Protecting Criminal Justice Information: Achieving CJIS Compliance on Mobile Devices
Protecting Criminal Justice Information: Achieving CJIS Compliance on Mobile Devices

It’s common today for law enforcement officers in the field to receive dispatch calls or access a subject’s arrest record via mobile technology. But what about a detective fingerprinting a murder victim at the scene of the crime and learning his identity instantly? Or an officer finding a missing person just hours after a department in another state posted the report? What if every photo of a crime scene had the time and location automatically recorded for evidential purposes? Mobile devices are making these scenarios possible by enabling dispatched officers to access and update criminal justice information (CJI) databases in real time.

The Criminal Justice Information Services (CJIS) department recognizes that mobility is playing an increasingly central role in law enforcement. Every year, CJIS releases an updated version of the CJIS Security Policy, which “provide[s] appropriate controls to protect the full lifecycle of CJI,” which includes a growing body of regulations governing information that is viewed, transmitted and stored electronically. Version 5.3, published in August 2014, includes regulations that are specific to mobile devices. Requirements in the new Policy Area 13 govern the use and management of mobile devices and address how existing policies apply to mobile. Policy Area 13 replaces the Mobile Appendix that appeared in the 2013 version of the policy, which outlined the future policies that this version makes effective.

This white paper provides guidelines for securing mobile devices accessing CJI, in accordance with the requirements of CJIS Security Policy Area 13: Mobile Devices, and provides an overview of how AirWatch technologies help support CJIS compliance. CJIS specifies that agencies must authorize, monitor and control wireless access to CJI for all wireless technologies, including all wireless access points, as well as cellular, Bluetooth, satellite, microwave and land mobile radio devices.

Mobile Device Management

For the first time this year, the CJIS Security Policy specifically calls out the use of smartphones and tablets. The CJIS Security Policy previously recommended mobile device management (MDM) as “necessary in most cases.” The Policy now requires law enforcement agencies to implement MDM. Previously, CJIS recommended centralized administration capable of remotely locking or wiping mobile devices, setting and locking device configuration, detecting jailbroken or rooted devices and enforcing folder- or disk-level encryption.

The updated policy adds “application of mandatory policy settings on the device and detection of unauthorized configurations or software/applications” to that list. Additionally, MDM must be used to “ensure that CJI is only transferred between CJI authorized applications and storage areas of the device,” and not stored or transmitted in unmanaged applications or areas (Section 5.13.2).
Wireless Device Risk Mitigations

CJIS requires that law enforcement agencies perform the following actions to maintain compliance on cellular and wireless devices:

Apply Available Critical Patches and Upgrades

New operating systems and software can introduce new threats and vulnerabilities, so it is critical to apply security patches and upgrades as soon as they are available. All users should also run the latest versions of any MDM or enterprise mobility management (EMM) applications. From the central console, AirWatch® administrators can view the OS version and app versions on devices in their deployment, and even push updates to users’ devices over the air (OTA). For device platforms that do not allow OTA updates, AirWatch administrators can prompt and require users to download the latest OS and application updates.

It is critical to choose an MDM or EMM solution that offers same-day support for new devices and OS versions. If a user purchases a new device or downloads an OS update that the MDM software does not support, the device will not be secured until the MDM provider comes out with an update. AirWatch works alongside the leaders in mobile technology and offers same-day support for new devices and OS updates across manufacturers. AirWatch supports all major devices and operating systems, which can be a key component in maintaining compliance.

There will often be a variety of devices that need access to CJI, such as a police officer running a tag on a tablet before he or she gives a ticket, or an officer delivering a parking ticket from a rugged device. A smartphone may be used in or outside the office to access CJI. The AirWatch management console is a central point to monitor and secure each device, regardless of location or form factor. For IT, this significantly reduces complexity in mobility management by unifying management across an entire organization. From a single point, administrators can apply patches and updates and see real-time views of all devices in a deployment and the software they are running.

Configure Devices for Local Device Authentication

CJIS requires mobile devices that access CJI to have local device authentication, or device-level passcodes. According to the CJIS Security Policy, when agencies implement the use of a PIN as a standard authenticator, they should:

- Be a minimum length of eight characters of 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 the previous 10 passwords
- Not be transmitted in the clear outside the secure location
- Not be displayed when entered
The standards are not quite as strict when a PIN is used for advanced authentication along with a certificate or token. If a PIN is entered to invoke a certificate or other form of advanced authentication, which is required in certain situations, it must meet the following requirements:

- Be a minimum of six digits
- Have no repeating digits (i.e., 112233)
- Have no sequential patterns (i.e., 123456)
- Not be the same as the User ID.
- Expire within a maximum of 365 calendar days.
- If a PIN is used to access a soft certificate which is 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 (3) PINs.
- Not be transmitted in the clear outside the secure location.
- Not be displayed when entered.

CJIS has added an exception to these requirements in the 2014 policy: When a PIN is used only for local device authentication, the only requirement is that it be a minimum of six digits.

With AirWatch, administrators can set security profiles to achieve each of the above requirements. For advanced security, administrators can require the use of a combination of numbers, letters and complex characters for passcodes up to 16 characters long.

Additionally, administrators can set a profile that will automatically wipe data from a device after a specified amount of failed login attempts. The CJIS Security Policy recommends configuring a remote wipe after a specified amount of failed login attempts based on the value placed on the information residing on the device. In addition, AirWatch can configure short session lock times and reset passcodes over the air (OTA) to help keep devices secure if they are left unattended.

**Use Advanced Authentication**

CJIS has added section 5.6.2.2 to clarify the situations that require advanced authentication (AA), which confirms the identity of a user beyond a username and password. According to the CJIS Security Policy, “The requirement to use or not use AA is dependent upon the physical, personnel, and technical security controls associated with the user location and whether CJI is accessed directly or indirectly.” Advanced authentication is required except in the following situations:

- When the user is requesting access to CJI from a secure location (see section 5.9 for secure location requirements)
- When technical security controls have been met (sections 5.5 and 5.10)
- When the user has only indirect access to CJI
CJIS has included a decision tree in this year’s policy to help agencies determine whether or not they should use advanced authentication.

When advanced authentication is required, agencies must use two of the following three factors for authentication on mobile devices: something you know (i.e. password), something you have (i.e. token), something you are (i.e. biometric).

With AirWatch, administrators can require multifactor authentication by enforcing a passcode at the device level and enforcing a secondary authentication method at the application or network level. AirWatch supports authentication through the use and implementation of software tokens, hardware tokens, smart cards, certificates and biometrics such as fingerprint scanners. AirWatch applications will soon integrate with EyeVerify to support secondary biometric authentication using eye vein verification. AirWatch also supports authentication with username/password, directory services credentials, SAML, or proxy authentication methods. Organizations can also leverage AirWatch® App Wrapping AirWatch and the AirWatch® Software Development Kit to create additional layers of authentication and security for public or custom applications.

The policy also outlines specific requirements for the storage of certificates or cryptographic keys on mobile devices. When used as an authentication method, certificates and cryptographic keys must be protected against being extracted, be configured for remote wipe on-demand and be configured to use a secure authenticator such as a PIN or password to unlock the key for use. Secure AirWatch applications also require users to enter a PIN and pass a second layer of authentication to allow secure access to CJI. AirWatch can be configured to automatically and remotely perform a device wipe after a certain number of failed logins or after any action that the administrator pre-sets to trigger a device wipe.

AirWatch supports protection against certificate and cryptographic key extraction by supporting devices which comply with this standard with a native key store.

Compensating controls for meeting the AA requirement

In this year’s policy, CJIS for the first time lists CSO-approved compensating controls to temporarily meet the AA requirement when an agency cannot meet requirements due to legitimate technical or business constraints. Compensating controls must meet the intent of the AA requirement, provide a similar level of protection and not rely upon existing requirements for AA as compensating controls.

To meet compensating control requirements, mobile device management must be implemented and provide at least two of the following:

- Possession of the agency issued smartphone, tablet, or iPad as an indication it is the authorized user
- Implemented password protection on the mobile device management application and/or secure container where the authentication application is stored
- Enable remote device locking
- Enable remote data deletion
- Enable automatic data wipe after predetermined number of failed authentication attempts
- Remote device location (GPS) tracking
• Require CJIS Security Policy compliant password to access the device
• Use of device certificates

Administrators can use AirWatch® Mobile Device Management controls to implement, enable and require all of the above requirements.

Encrypt All CJI Data Resident on the Device
Device-level encryption enables users to encrypt sensitive information stored on mobile devices. Mobile device manufacturers support their own device level FIPS 140-2 validation by developing cryptographic modules or using pre-validated OpenSSL cryptographic modules at the device level. AirWatch users should be aware of the FIPS 140-2 certification of the device types in their deployment to ensure an end-to-end secure mobile architecture.

For devices that include device or SD card-level encryption, AirWatch can enforce the use of encryption remotely from the console, for both in-device drives and removable drives. For hosting platforms and device applications that do not exercise FIPS 140-2 validated cryptographic modules or libraries, AirWatch supports FIPS 140-2 validated solutions such as AirWatch® Secure Content Locker®, which uses the FIPS 140-2 validated OpenSSL AES-256 cryptographic module to provide encryption for data at rest and in transit.

AirWatch also includes a number of data loss prevention features administrators can use as an additional safeguard for CJI. Features like hyperlink and document stripping in emails, disabling Apple AirDrop and using advanced data loss protection (DLP) policies in AirWatch Secure Content Locker can reinforce security around content.

With AirWatch Secure Content Locker, administrators can employ advanced DLP settings. Documents can be given expiration dates to ensure content on the device consists of only the most up-to-date and necessary documents. Administrators can also leverage geofencing to set a virtual perimeter within which users can access sensitive data. Once a device leaves the perimeter, access is automatically disabled.

Erase Cached Information When Session is Terminated
The CJIS Security Policy requires that any browser accessing CJI must erase all cached information when the session is terminated. With AirWatch, administrators can disable native browsers and public browser applications to drive all browsing through the secure AirWatch® Browser. With AirWatch Browser, a user’s browsing cache and cookies can automatically be cleared each time the browser is closed. Administrators can also customize web browsing, whitelist and blacklist websites, leverage existing web filters and more.

AirWatch Browser is pre-configured to use app tunneling through the AirWatch® Mobile Access Gateway to proxy access to internal resources in a LAN. The AirWatch Mobile Access Gateway provides a single, secure point of entry for all compliant devices to access enterprise services. Communication between AirWatch Browser and internal networks is encrypted using TLS/SSL and certificate-based authentication. Administrators can enable VPN-like functionality without requiring a third-party VPN on the device.
Employ Personal Firewalls or Run a MDM System that Facilitates the Ability to Provide Firewall Services from the Agency Level

The CJIS security policy recommends the following capabilities for firewall services:

- Audit and limit the applications installed on the device – From the AirWatch console, administrators can audit applications, disable applications, blacklist certain apps and run reports on usage.

- Block unsolicited requests to connect with the device – AirWatch enables administrators to prevent unknown devices from connecting to corporate networks and can configure certificate-based access to corporate applications, email, VPN and Wi-Fi networks.

- Filter incoming traffic by IP address or protocol – AirWatch VPN On Demand and AirWatch AppTunnel enable administrators to grant access based on group, allowing or denying access to sites based on IP address.

- Filter incoming traffic by destination points (same as above) – AirWatch can enforce a global proxy that forces all traffic to be routed through the VPN back to the company and then disseminated from the organization's network. For devices that don’t have global proxies, administrators can configure mandatory VPN to route traffic through the organization’s network. After the route is configured, all traffic will go through the organization’s existing web filtering.

- Maintain an IP traffic log – As stated by CJIS, this may not be feasible on most mobile operating systems, but could be run on applications that communicate over or accept connections from a secure network.

AirWatch also partners with several network access control (NAC) providers to filter traffic and ensure the security of Wi-Fi networks.

Employ Antivirus Software or Run a MDM System that Facilitates the Ability to Provide Antivirus Services from the Agency Level

AirWatch can push antivirus applications to devices and integrate with various antivirus software providers. As stated in the CJIS Security Policy document, “One method to compensate for the technical infeasibility of traditional anti-virus and malicious code protection is to install an MDM that performs periodic system integrity checks that validate device configuration and status against an approved baseline.”

From the AirWatch console, administrators can schedule and run routine device integrity checks to ensure the device has not been compromised. With the AirWatch compliance engine, automated actions can be configured to act upon unauthorized actions such as jailbreaking or rooting a device. For example, if a device is found to be in a compromised state, the AirWatch compliance engine can automatically wipe all CJI data off the device to ensure the organization remains compliant with the CJIS Security Policy and that all CJI data remains out of malicious hands.

Other Considerations

The CJIS Security Policy outlines several other factors that necessitate the use of third-party management software, such as the ability to manage multiple users, implement audit and accountability functions and require local device authentication. These requirements cannot be met with a limited function operating system alone and require the use of MDM.
The Policy now also requires “enhanced incident reporting and handling procedures to address mobile device operating scenarios.” According to CJIS, “Rapid response to mobile device related incidents can significantly mitigate the risks associated with illicit data access either on the device itself or within online data resources associated with the device through an application or specialized interface.” CJIS requires special procedures for loss of device control, the total loss of a device or any form of device compromise.

AirWatch helps administrators meet these requirements through both automated, pre-set actions and remote capabilities that can be performed on demand. The AirWatch compliance engine enables administrators to automate escalating actions when certain conditions are met. For example, a pre-set profile can trigger a device to automatically lock after a specified period of time. Administrators can also remotely lock a device that has left agency control or is suspected to be compromised, as well as change the password. Any device can be remotely wiped of all content and restored to factory settings at any time.

### Preparing for the Future

When handling and protecting CJI, there are measures organizations can take to go beyond the minimum security requirements set forth by the CJIS Security Policy. Over time, more risks will emerge, and remaining a step ahead of new threats can help organizations remain compliant even as policies evolve and change. An organization should look to an EMM provider that has the ability to scale with the organization and provide same-day support for all OSes and new devices. With a properly configured EMM solution in place, organizations can be prepared for an audit at a moment’s notice.

A complete EMM solution set such as AirWatch® Enterprise mobility Management gives organizations the ability to protect CJI beyond basic requirements and give field officers and government officials unprecedented access to the data they need to protect and serve.

For more information, visit the [FBI CJIS Security Policy Resource Center](#).
Additional Resources

For additional information, visit: www.air-watch.com/industries/government

To get started with a free trial of AirWatch, visit www.air-watch.com/free-trial.

AirWatch Global Headquarters
1155 Perimeter Center West
Suite 100 Atlanta, GA 30338
United States
T: +1 404 478 7500
E: sales@air-watch.com

About AirWatch by VMware

AirWatch by VMware is the leader in enterprise mobility management with a platform including industry-leading mobile device, email, application, content and browser management solutions. Acquired by VMware in February 2014, AirWatch is based in Atlanta and can be found online at www.air-watch.com.