GENERAL ORDER

37

EFFECTIVE: January 7, 2014

REVISED:

SUBJECT: CJI Security

ISSUED BY: Fernando M. Solorzano

I. PURPOSE

Ensure compliance with CJI Security requirements as per FBI CJIS Security Policy §5.9. For the purpose of this policy, all information provided by the CLETS network is considered CJI.

II. PHYSICALLY SECURE LOCATION

The Communications Center, Communications/Records Supervisor's office and Lead Dispatcher's office are designated as the Physically Secure Location. Unauthorized removal of CJI material is prohibited.

III. SECURITY PERIMETER

The door to the Communications Center is the Security Perimeter of the Physically Secure Location. All personnel who pass through the security perimeter must be authorized and are subject to Access Control or Visitor Control procedure(s) below.

IV. PHYSICAL ACCESS AUTHORIZATIONS

Only personnel authorized and credentialed by the authority of the Chief of Police may have unescorted access into the Physically Secure Location. Personnel may only enter the Physically Secure Location to conduct official business. The list of authorized personnel shall be provided to the Lock Shop to allow for programming the appropriate access control device(s).

V. PHYSICAL ACCESS CONTROL

The Security Perimeter must be secured at all times. Authorized personnel that require access to the Physically Secure Location must do so by utilizing a personally issued credential (proximity-enabled ID card or fob). Every person entering the Physically Secure Location must present his/her credential to the Access Control Device for each entry. Multiple personnel may NOT enter the Physically Secured Location simultaneously unless each person presents his/her credential to the Access

Control Device (even if the door is open). In the event an employee requires access to the Physically Secure Location and does not have his/her credential, Visitor Control procedures apply. Electronic logs of entries into the Physically Secured Location must be maintained for three (3) years.

VI. VISITOR CONTROL

All non-credentialed visitors to the Physical Secured Location must be issued a visitor badge with their name and date/time of entry recorded in the Visitor's Register. All visitors that are exposed to CJI must also sign a "Dispatch Visitor Form"; however, frequent visitors (vendors, contractors, maintenance personnel, etc.) are only required to sign a form once per year. Authorized personnel that do not have their credential must be issued a badge and be recorded in the register; however they are not required to sign a "Dispatch Visitor Form". Visitors are permitted to leave and re-enter the Physically Secured Location for a period not to exceed twenty-four (24) hours without being issued a new badge. The Visitor's Register must be maintained for three (3) years.

VII. CONTROLLED AREA

CJI access permitted outside of the Physically Secured Location (i.e., MDC, Investigations) is permitted under the following circumstances:

1. The Controlled Area may only be accessed by employees authorized to access or view CJI when CJI is present.
2. The Controlled Area must be locked when unattended.
3. Information system devices and documents containing CJI must be positioned in such a way as to prevent unauthorized individuals from access and view.

APPROVED