*** * * * ATTENTION: AGENCY TAC/POC * * * ***

REVIEW AND DISTRIBUTE THIS NOTICE ACCORDINGLY

Extension for Advanced Authentication Requirement

Notice:

Effective February 20, 2013, the requirement to implement Advanced Authentication (AA) under the two exceptions in Section 5.6.2.2.1 of the CJIS Security Policy has been extended to **September 30, 2014**. This includes considering a police vehicle a physically secure location. This extension was granted after the FBI agreed to a request from the CJIS Advisory Policy Board (APB) Chair and the APB Executive Committee to extend the time agencies had to implement AA.

What Does This Mean:

The CJIS Security Policy states that AA is required when a request for FBI CJIS-provided criminal justice information (CJI) originates from an area that is not physically secured, or the physical origin of the request cannot be determined. Additionally, if a request for CJI originates from within a physically secure location but certain technical security controls have not been implemented, then AA is required.

See Section 5.9 for the definition and requirements of a physically secure location, and Sections 5.5 and 5.10 for technical security control requirements.

The FBI provided two exceptions to the policy for the purposes of interim compliance:

1. For information systems accessing CJI from devices associated with *and* located within police vehicles if the information system was not procured or upgraded anytime after September 30, 2005. The FBI considers a police vehicle a physically secure location until September 30, 2013 for the purposes of this policy.

2. If IPSec was implemented to meet the AA requirements in Version 4.5 of the CJIS Security Policy.

Most agencies in North Carolina that use DCIN fall under the second exception, and, therefore, had until September 30, 2013 to implement AA. IPSec was funded to meet the AA requirements in Version 4.5 of the CJIS Security Policy, and is required when connecting to LEMS to use DCIN. The most common implementation of IPSec to connect to DCIN is by establishing a Virtual Private Network (VPN) utilizing a Cisco ASA 5505 adaptive security appliance.

Because the FBI agreed to the extension, the CJIS Security Policy will be updated reflecting the new drop-dead date of **September 30, 2014**.

Even though the extension has been granted, agencies are still encouraged to move towards AA implementation as soon as possible. Please note that if your agency does not fall under either exception noted above, your agency is already required to have AA implemented.

Questions regarding this extension or the AA requirement can be directed to the NC DOJ Information Security Officer, Brian Dickerson, at bdickerson@ncdoj.gov, or SBI Assistant Special Agent in Charge Joshua Hickman at jhickman@ncdoj.gov.