LEADS Daily Briefing
for April 16, 2020

CJIS Security Policy - Mobile Devices

The use of any mobile computing device to access LEADS/NCIC/III, or any other information system which contains Criminal Justice Information (CJI), is subject to additional security requirements per FBI CJIS Security Policy (CSP). The CSP defines a mobile device as any portable device used to access CJI via a wireless connection (e.g. cellular, WiFi, Bluetooth, etc.). These devices may be smart phones, tablets or laptops which can be removed from a secure location.

It is important that agencies wishing to implement any type of mobile computing solution that accesses CJI first ensure the implementation complies with all aspects of the CSP including Policy Area 13: Mobile Devices, and Policy Area 6: Identification and Authentication. Agencies should pay particular attention to Policy Areas 5.13.2 Mobile Device Management (MDM) and 5.6.2.2 Advanced Authentication. These two policy areas (along with all other CSP policy areas) must be in place prior to a mobile device accessing CJI.

The LEADS Administration staff maintains a process of reviewing compliance with CSP prior to granting requests for additional CDCs.

For assistance with the CJIS Security Policy please contact the Illinois CJIS Information Security Officer, Derek Blaszkiewicz, at 815/740-3064 or via email derek.blaszkiewicz@Illinois.gov

Operator's Initials	Date	Operator's Initials	Date	Operator's Initials	Date	Operator's Initials	Date	Operator's Initials	Date