Protected Information Handout

CJIS Security Policy v5.1:

4.1 Criminal Justice Information (CJI)

Criminal Justice Information is the term used to refer to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their missions including, but not limited to biometric, identity history, biographic, property, and case/incident history data. The following categories of CJI describe the various data sets housed by the FBI CJIS architecture:

1. Biometric Data—data derived from one or more intrinsic physical or behavioral traits of humans typically for the purpose of uniquely identifying individuals from within a population. Used to identify individuals, to include: fingerprints, palm prints, iris scans, and facial recognition data.
2. Identity History Data—textual data that corresponds with an individual's biometric data, providing a history of criminal and/or civil events for the identified individual.
3. Biographic Data—information about individuals associated with a unique case, and not necessarily connected to identity data. Biographic data does not provide a history of an individual, only information related to a unique case.
4. Property Data—information about vehicles and property associated with crime.
5. Case/Incident History—information about the history of criminal incidents.

The intent of the CJIS Security Policy is to ensure the protection of the aforementioned CJI until such time as the information is either released to the public via authorized dissemination (e.g. within a court system or when presented in crime reports data), or is purged or destroyed in accordance with applicable record retention rules.

4.3 Personally Identifiable Information (PII)

For the purposes of this document, PII is information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name. Any FBI CJIS provided data maintained by an agency, including but not limited to, education, financial transactions, medical history, and criminal or employment history may include PII. A criminal history record for example inherently contains PII as would a Law Enforcement National Data Exchange (N-DEx) case file. PII shall be extracted from CJI for the purpose of official business only. Agencies shall develop policies, based on state and local privacy rules, to ensure appropriate controls are applied when handling PII extracted from CJI. Due to the expansive nature of PII, this policy does not specify auditing, logging, or personnel security requirements associated with the life cycle of PII.

Notes from the FBI CJIS Division concerning N-DEx:

Information collected directly by an agency is not subject to CJIS controls unless that information has been submitted to N-DEx. The information must then be protected according to the standards of CJI.

If an information system contains any CJI, the information system, it's back-ups, the network that carries the unencrypted traffic from the information system, any terminals that can access the information system, any printers used to create hard copy from the information system, and any other information systems that exchange information with the system containing CJI, must also be protected according to the standards of CJI and are subject to audit by the CSA and the FBI CJIS division.