NONCRIMINAL JUSTICE AGENCY SUPPLEMENTAL GUIDANCE

This supplemental guidance for noncriminal justice agencies (NCJA) is provided specifically for those whose only access to FBI CJI is authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes, via their State Identification Bureau and/or Channeling agency. This guidance does not apply to criminal justice agencies covered under an active user agreement with the FBI CJIS Division for direct connectivity to the FBI CJIS Division via the FBI CJIS Wide Area Network. Examples of the target audience for this supplemental guidance include school boards, banks, medical boards, gaming commissions, alcohol and tobacco control boards, social services agencies, pharmacy boards, etc. The information below identifies the sections of the CJIS Security Policy most closely related to the NCJA's limited scope of interaction with CJI.

1. The following CJIS Security Policy sections comprise the minimum standard requirements in all situations:
    a. 3.2.9 – Local Agency Security Officer (LASO)
    b. 5.1.1.6 – Agency User Agreements
    c. 5.1.1.7 – Outsourcing Standards for Channelers*
    d. 5.1.3 – Secondary Dissemination
    e. 5.2.1.1 – All Personnel (Security Awareness Training)
    f. 5.3 – Incident Response
    g. 5.4 – Auditing and Accountability
    h. 5.8 – Media Protection
    i. 5.9.2 – Controlled Area
    j. 5.11 – Formal Audits **
    k. 5.12 – Personnel Security***

    * Note: Outsourcing Standard applies when contracting with channeling or outsourcing agency.

    **Note: States shall periodically conduct audits of NCJAs. The FBI CJIS Division shall triennially conduct audits of a sampling of NCJAs.

    *** Note: See the National Crime Prevention and Privacy Compact Council's Outsourcing Standard for Contractor background check requirements.

2. Agencies located within states having passed legislation authorizing or requiring civil fingerprint-based background checks for personnel with access to criminal history record information for the purposes of licensing or employment shall follow the guidance in Section 5.12. Agencies located within states without this authorization or

requirement are exempted from the fingerprint-based background check requirement until such time as appropriate legislation has been written into law.

3. When receiving CJI via encrypted e-mail or downloading from a web-site and subsequently storing the information as an encrypted electronic image Authorized Recipients should, in addition to all of the aforementioned sections, focus on compliance with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication (web-site access)
    c. 5.10.1.2 – System and Communications Protection – Encryption

4. When receiving CJI via e-mail or retrieving CJI from a website and subsequently storing the CJI electronically, Authorized Recipients should, in addition to 1.a–1.k above, focus on compliance with policy sections:
    a. 5.5.2.4 – Access Control – Encryption
    b. 5.6 – Identification and Authentication
    c. 5.7 – Configuration Management
    d. 5.10 – System and Communications Protection and Information Integrity

5. If an NCJA further disseminates CJI via encrypted e-mail to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should, in addition to 1.a–3.c above, focus on compliance with policy sections:
    a. 5.7 – Configuration Management
    b. 5.10 – System and Communications Protection and Information Integrity

6. If an NCJA further disseminates CJI via secure website posting to Authorized Recipients, located outside the NCJA's designated controlled area, the NCJA should focus on all sections outlined in 1.a-4.d above.