Oregon
John A. Kitzhaber, M.D., Governor

Department of State Police
Law Enforcement Data System
P.O. Box 14360
Salem, OR 97309-5074
(503) 378-3055
FAX (503) 364-2661

March 14, 2012

To All LEDS Representatives and Agency Administrators:

I want to take a minute to address some issues that we are getting many questions on, and they are the security requirements for IT staff or contractors who service your networks and servers that access criminal justice information (CJI), the Security Awareness Training requirements for all persons with physical and logical access to the equipment used to access CJI including information technology administrators and staff , and the Two-Factor or Advanced Authentication requirements for devices used to access CJI.

Personnel Security: In accordance with the FBI CJIS Security Policy Version 5.0, all persons who have unescorted access to CJIS Secure Areas, including server rooms that house the equipment that provides access to CJIS information from LEDS or NCIC, must undergo a state and national fingerprint-based criminal history check. The policy also requires any person who works on, modifies, repairs or maintains the equipment used to provide access to CJIS information, whether they are escorted or not, to undergo the same state and national fingerprint-based background check. CJIS secure areas also include all areas where terminals that can access LEDS/NCIC CJIS information are located.

Security Awareness Training: Basic security awareness training is required within six months of initial assignment, and biennially thereafter, for all personnel who have access to CJI. The CJIS Security Policy, Section 5.2 provides the minimum security awareness topics required for those with access to CJI, those with both physical and logical access to CJI, and all Information Technology personnel (system, security, and network administrators and staff, etc.). Records of individual basic security awareness training and specific information system security training shall be documented, kept current, and maintained by LEDS.

For Oregon, the CJIS Security Awareness Training is available online at the Law Enforcement Data System training portal, https://www.cjisonline.com/. Coordinate directly with your agency LEDS Representative for instructions on how to access and complete the training. The LEDS policy regarding the CJIS Security Awareness Training can be found on our secure site at, http://www.oregon.gov/OSP/CJIS/Secure_Link/LEDS_Manual.shtml, Chapter 8 in the LEDS Representative Manual section. If LEDS Representatives have any questions, please contact the LEDS Training Office at 503-378-3055, extension 55015. For agencies that were waiting for a letter from LEDS advising them to conduct the training, this serves as that letter.

Security/Advanced Authentication for Devices: Many agencies are providing staff with business cell phones, laptops, and other devices and there is a natural transition to want to be able to access CJI information on these devices. This is possible, but there are some specific security requirements that must be implemented, and agencies should not provide the capability until the security requirements are in place.

For devices that are accessing CJI from a non secure area you must comply with the Advanced Authentication requirement outlined in the CJIS Security Policy chapter 5.6.2.2.1. Follow the decision tree in chapter 5.6.2.2.2 to assist you in determining if Advanced Authentication applies to your specific circumstance.

CJIS Security Policy Version 5.0, Section 5.5.7.3, outlines the requirement for accessing CJI via hand held devices.

Organizations shall, at a minimum, ensure that cellular devices: 1) Apply available critical patches and upgrades to the operating system, 2) Are configured for local device authentication, 3) Use advanced authentication, 4) Encrypt all CJI resident on the device, 5) Erase cached information when session is terminated, 6) Employ personal firewalls, and 7) Employ antivirus software.

Any hand held device that does not comply with CJIS security requirements is not authorized for use in accessing and processing CJI information. Please anticipate being required to identify the advanced authentication method that will be used for all hand-held device terminal access requests. These same requirements apply to any mobile device or laptop that is not secured in a vehicle. Once the device leaves the area which is considered a CJIS secure area, advanced authentication is required, in order to access your LEDS application.

The CJIS Security Policy can be found at:

http://egov.oregon.gov/OSP/CJIS/docs/CJIS_Security_Policy_Ver5_02092011.pdf

Please contact me at 503-378-3055, extension 55020 with any questions.

Sincerely,

Terry O'Connell
Director, LEDS