable in another. There may even be differences within the same state, due to variables inherent in law enforcement processes.

2. Ultimate responsibility for CJIS compliance rests with the law enforcement agency, not the vendor. Although using cloud services is an effective way to manage and access data, agencies should not assume that a cloud solution will transfer total responsibility to the cloud provider. Agencies are still responsible for areas such as training, policy, device and data security, as well as the specific responsibilities applicable to the device type (such as those in CJIS 5.13 for mobile devices).

3. Plan on a collaborative approach and start with the person responsible for CJIS compliance at your agency (often the NCIC coordinator). Determine if other agencies already have the capability that you're seeking and learn from their process. Ask to review a copy of their CJIS application. Work with your mobile device provider so you understand and utilize built-in security features. Carefully vet potential cloud vendors and ask them for referrals to agencies already using their services. With CJIS, experience counts.

Pathway to change: The CJIS advisory process

Author's Note: The information provided on this page has been derived from the website of the CJIS Division of the FBI and has been condensed for inclusion in this publication. Readers are encouraged to visit the CJIS Advisory Process page[4] for more information.

The CJIS advisory process was established by the FBI to facilitate interaction with the user community and establish a method for reviewing technical and operational issues related to all CJIS Division programs. In keeping with the shared management approach of CJIS, the advisory process is administered by the CJIS Advisory Policy Board (APB), which includes 35 representatives from criminal justice agencies and organizations from across the United States. Twenty of those representatives are chief executives at the state or local level. Supporting the CJIS APB are regional working groups, featuring a state and local representative from each state.

CJIS has established a process to submit ideas and proposals through the advisory process, which can be an effective way for an agency, group of agencies or an organization to seek change and/or guidance on emerging technology. A biannual solicitation for agenda items is sent out to all CJIS APB members, and topics can be submitted at any time by the following process:

1. Download the topic discussion form[5]
2. Submit form in writing and include:
   - Clear statement of request
   - How the subject of the topic is currently handled
   - Suggested solution
   - Scenario/example
   - Outline of the benefits to the criminal justice community
   - Description of the impact on state/local agencies or the users of the system
   - Degree of importance
   - Contact information

State and local agencies should submit their proposals to their state's CSO, who will be responsible for the initial review. Professional organizations may submit topic proposals directly to the CJIS Division of the FBI. Ensure that the extent of any problem or challenge is clearly explained so that, if change is required, the reviewers can establish a priority.

Proposals are subsequently sent to the CJIS Training and Advisory Process (CTAP) unit. FBI personnel conduct an analysis on each proposal to determine whether it will be considered at the next set of advisory process meetings. Proposed changes are reviewed by the APB working groups, and the CTAP unit advances the proposal to the APB for further deliberation. After the proposal has been reviewed by the APB, a recommendation is sent to the FBI director. If the director agrees with the APB recommendation, CJIS staff then enacts the change.

While this process may seem arduous, the initial submission form is relatively straightforward. Agencies and organizations who are eager to embrace emerging or alternative technologies can ultimately achieve more effective CJIS compliance.

Incident Reporting

CJIS Policy notes that a significant level of smartphone vulnerability is related to the device's form factor, i.e., smaller mobile devices are easily stolen, misplaced or lost. CJIS recommends responding to these incidents rapidly in order to mitigate the risks associated with either illicit access of data on the device itself or unauthorized use of the device to access online data resources.

This is most effectively accomplished through policies that issue devices to individuals and assign levels of accountability consistent with other high-value or sensitive equipment, e.g., radio, firearm, badge, ID card.

Officers should be required to immediately report a device compromise or loss, and their agency's MDM must be utilized to remotely suspend, disable or wipe the compromised device as appropriate.

Tracking considerations

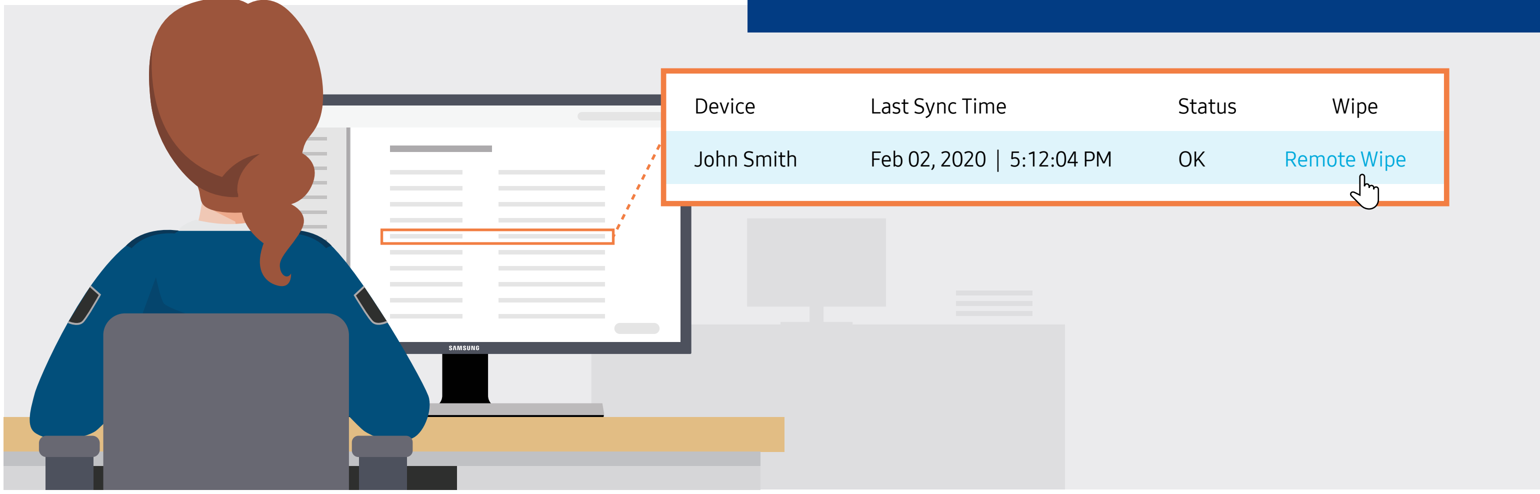
MDM software may allow a lost or stolen smartphone to be tracked down via GPS. While this capability doesn't circumvent the requirements for secure storage, it could aid in the recovery of a device — and substantially reduce the time that the device might be exposed to unauthorized use. Although location tracking isn't currently required by CJIS policy, the CJIS Mobile Appendix G-4 recommends that it "be applied to agency owned devices where possible as a risk mitigation factor." Appendix G-4 also addresses device tracking in BYOD scenarios, noting, "Enabling of device tracking on personally owned devices in a BYOD environment may raise employee privacy concerns and should be considered only for critical systems with the full knowledge of the employee and concurrence of the legal department."

The importance of device updates

Regular security patches and updates are key to protecting devices from cyberattacks. CJIS Policy requires agencies (or supporting vendors) to develop and implement an update policy that ensures prompt installation of newly released security-relevant patches, service packs and hot fixes. CJIS recommends those polices include these processes:

- Patch testing before installation
- Rollback capabilities when installing patches or updates
- Automatic updates without individual user interaction
- Centralized patch management

Managing device updates is a key function of an effective and full-featured MDM. Agencies should have a solid working knowledge of the capabilities of their MDMs and leverage them to remotely maintain their mobile devices.



Device	Last Sync Time	Status	Wipe
John Smith	Feb 02, 2020 | 5:12:04 PM	OK	Remote Wipe

How Samsung secures devices and supports device management

Samsung offers powerful solutions to secure data and manage devices for optimal security.

Knox security platform: Every Samsung smartphone and tablet is built on the Knox platform, which is Samsung's implementation of the Android OS. Knox is designed to satisfy the stringent security demands of regulated industries such as law enforcement, finance and healthcare. Rather than merely validate the integrity of the device at boot-up or login, Knox constantly verifies device integrity via a chain of security checks, starting at the hardware level and extending to the OS. Knox detects any tampering attempts and locks down at-risk devices. It also encrypts data stored on the device, even when the device is turned off or reset.

To achieve this advanced security, the Knox platform leverages a process architecture known as TrustZone, in which highly sensitive computations are isolated from the rest of the device's operations. It also uses real-time kernel protection to constantly inspect the core of the OS during run time, and it protects apps and data by strictly defining what each process is allowed to do and what data it can access.

Samsung has partnered closely with Google to ensure alignment of Knox and Android Enterprise security features.

Knox Platform for Enterprise (KPE): KPE provides tools for regulated organizations, such as law enforcement agencies, to address their unique security challenges, like CJIS compliance. It provides Samsung-specific security enhancements and complements standard Android Enterprise security features, such as Android Work Profile. As an optional component of KPE, Sensitive Data Protection (SDP), a feature unique to Samsung, allows KPE to encrypt work data on every agency-managed device while it's powered on. This is an improvement on the industry norm, which is to encrypt data at rest when the device is powered down.

Integration with leading MDMs: Agencies need an MDM platform to effectively manage smartphones and tablets. KPE and Knox Mobile Enrollment integrate with more than 20 top MDM platforms. In the Knox solution set, Samsung offers several enterprise-grade tools to help admins manage mobile devices throughout their life cycle:

- **Knox Configure:** Agencies can use Knox Configure to remotely provision and configure devices in bulk. After configuring devices at launch, you can change these configuration profiles as needed and push them to clients over the air.

- **Knox Mobile Enrollment:** You can automatically bulk enroll devices in an EMM with Knox Mobile Enrollment — for free.

- **Knox Manage:** Samsung's cloud-based EMM platform, Knox Manage allows agency admins to better manage Android, iOS and Windows 10 devices. Knox Manage lets you blocklist particular apps and websites, and it enables remote device control, device location tracking and remote wipe.

- **Knox Enterprise Firmware-Over-The-Air (E-FOTA):** IT admins can remotely deploy OS and security updates to corporate devices with Knox E-FOTA — no user interaction required. Updates can be tested before deployment to ensure your existing apps will keep running smoothly. For greater device security, you can deploy regular security patches on a set schedule.

- **Knox Capture:** A highly adaptable solution, Knox Capture supports scan logic for business apps. With an intuitive UI and powerful scanning engine, Knox Capture can be used to manage the input, formatting and output configuration of scanned barcode data, without writing a single line of code.

- **Knox Asset Intelligence:** A data-driven analytics solution, Knox Asset Intelligence provides operational visibility and delivers actionable fleet-level insights about your deployed Samsung devices.

Samsung DeX extends mobile devices for in-vehicle computing

Samsung's DeX platform allows agencies to further extend the utility of an officer's smartphone so it can deliver a desktop computing experience in a patrol vehicle or at the station. By connecting the officer's smartphone to a full-sized monitor (via an HDMI adapter, or wirelessly to any Miracast-enabled display), DeX allows mobile and web apps to be navigated on a larger screen with a keyboard and touchpad or mouse.

Across the U.S., a growing number of agencies are leveraging DeX to replace in-vehicle laptops, resulting in significant cost savings, improved user experience and more comfortable vehicle ergonomics. A study by the Public Safety Network estimated that transitioning to DeX could save agencies more than 15 percent in the first year of use, with likely savings of about 30 percent in each of the following two years.[6]

As agencies consider adopting innovative mobile solutions like Samsung DeX, it's even more critical that they establish a strong framework for CJIS smartphone compliance.

Conclusion

Smartphones allow officers to work much more efficiently in the field, providing unrivaled utility that improves officers' situational awareness and their overall effectiveness. With a robust CJIS-compliant smartphone program, officers gain full access to mission-critical and mission-essential information — regardless of their assignment or proximity to a patrol vehicle — resulting in a significant ROI.

Failure to properly safeguard data subject to CJIS Policy can result in revoked access, leaving information gaps across departments. Conversely, following CJIS policy and implementing a strong MDM/EMM plan, alongside officer-friendly Advanced Authentication, will allow agencies to maintain reliable CJI access for their officers, wherever they may need it.

Footnotes

1. https://www.fbi.gov/file-repository/cjis_security_policy_v5-9_20200601.pdf/view
2. https://www.nccoe.nist.gov/projects/use-cases/mobile-sso
3. https://csrc.nist.gov/projects/cryptographic-module-validation-program
4. https://www.fbi.gov/services/cjis/the-cjis-advisory-process
5. https://www.fbi.gov/file-repository/cjis_topic_paper_submission_form.pdf/view
6. https://www.samsung.com/us/business/short-form/bringing-mobile-first-to-public-safety/

This white paper is for informational purposes only. Samsung makes no warranties, express or implied, in this white paper.

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

Follow us: youtube.com/samsungbizusa | @SamsungBizUSA

SAMSUNG