Confidentiality and the Criminal Justice System

MCAA of SC
Spring Meeting
April 8, 2016

Criminal Justice Information

- Definition
- CHRI
- Confidentiality / Security
- Local, State, Federal systems
- Dissemination/ Disposal / Disposition
- Expungement / Sealed records
- Penalty and sanctions (violations)

Definition: Criminal Justice Information (CJI)

FBI – Refers to all of the FBI CJIS provided data necessary for law enforcement and civil agencies to perform their mission.

(Security Policy 5.4 – FBI - Criminal Justice Information Services Division)

CJI - Data elements

- Biometric (fingerprints, palm prints, etc)
- Identity– Criminal History Record Information associated with fingerprints of persons (CHRI)
- Other data sets (see policy FBI.GOV, 200 pages)

CJI Systems

- FBI / NCIC 2000 – National Crime Information Center (people, property, links to CHRI)
- III – Interstate Identification Index (Criminal History, wanted persons, etc.
- NICS – Firearm background check
- NICB – Vehicle Thefts/recovery/tracking
- Nlets – CJA Communications network.

NCIC – CHRI / III

Computerized Criminal History
Local arrest records

Criminal History Record Information – III

- Considered to be "restricted data"
- Controlled access
- Restrictions on use and dissemination
- III and NCIC specifically identified in Federal Regulation Title 28, Part 20 CFR, and in the NCIC Operating Manual

CHRI - III

- Computerized Criminal History from State / FBI NCIC (CHRI/III)(4.1.1)
- Authorized Access (NCIC operators, CJ personnel authorized to receive)
- Proper use (Attn, Purpose code / justification for search)
- Dissemination of CHRI

CHRI - III

- Designed to track offender through the CJ process (arrest, court, detention, disposition, PPP.
- Access and Use is for law enforcement official business only
- ONLY SLED can disseminate to private entities (general public, website)
- Exceptions – allowed by law/state statute

CHRI /III - Exceptions

- LE agencies can disseminate their own CHRI (local arrest record) to public / courts / DSS
- LE agencies can disseminate SLED (state CCH record) as allowed by statute (DSS – EPC)
- Prosecutor's can provide FBI – NCIC CHRI on defendant to Defense Attorney for criminal trial
- (NO ACCESS FOR CIVIL Purposes, non criminal justice purposes)

Restricted Files

Restricted Files 4.2.2

- Gang Files
- KST (Known or suspected Terrorist
- Supervised Release
- NSOR (National Sex Offender)
- Historical Protection Order
- Identity Theft

Restricted Files 4.2.2

- Protective Interest Files
- Person With Information (PWI) data in missing person files
- Violent Person
- NICS Denied Transaction

Restricted Files 4.2.2

- CHRI – NCIC rap sheet
- Prosecutor provides current record copy to Defense Attorney (criminal trial)
- NCIC record may have restricted file attached (Gang, KST)
- Must not be Released (tear off restricted section)

Restricted Files 4.2.2

- Exempted under Code of Federal Regulation (Title 28, Part 20)
- Not to be released under FOIA, subpoena (civil, criminal, or court order)
- Applies to State & III CCH record copies of CJ agencies (Law enforcement, courts, etc.)

Privacy Laws

Privacy of Protected Data

Privacy Laws

- Federal – Identification data such as SSN, UNI / FBI # (= CJIS data)
- State Privacy Laws – SSN, complete Date of Birth, DL info, financial, etc.
- EMS employee names(LE reports – medic #) SC Code of Laws 44-61-160
- CJI accessible to agencies for use in performing Criminal justice functions

Privacy Laws

- Identity Information must be deleted/redacted from police reports/ documents prior to release under FOIA, Subpoena, court order, etc.)
- Agency to inform requestor of redacted information due to FBI Security Policy, Privacy Laws and restriction of access

RMS Security

Records Management Systems
Security Requirements
FBI, State, Local

RMS – Security

- Criminal justice agencies (prosecutor, courts, law enforcement, probation, federal)
- Warrants, police reports, NCIC attachments, CHRI (documents in a case file)
- Technology (cut and paste CJI data from NCIC into police report/files)

RMS - Security

- Background checks (personnel accessing facility where CJI is stored)
- Mandatory Security Awareness training (direct access / indirect access)
- NCIC certification mandatory for direct access to CJI

RMS - Security

- Federal requirements for RMS / access to CJI
- State requirements
- USER Agreements
- NCIC Training / Reaffirmation (2 years)
- Security Awareness Training (2 years)

RMS Security

- RMS - Paper documents, Electronic, Digital, email, computer programs
- Secure network needed to email sensitive data (police reports, ID info.
- Fax – secure office and authorized to receive CJI
- Encryption requirement to email CJI data
- Dedicated lines required (IAFIS, FP transmissions, etc.

Dissemination

Dissemination of CJI

- CHRI - Criminal History Record Information

Required to maintain internal log documenting the release of III to authorized personnel

(Greenville County has electronic system

Records maintains internal manual log)

Dissemination - CJI

- NCIC operator accesses State/III CCH

Required fields: Purpose code, ATN field, name of subject, FBI #, Justification, etc.

ATN field – name of person to receive and use the information (not secretary or assistant name). Investigator, Judge, prosecutor, probation agent, etc.

Dissemination – Release of Information

- Records Division – process local backgound checks for general public, private companies…
- Maintain E – dissemination of reports, background checks
- Subpoena to court/track volume of requests

POLICY

POLICY

- POC – Point of contact for SLED regarding audits / FBI
- TAC – Terminal Agency Coordinator
- Security – controlled access through Information Systems, passwords
- Level of access (Job function)
- Deleting access (job change, leave employment

POLICY

- SLED and FBI Audits
- NCIC access controls
- Inspection of Dissemination logs
- Internal Policy to handle misuse (accidental or intentional)
- Must meet minimum standard of FBI security policy (access, encryption, etc)

POLICY

- Written policy regarding use of SLED / FBI system to ensure confidentiality and use of CJI
- Minimum requirements listed in 5.4
- Local policy
- Employee acknowledgement form
- Policy includes Information Technology requirements, firewalls, etc.

DISPOSAL

Disposition / Disposal

- CHRI – III copies should not be kept indefinite or referred to without a new query (records change routinely due to dispositions update, expungements, corrections)
- Copies must be shredded / burned (mandatory)

Disposition/Disposal

- Law enforcement case files – 30 year retention (contains CJI)
- Records must be secured / stored for future reference / (Indefinite digital storage)
- Active investigations, Appeals, new trials, etc.

Expungement / Sealed

Expungement / Sealed

- State Law changes
- Courts expungement completely
- SLED expunges completely
- Law enforcement agencies - Records Division (completely expunged on orders where subject was convicted and paid for expungement)
- Police reports not destroyed (local and CJI information regarding investigation)

Expungement / Sealed

- Confidentiality also applies to FOIA
- 30-4-40 – Record is exempt because confidentiality falls under another state statute (expungement order)
- We do not release copies to anyone!!!
- Exception: we have pulled orders for Clerk of Court / arresting agency

Expungement / Sealed

- Expunged Records – Police reports defendant statement, waiver, warrant copies, Name, personal identifying information deleted from RMS/replaced with ZZZZZ (arrest stats, etc.)
- Jail data purged (limited data retained for stats, reference)

Expungement / Sealed

- Sealed – Police reports (Law enforcement agencies seal the record for 3 years, 120 days. Accessible to criminal justice agencies/prosecutors)
- Sealed – Detention RMS /Paper documents – Controlled access
- Cover sheet placed in front of paper / Digital files

Expungement / Seal

- RMS – Paper, Digital and Electronic systems (controlled access to authorized personnel)
- Limit access due to liability issues

Summary:

- Must be protected from unauthorized release/dissemination
- Federal regulation
- Privacy Laws
- CYA

Questions:

Captain Jinny Moran,
County Records Manager
864 467-5211 –
jmoran@greenvillecounty.org

Source material:
U.S.DOJ / FBI CJIS Security Policy 5.4 (10/6/2015)
NCIC Operations Manual
S.C. Code of Laws

Disclaimer: This presentation is not inclusive of all exemptions. Agencies should refer to established laws and regulations regarding the protection of Criminal Justice Information.