NEVADA CRIMINAL JUSTICE INFORMATION ADMINISTRATIVE POLICIES

Section 1 ADMINISTRATIVE RESPONSIBILITIES

~~1.1~~ *1.0 General*

The primary function of the Nevada Criminal Justice Information System (NCJIS) is to provide an efficient and effective system for the expeditious exchange of criminal justice or related information. Administrative responsibilities are ~~as~~ necessary *and are considered to be as* important as the system itself. Without completion of the many administrative responsibilities that are required by the Federal Bureau of Investigations (FBI) Criminal Justice Information Services (CJIS), CJIS Systems Agency (CSA), CJIS Systems Officer (CSO) and the many users of the system, NCJIS would not function properly.

Criminal Justice Information (CJI) is information accessed via any system (including but not limited to) CJIS, NCJIS, NDEx, Nlets, and CLETS. Access to CJI by these systems must be approved by the CSO and are subject to these Nevada Administrative Policies.

1.1 ~~Requirements for Access to NCJIS~~ *Requirements for Access to Criminal Justice Information (CJI)*[KM1]

1. In order to have access to CJI, each agency must be assigned a unique nine-character ORI. Eligibility for an ORI; includes any court or government agency which performs a function in the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its budget (more than 50%) to a function in the administration of criminal justice as well as certain approved noncriminal justice governmental, public safety or private entities as defined in Nevada Revised Statute (NRS) 179A.020 – NRS 179A.030, NRS 432B, NRS 424 and Title 28 Code of Federal Regulations 20.33 (a) (6).

2. Liaison personnel must be identified by the agency and provided to the CSO when necessary, as follows:

Agency Administrator (AA) See responsibilities of the AA
Local Agency Security Officer (LASO) See responsibilities of the LASO
Terminal Agency Coordinator (TAC) See responsibilities of the TAC
NonTerminal Agency Coordinator (NTAC) See responsibilities of the NTAC

~~1. Any court or government agency which performs a function in the administration of criminal justice pursuant to a statute or executive order and which allocates a substantial part of its budget (more than 50%) to a function in the administration of criminal justice may be granted online terminal or non-terminal access.~~

~~2. Certain approved noncriminal justice governmental, public safety or private entities as defined in Nevada Revised Statute (NRS) 179A.020 – NRS 179A.030, NRS 432B, NRS 424 and 28 CFR 20.33 (a) (6) may be granted online terminal access to Criminal Justice~~

~~Information (CJI).~~

~~3. For initial access to NCJIS, the Agency Administrator (AA) must request a New User Packet from the CSA.~~

3. Agencies that have been approved for access to CJI must enter into an *Interlocal Contract between Public Agencies* with the DPS, and are legally bound thereby and agree to abide by all provisions contained therein. The contract serves to identify the responsibilities between the CSA and the CJI authorized agency. Agreement shall be reviewed at the next compliance audit. The agreement shall remain in force until:

   - USER violates any portion of the agreement or policies which result in the termination of said access; OR
   - USER advises the CSO in writing of the agency's wish to cancel access; OR
   - Until renewed by the CSA.

4. The computer equipment necessary for connection to NCJIS must be compatible with NCJIS. Any request for a specific technological change that may increase NCJIS cost or depart from an established NCJIS policy must be submitted to the CSA and approved by the CSO.

5. Agencies that have been approved for terminal access will be responsible for costs associated with initial connection, additional connections, compatible computer and terminal equipment, reoccurring line costs or any costs associated with additional circuitry between the agency and NCJIS.

6. Any terminal, computer system or other equipment that has direct access to NCJIS must be under the management control of an authorized criminal justice agency or an approved governmental agency that has been authorized by local ordinance, state statute or federal regulations.[KM2]

4. Terminal agencies that provide service to another terminal or non-terminal agency must establish a written User Agreement/Letter of Understanding between their agency and any agency for which they provide service that delineates responsibilities for both.

5. Nonterminal agencies must maintain an active User Agreement/Letter of Understanding with a terminal agency delineating responsibilities for both.

6. Contractors shall be permitted access to CJI, pursuant to an agreement which specifically identifies the contractor's purpose and scope of providing services. The agreement between the agency and the private contractor shall incorporate the CJIS Security Addendum.

7. Prior to access, the AA must ensure that all authorized personnel have met the NCJIS/NCIC screening criteria as described in Section 2.1 of this document.[KM3]

8. The AA must appoint a TAC and a Local Agency Security Officer (LASO).

9. Before access to NCJIS, the TAC must be trained according to Section 3.0 of this document.[KM4]

10. All foreign host connections must follow current procedures as posted on NVSHARE by DPS General Services Division.[KM5]

1.2 Contract between Public Agencies (Interlocal Contracts, User Agreements, Letters of Understanding, Security Addendums)

1. All agencies that have been approved for direct access to NCJIS must enter into an *Interlocal Contract between Public Agencies* with the Department of Public Safety (DPS), General Services Division Division and are legally bound thereby and agree to abide by all provisions contained therein. The contract serves to identify the responsibilities between the CSA and the terminal agency. Agreement shall be reviewed at the next compliance audit by the NCJIS Audit staff. The agreement shall remain in force until:

   a. USER violates any portion of the agreement or policies which result in the termination of said access; OR

   b. USER advises the CSO in writing of the agency's wish to cancel access; OR

   c. Until renewed by the CSA.[KM6]

2. Terminal agencies that provide service to another terminal or non terminal agency must establish a written User Agreement/Letter of Understanding between their agency and any agency for which they provide service that delineates responsibilities for both.

3. Nonterminal agencies must maintain an active User Agreement/Letter of Understanding with a terminal agency delineating responsibilities for both.[KM7]

4. A User Agreement/Letter of Understanding between agencies is not required when validations are the only function being performed for an agency.[KM8]

~~5. Contractors shall be permitted access to NCJIS/NCIC systems and its data, pursuant to an agreement which specifically identifies the contractor's purpose and scope of providing services. The agreement between the agency and the private contractor shall incorporate the CJIS Security Addendum.[KM9]~~

~~1.3~~ *1.2* Responsibilities of the Agency Administrator (AA)

~~1. Is responsible for ensuring compliance with all applicable laws, rules and regulations regarding NCIC/NCJIS/JLINK.~~

~~2. Ensure their agency TAC has been certified in the NCJIS/NCIC Proficiency Seminar provided by the CSA as described in Section 3, Personnel Training.~~

~~3. Ensure the TAC has access to documentation that all authorized personnel have met the NCJIS/NCIC screening criteria.~~

~~4. Ensure that the Security Awareness Training outlined in the CJIS Security Policy is implemented.~~

~~5. Allow TAC access to all systems and areas relating to NCJIS/NCIC for administrative and auditing purposes.~~

1. *Communicate type of access the Agency will be using to access to CJI.*
2. *Must always have an appointed TAC and LASO or NTAC. The AA must notify the CSA within 10 days as changes in appointments occur.*
3. *Is responsible for ensuring compliance with all applicable laws, rules and regulations regarding access to CJI and the systems supporting accesses.*
4. *Ensure agency training requirements are met, as described in Section 3, Personnel Training.*
5. *Ensure the TAC or NTAC has access to documentation that all authorized personnel have met the authorized access to CJI screening criteria. (See Security Requirements Section 2*
6. *Allow TAC access to all systems and areas relating to CJI for administrative and auditing purposes.*

Note: Please reference Section 3 – Technical Compliance.

~~1.4~~ *1.3* Responsibilities of the Terminal Agency Coordinator (TAC)

The TAC is designated as the liaison between their agency and the CSA/CSO, with regard to access to the ~~NCIC/NCJIS.~~ *CJI. The TAC is responsible for the following:*

~~1. Must be a current certified operator that, at a minimum, meets the standard of the agency; i.e. Full Terminal Agency TAC should hold an Inquiry/Entry certification.~~

1. Must be authorized for access to CJI , at a minimum equal to their agency's CSO approved level of access; i.e. Full Terminal Agency TAC should hold an Inquiry/Entry certification.

2. Is required to attend all mandatory training set by the CSA/CSO.

3. Employ a formal sanction process for personnel failing to comply with established system related policies, including, but not limited to: NCJIS Policies, CJIS Security Policy, Nlets and CLETS as detailed in the Interlocal Contract between Public Agencies. *Agency systems such as Nlets, N-DEx or CLETS, with CJI access must either include these systems in the agency formal sanction process or create standalone sanction processes.*

4. Serves as the central contact point in his/her agency for quality control matters, dissemination of manuals and other documentation and all audits *regarding CJI* which includes federal, state and technical.

~~5. Agencies with N-DEx access must either include N-DEx in the formal sanction process or create an N-DEx only sanction process.~~[KM10]

6. The TAC must immediately notify the CSA of any intentional misuse of ~~CHRI~~ *CJI and the steEITS the agency has taken; investigation and findings, training, dismissal, criminal charges.*

7. Ensure proficiency training for all authorized personnel as outlined in Section ~~3.~~ *4*

8. Ensure the validation process is completed by the prescribed due date.

9. Monitor terminal operators to ensure compliance with the proper use of purpose codes and attention fields.

~~10. Obtain approval from the CSA's ISO prior to relocating NCJIS terminal equipment. Approval is required when moving NCJIS terminals to locations where the physical security boundaries and technical security measures have not already been inspected and approved by the ISO. The ISO must be notified by means of a Help Desk ticket at least three weeks prior to the planned start of operations at the new site.~~

~~11. Moving an NCJIS terminal within the physical and technical security boundaries of the original location does not require approval. Moving an NCJIS terminal to a different location that already houses NCJIS terminals also does not require approval. However, you should contact your LASO to ensure access will not be lost if the terminal is moved.~~

~~12. After moving an NCJIS terminal, the JLClient refresh program must be run and the location of the terminal is updated.~~[KM11]

~~13. Assign unique identifiers for your agency's operators and operators from other agencies that are on loan to your agency, including task force members.~~

10. Assign unique identifiers for their agency's operators and operators from other agencies that are on loan *to the TAC's* your agency, including task force members. [KM12]

11. *The TAC's* may appoint Assistant Terminal Agency Coordinator(s) (ATAC) to assist them with *their* TAC duties. The TAC must notify the *NCJIS Compliance Unit (NCU)* of the appointment of an ATAC(s) via mail, fax or e-mail.

12. The TAC must ensure that all changes in policies and procedures, regarding CJI and CJI systems and areas, such as training materials and other related media are provided to all CJI authorized agency personnel as they pertain to his or her agency. ~~Documentation of distribution must be maintained through one complete NCJIS audit cycle.~~

13. Cooperate and give assistance to the NCU Audit Staff with required or directed compliance audits.

14. TACs must immediately update required lists and JLClient as changes occur within their agency, terminals, CJI authorized personnel or operator information. CJI authorized personnel, operators, and ~~where applicable~~ terminal information must be validated annually and documentation maintained for one audit cycle.

15. Assign CJI access according to the personnel's level of training. The NTACs and TACs must maintain an accurate documentation listing of CJI authorized personnel and their level of access (such as operator, requesting, and view only). Immediately update required lists and JLClient as changes occur with agency, terminal, CJI authorized personnel or operator information. For NTACs, CJI authorized personnel lists must be forwarded to the agency providing you with CJI.

16. Only the *AA, TAC, NTAC, or ATAC* ~~or AA~~ can request an offline search. ~~from EITS Help Desk.~~

17. If there is a change of AA, the agency must notify the CSO ~~in writing~~ within ten days.

In addition the following is highly recommended for a TAC:

- The TAC (or an ATAC) must be available during hours that are conducive to the administration of the criminal information systems.

- As the agency's expert on NCIC/NCJIS/JLink, the TAC should have an extensive knowledge of each criminal information system's Policy and Procedures, System Security, System Discipline, and Validation and Sanction Process. ~~is required~~. (See TAC Responsibilities and NCJIS Administrative Policies)

- Should serve in a supervisory and/or administrative capacity within their agency, in order that, they may speak on behalf of their agency and affect changes in policy within their department, if necessary.

Is encouraged to attend the quarterly Technical Subcommittee meetings to keep up-to-date on issues relating to the varied criminal information systems

~~18. May appoint Assistant Terminal Agency Coordinator(s) (ATAC) to assist them with his or her TAC duties. The TAC must notify the Program Development and Compliance Unit (PD&C) of the DPS, General Services Division of the appointment of an ATAC(s) via mail, fax or e-mail.~~

~~19. The TAC must ensure that all changes in policies and procedures, NCJIS and NCIC Newsletters, Technical and Operational Updates (TOUs), training materials and other related media are provided to all authorized terminal agency personnel as they pertain to his or her agency. Documentation of distribution must be maintained through one complete NCJIS audit cycle.~~

~~20. Cooperate and give assistance to the NCJIS Audit Staff with required or directed compliance audits.~~

~~17. Immediately update JLClient as changes occur with agency, terminal or operator information.~~

~~1.5 Responsibilities of the Local Agency Security Officer (LASO)~~

~~1. The TAC must be included in all actions that relate to terminal, security or JLINK.~~

~~2. Ensure that after the move of an NCJIS terminal, the JLClient refresh program is run and the location of the terminal is updated.~~

~~3. Ensure the administration of secure remote access (Refer to CJIS Security Policy).~~

4. Assist in maintaining network topology documentation.

5. Support security-related configuration management.

5. Provide guidance in implementing security measures.

6. Serve as the security point of contact for computer incident notifications and distributing security alerts to the CSA ISO.

7. Disseminate security related training materials.

8. Assist CSA ISO in the technical security audits.

9. Develop Security Awareness training program.

10. Conduct or assist with the presentation of the Security Awareness training program.

11. The LASO will ensure that contractors with remote access to criminal justice agency infrastructure that carries, stores, or processes CJI meet CJIS Security Policy requirements. When the contracting entity is remotely connected, the entity's infrastructure becomes part of the criminal justice agency network and is subject to all physical, technical, and personnel security requirements.[KM13]

1.6 ORIs, Terminal Ids, Agency Codes and Operator Functions

1. In order to obtain information from NCJIS, each authorized agency must be assigned a unique nine-character ORI. Agencies that have limited access to Nlets are required to have a nine-character ORI ending in "S".[KM14]

2. Any terminal agency that agrees to perform inquiries, entries, hit confirmations, validations and/or acts as holder of record for any authorized agency must have the ORI of the agency they are servicing appended to his or her terminal. The appended ORI must be used for any transaction performed for that agency. If that ORI cannot be appended to the terminal, a log must be maintained of the transactions performed for that agency. The log must contain the same information as required in the NCJIS Policies, CJI Section.[KM15]
3. Agencies that provide service to a Non-Terminal Agency (NTA) must advise the CSA when the service to the NTA is terminated.

4. *18.* Each terminal accessing NCJIS must be issued a unique terminal identification number *The TAC is responsible for assigning unique terminal identification numbers*. If the terminal

has multiple screen capability and all screens are to access NCJIS, each screen must be assigned a unique terminal ID and ORI.[KM16]

~~5. Each agency is assigned a unique agency code by the CSA which cannot be changed.~~

1. 4 Responsibilities of the Non-Terminal Agency Coordinator (NTAC)

NTACs are designated as the liaisons between their agency and the CSA/CSO, with regard to access to CJI. For purposes of this section a Servicing Agency is an agency with computer access to CJI which they provide to another CSO authorized agency.

1. *Ensure agency authorized personnel have met NCJIS screening criteria. (See Personnel Security 2.1)*

2. *Complete all mandatory training set by the CSA/CSO.*

3. *Ensure proficiency training for all authorized personnel as outlined in Section 3. NTAC must ensure that all changes in policies and procedures regarding CJI are provided to authorized agency personnel as they pertain to his or her agency.*

4. *Provide and maintain a current and up to date listing of their agency's authorized personnel to their Servicing Agency.*

5. *Employ a formal sanction process for personnel failing to comply with established related policies, including, but not limited to: NCJIS Policies, CJIS Security Policy, Nlets, N-DEx and CLETS as detailed in the Interlocal Contract between Public Agencies. Agency systems such as Nlets, N-DEx or CLETS, with CJI access must either include these systems in the agency formal sanction process or create standalone sanction processes.*

6. *The NTAC must immediately notify the CSA of any intentional misuse of CJI and the steEITS the agency has taken; ie. investigation and findings, training, dismissal or criminal charges.*

7. *Cooperate and give assistance to the NCU Audit Staff with required or directed compliance audits.*

8. *Only the NTAC or AA can request an offline search from EITS Help Desk.*

9. *If there is a change of AA the agency must notify the CSO with ten days.*

In addition the following is highly recommended for a NTAC:

- *The NTAC be available during hours that are conducive to the administration of the criminal information systems.*

- *As the agency's expert for CJI, the NTAC should have an extensive knowledge of each system's Policy and Procedures, System Discipline and Sanction Process; ie. NCIC, CLETS, N-Dex*

- *Should serve in a supervisory and/or administrative capacity within their agency, in order that they may speak on behalf of their agency and affect changes in policy within their agency.*

~~1.7~~ *1.5* Termination of access to NCJIS

1. At the recommendation of the CSO and approval by the Director of the DPS, the CSA may suspend or terminate access to NCJIS for a violation of a specific term of the *Interlocal Contract between Public Agencies*. In addition, any violation of NCJIS, state or federal statutes, regulations or rules incorporated in the Administrative Policies of NCJIS/NCIC/Nlets/CLETS shall be deemed a breach of terms. Suspension or termination shall commence upon 30 days advance written notice to the user from the CSO.

2. Any agency may terminate access to NCJIS with written notice from the AA to the CSA.

3. In the event of termination of access to NCJIS, any computers used to access NCJIS/NCIC information must be sanitized according to Department of Defense (DOD) requirements. Any removable or disposable media such floppy discs, CD ROMs, DVDs, or magnetic tapes used to store any NCJIS/NCIC data must be sanitized or destroyed. See the CJIS Security Policy for further guidance.[KM17]

REQUIREMENTS

2.0 General

1. Data stored in NCJIS is documented CJI and must be protected to ensure authorized dissemination and use.

2. Agencies utilizing NCJIS, NCIC, N-DEx, Nlets and CLETS are responsible for ~~the~~ maintaining the security and confidentiality of these systems and ~~its~~ *their* data.

3. The Nevada CSA prohibits dissemination of any information received from NCJIS to any unauthorized person. *Dissemination is defined in NRS 179A.060.* This includes but is not limited to Department of Motor Vehicles information or photos. It is forbidden for agency personnel to request and/or perform inquiries for curiosity or for any reason other than authorized by NCJIS, NCIC, NRS or local ordinance. Unauthorized inquiry or dissemination may result in agency sanctions.

4. If the unauthorized inquiry or dissemination includes CHRI, the person may be subject to criminal charges pursuant to NRS 179A.900.

5. The CSA routinely conducts random reviews of *Criminal Justice Information (CJI)* ~~Interstate Identification Information (III)~~ transactions to ensure the ~~III~~ information is being used for authorized purposes.

2.1 Personnel Security

1. The TAC/*NTAC's* must be granted access and make available for audit review documentation that authorized personnel have met the NCJIS/NCIC screening criteria.

2. Before unescorted access for authorized personnel is granted, a state of Nevada and national fingerprint based record check, and a wants/warrants check must be performed.

   NCJIS/NCIC screening criteria:

   a. State of Nevada and national fingerprint results confirming no felony or gross misdemeanor arrests without disposition.

   b. State of Nevada and national fingerprint results confirming no felony or gross misdemeanor convictions.

c. Wants/Warrants check confirming they are not a fugitive from justice. (This is not part of the fingerprint processing and must be performed as a separate NCJIS/NCIC transaction.)

Note: Reference CJIS Security Policy 5.12.1.1

3. In the event an agency wishes to allow access to an individual who fails the above screening criteria, a written request to the CSO requesting access must be submitted. The written request must contain the following information:

   a. Subject's name.

   b. Subject's date of birth.

   c. Subject's social security number.

   d. Length of employment with agency.

   e. Job title.

   f. Type of NCJIS access.

   g. Arrest and disposition information along with copies of any documentation obtained by the agency regarding the disposition.

   h. The request must also state that the agency has disciplinary procedures in place for misuse of NCJIS information and the agency will accept responsibility and liability for any misuse of NCJIS information initiated by the subject.

NOTE: Background re-investigations are highly recommended every five (5) years as a best business practice.

~~2.2 Physical Security~~

1. TACs must establish internal written procedures (IWP) regarding their agency's physical security. The IWEITS must detail requirements 2-5 listed below.[KM18]

2. Terminal equipment and/or printers must be placed in a physically secure location away from unauthorized viewing or access. Such sites include locations or vehicles housing MDTs or

laptop computers capable of accessing CJI. [KM19]

3. Hard copy CJI obtained through NCJIS is considered confidential and must be maintained in a secure records environment and must be destroyed by shredding or burning by authorized personnel.[KM20]

4. Media protection policy and procedures shall be documented and implemented to ensure that access to electronic and physical media in all forms is restricted to authorized individuals. Procedures shall be defined as outlined in the CJIS Security Policy. (This includes terminals that are being replaced by a new terminal.)[KM21]

5. Authorized personnel must at all times escort visitors, inmate workers, maintenance persons, non-employees or any unauthorized personnel to areas where CJI is viewable or accessible. An unauthorized person being escorted in a physically secure area must be escorted by a person who is sufficiently familiar with the equipment in the area and the tasks being performed. The escort must be able to identify an unauthorized act and alert security personnel. If the escort does not have this set of knowledge and skills, then the unauthorized person is not considered escorted.[KM22]

~~2.3 Logical Security~~

~~1. A terminal operator must use his or her own unique operator ID and password for all terminals that access CJI. Using someone else's ID and password to log on is strictly prohibited.~~

~~2. Terminal operator passwords must be kept confidential.~~

~~3. The TAC must ensure that all terminals that access CJI are locked down or logged off when not in physical sight of the operator.~~

~~4. Agencies accessing CJI through mobile devices must have prior written approval from the CSA ISO.~~

~~5. All computers and network equipment directly interfaced with NCJIS that have access to CJI through NCJIS, NCIC, N-DEx, Nlets or CLETS must be under the management control of an authorized agency.~~[KM23]

Section 3 *Technical Compliance*[KM24]

3.0 Technical Compliance

The portion of NCJIS Policies related to technical compliance is meant to be an enhancement to the Federal Bureau of Investigation's CJIS Security Policy. If you do not have this policy, it is available at httEITS://www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center or through your State of Nevada CJIS Information Security Officer. You should be familiar with the FBI policy first, as it is the primary document. Also, if your version of CJIS Security Policy is over 1 year old, you should check for a newer version as the CJIS Security Policy is updated approximately once a year.

Please understand that all of CJIS Security Policy can be reduced to, "Prevent unauthorized access, and detect and report it when it occurs." The rest of the CJIS Security Policy and the technical compliance section of this document set the level of effort and provide clarifying details.

3.1 Physical Security

The CJIS Security Policy states, in section 5.9.1, "A physically secure location is a facility, a criminal justice conveyance, or an area, a room, or a group of rooms within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems." While useful information, this does not provide any specific instructions on appropriately securing CJI using physical controls.

The Nevada minimum standard for physical security is the following statement: any successful attempt for unauthorized access will show at least some sign of permanent physical damage, using only tools available from a home improvement store. Examples are broken window, broken door knob/lock/frame, a cut padlock, wall or ceiling damage; the list goes on. This means that physical security is not meant to be an impenetrable barrier, just that if the barrier is breached, the resulting destruction should alert an agency that there has been unauthorized access. Note that this is the minimum standard. Agencies are encouraged to use stronger controls and multiple risk mitigating strategies beyond the minimum standard.

Common pitfalls in establishing a physically secure perimeter are:

- *Drop ceilings with more than 18" of maneuvering space above the drop ceiling*
- *Doors with hinges mounted on the unsecure side*
- *Keys shared with maintenance or emergency personnel who are not authorized to CJI*
- *Cage (chain link) walls not extending to a hard ceiling and/or floor, or not tightly enclosing any wall penetrations.*

A common set of mitigations for any of these issues is use of DVR recordings of surveillance cameras in combination with motion detectors. The DVR recordings can help determine unauthorized access after the fact, but the recordings by themselves won't necessarily alert you to an unauthorized access event. Coupled with motion detectors, or other types of intrusion alarms, you can be alerted to a potential issue and then use the DVR recordings to determine what actually occurred. These are just examples of what are considered minimum standards; any measures that can promptly indicate unauthorized access are acceptable mitigation for physical security shortcomings.

3.2 General and Administrative Technical Guidelines

The statement, "Prevent unauthorized access, and detect and report it when it occurs" is also a good benchmark for technical security compliance. Another way of saying this is that prevention of unauthorized access is the ideal, but detection of unauthorized access is paramount.

The primary focus of the CJIS Security Policy is confidentiality and appropriate use of information that belongs to the FBI CJIS Division. This is understandable, given their perspective. While it is beyond the scope of Nevada CJIS Systems Agency authority, a criminal justice agency's primary concern should be the integrity of the agency's own records, and not focus all their effort on just complying with the CJIS Security Policy and protecting the confidentiality of FBI CJIS data.

Data stored in NCJIS is documented CJI and must be protected to ensure authorized dissemination and use. Agencies utilizing NCJIS, NCIC, N-DEx, Nlets and CLETS are responsible for maintaining the security and confidentiality of these systems and its data.

1. The computer equipment necessary for connection to NCJIS must be compatible with NCJIS. Any request for a specific technological change that may increase NCJIS cost or depart from an established NCJIS policy must be submitted to the CSA and approved by the CSO.

2. Agencies that have been approved for terminal access will be responsible for costs associated with initial connection, additional connections, compatible computer and terminal equipment, reoccurring line costs or any costs associated with additional circuitry between the agency and NCJIS.

3. Any terminal, computer system or other equipment that has direct access to NCJIS must be under the management control of an authorized criminal justice agency or an approved governmental agency that has been authorized by local ordinance, state statute or federal regulations.

4. All foreign host connections must follow current procedures as posted on NVSHARE by DPS General Services Division. [SD25]

5. Obtain approval from the CSA's ISO prior to relocating NCJIS terminal equipment. Approval is required when moving NCJIS terminals to locations where the physical security boundaries and technical security measures have not already been inspected and approved by the ISO. The ISO must be notified by means of a Help Desk ticket at least three weeks prior to the planned start of operations at the new site.

6. Before moving devices that were previously connected to CJIS networks to different locations (i.e. storage, disposal facilities, or other operational sites) the preferred method is sanitization, as mentioned in section 3.3 paragraph 2, prior to moving the equipment. If sanitization is not practical prior to the move, then the transport of devices containing CJI will be performed by two or more authorized personnel. If this requirement cannot be met please contact the Nevada CJIS ISO for other mitigating strategies.

7. Moving an NCJIS terminal within the physical and technical security boundaries of the original location does not require approval. Moving an NCJIS terminal to a different location that already houses NCJIS terminals also does not require approval. However, you should contact your LASO to ensure access will not be lost if the terminal is moved.

8. Ensure that after the move of an NCJIS terminal, the JLClient refresh program is run and the location of the terminal is updated.

9. The LASO will ensure that contractors with remote access to criminal justice agency infrastructure that carries, stores, or processes CJI meet CJIS Security Policy requirements. When the contracting entity is remotely connected, the entity's infrastructure becomes part of the criminal justice agency network and is subject to all physical, technical, and personnel security requirements.

3.3 Logical Security

1. Each terminal accessing NCJIS must be issued a unique terminal identification number. If the terminal has multiple screen capability and all screens are to access NCJIS, each screen must be assigned a unique terminal ID and ORI.

2. In the event of termination of access to NCJIS, any computers used to access NCJIS/NCIC information must be sanitized according to Department of Defense (DOD) requirements and standard NIST 800-88r1; however, if the data stored on the media is deemed by the appropriate authorities as more valuable than the medium, then the preferred method should be physical destruction of the medium.[SD26] Any removable or disposable media such as floppy discs, CD ROMs, DVDs, or magnetic tapes used to store any NCJIS/NCIC data must be sanitized or destroyed. See the CJIS Security Policy for further guidance[SD27].

3. If incoming facsimiles are distributed by email the following applies:
Inter-agency emailing or using ESEND to send unencrypted CJI obtained from NCJIS is prohibited unless pre-approved by the Nevada CJIS ISO.

4. If you plan to move CJI across any wireless technology, please contact the Nevada CJIS ISO for prior configuration consultation.

5. [SD28][SD29][SD30]Access to CJI via a regular terminal (i.e. desktop/laptop computer) should use two sets of credentials: one for the terminal itself and one for accessing the CJI application(JLink, for example). Both sets of credentials should be unique from one another and amongst all users, even if multiple users use the same device. Password complexity, as required by CJIS policy should apply to both sets of credentials. [SD31]

6. *A terminal operator must use his or her own unique operator ID and password for all terminals that access CJI. Using someone else's ID and password to log on is strictly prohibited.*

7. *Terminal operator passwords must be kept confidential.*

8. *The TAC must ensure that all terminals that access CJI are locked down or logged off when not in physical sight of the operator.*

9. *Agencies accessing CJI through mobile devices must have prior written approval from the CSA ISO.*

10. *All computers and network equipment directly interfaced with NCJIS that have access to CJI through NCJIS, NCIC, N-DEx, Nlets or CLETS must be under the management control of an authorized agency.[KM32]*

PERSONNEL TRAINING[KM33]

~~3.0~~ *4.0* General[KM34]

1. Training provided to agencies by the CSA is outlined in the NCJIS Training Standards. TACs must be certified according to the following:

   a. An appointed TAC who is a current operator must attend the NCJIS/NCIC Proficiency Seminar and become certified within six months of initial assignment and every two years thereafter.

   b. An appointed TAC who is not a current operator can be trained by another CSA certified TAC as an operator. The TAC must then attend the NCJIS/NCIC Proficiency Seminar to become certified as a TAC within six months and every two years thereafter.

   c. A TAC who is currently certified by the CSA may transfer his or her certification to another agency of equivalent appointment upon approval by the hiring agency.

2. TACs that have *four or more* years of experience and have attended at least two consecutive NCJIS/NCIC Proficiency Seminars may be eligible to participate in the *State of Nevada NCJIS/NCIC proficiency Challenge Program. The NCJIS/NCIC proficiency Challenge Program allows a TAC to take a test in lieu of attending an NCJIS/NCIC proficiency seminar.* ~~Further information is available in the NCJIS Training Standards.~~

   The Department of Public Safety NCJIS Compliance Unit can mandate that a TAC attend NCJIS/NCIC proficiency Training if an agency is failing to meet compliance.

NOTE: Failure to attend retraining every two years will result in loss of access.

~~3.1~~ *4.1* TACs to Provide Training

1. Per CJIS Security Policy, at a minimum all personnel who have access to CJI must be trained in the following topics. Training shall be required within six months of initial assignment, and every two years thereafter. Training must include:

   ~~a.~~ Liability of misuse – describe responsibilities, expected behavior and implications of noncompliance with regard to CJI or its systems.

~~b.~~ Physical policy and procedures – physical access, visitor control, challenging strangers, reporting unusual activity, threats, vulnerabilities and risks associated with handling CJI.

~~c.~~ Confidentiality – protect information subject to confidential concerns.

~~d.~~ Dissemination – authorized personnel list, marking (using caveats such as "For Official Use Only", "Do Not Reproduce", or "Do Not Disseminate") and secondary dissemination logging.

~~e.~~ Storage –instruct what your agency will accept as a secured records environment

~~f.~~ Destruction – instruct how your agency will destroy fixed media and any CJI hard copy.

2. TERMINAL OPERATORS

~~a. The TAC must ensure that all terminal operators are trained and certified within six (6) months of employment or assignment and every two years thereafter. During the initial six (6) month period (before the operator is certified), the operator must be physically supervised by a certified terminal operator and advised of the responsibilities and legal liabilities connected with access to NCJIS. A confirmation document (or "Declaration of Understanding") outlining the operator's responsibilities and liabilities must be maintained in the operator's training file until the operator has completed NCJIS/NCIC certification.~~

a. A confirmation document (or "Declaration of Understanding") outlining the operator's responsibilities and liabilities *must be signed upon granted access to the system* and maintained in the operator's training file ~~until the operator has completed NCJIS/NCIC certification~~ *and available for audit purposes.*

b. The TAC must ensure that all terminal operators are trained and certified within six (6) months of employment or assignment and every two years thereafter. During the initial six (6) month period (before the operator is certified), the operator must be physically supervised by a certified terminal operator and advised of the responsibilities and legal liabilities connected with access to NCJIS.

~~b.~~ *c.* The TAC must train the agency's personnel within his or her level of access. Training must include the ~~Justice Link Documentation System including~~ *following (where applicable):*

1. CJIS Security Policy

2. NCJIS Policies

3. Applicable sections of the NCIC Operating Manual

4. Applicable sections of the NCJIS Operating Guide

5. Internal Written Procedures required by NCJIS Policy

6. Any Policies providing additional CJI access (ie: NDEx and CLETS)

~~c.~~ *d.* The TAC must update his or her agency's terminal operator's certification dates in JLINK only after the terminal operator receives NCJIS/NCIC proficiency training or retraining. A temporary access date will be entered or changed only by ~~the EITS~~ *EITS* Help Desk or the ~~PD&C~~ *NCJIS Compliance* unit.

3. ADMINISTRATORS/UPPER LEVEL MANAGERS/SUPERVISORS

~~a.~~ The Nevada CSA provides peer level training on the NCJIS/NCIC System for criminal justice administrators/upper level managers/supervisors. This training is available on NVSHARE. Training will include regulations, policy, audit sanctions and related civil liability.

NOTE: Failure to provide retraining to terminal operators will result in the operator's loss of access to NCJIS.

~~3.2~~ *4.2* Security Awareness Training

The information provided in the Security Awareness training shall be maintained and available for audit review. See CJIS Security Policy for specific training requirements.

~~3.3~~ *4.3* Personnel Training Record Retention

The TAC must maintain records of the most recent training, testing and proficiency certification.

~~4.0~~ *5.0* Criminal Justice Information (CJI)[KM35]

~~1.~~ 1. As defined by CJIS: Criminal Justice Information (CJI) is the abstract term used to refer to all of the FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the FBI CJIS provided data necessary for civil agencies to perform their mission; including, but not limited to data used to make hiring decisions. *(See Section 10 Non-criminal Justice Compliance)*

~~2.~~ 2. A facsimile device may be used to transmit hard copy CJI if both agencies are authorized to receive CJI and the device is in a secure location.

~~3. If incoming facsimiles are distributed by email the following applies:~~

~~a. Inter-agency emailing or using ESEND to send unencrypted CJI obtained from NCJIS is prohibited unless pre-approved by the LASO.~~

~~4. If CJI is received or stored on any mobile device, the following rules apply:~~

~~a. Wireless link must be encrypted (per CJIS Security Policy).~~

~~b. Data on any mobile device must be encrypted at rest (per CJIS Security Policy).~~

~~c. Access must be protected by a Personal Identification Number (PIN).~~[KM36]

~~5.~~ *3.* All CJI must be maintained in a secure records environment accessible only to authorized personnel.

~~6.~~ *4.* CJI must be used for the purpose for which it was provided and afforded the maximum protection. It is forbidden for agency personnel to request and/or perform inquiries for curiosity. Any inquiry other than a criminal justice purpose must be governed by a federal, state or local statute(s).

~~7.~~ *5.* CJI must be disposed of by shredding or burning.

6. A Regulatory Body having jurisdiction over auditing compliance issues within an agency

can confirm presence of CJI within agency files. The Regulatory Body may not retain copies or make note of CJI specific information.

7. Any terminal agency that agrees to perform inquiries, entries, hit confirmations, validations and/or acts as holder of record for any authorized agency must have the ORI of the agency they are servicing appended to his or her terminal. The appended ORI must be used for any transaction performed for that agency. If that ORI cannot be appended to the terminal, a log must be maintained of the transactions performed for that agency. The log must contain the same information as required in the NCJIS Policies, CJI Section.[KM37]

8. Hard copy CJI obtained through NCJIS is considered confidential and must be maintained in a secure records environment and must be destroyed by shredding or burning by authorized personnel.[KM38]

~~4.1~~ *5.1* Criminal History Record Information (CHRI)

1. As defined by CJIS: Criminal History Record Information (CHRI) is a subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges. *CJI* also includ~~ed~~s ~~are~~ Pre-Sentence Investigation (EITSI) reports, Pre-Arraignment Screening (PAS) forms, recidivism reports and any other reports, forms or documents of a similar nature which contain ~~CHRI obtained from JLINK~~ CJI obtained *from any protected criminal justice information system.*

2. Inquiries for CHRI must include the proper purpose code for which the information is to be used. TACs must establish IWEITS noting which purpose codes are to be used by the agency when making inquiries for CHRI. Refer to the NCIC Operating Manual and Nlets User & Technical Guide for the list and description of available purpose codes.

NOTE: Purpose Code "E" is available for licensing and noncriminal justice employment purposes authorized by state statute or ordinance. Purpose Code E is used for <u>NCJIS inquiry only</u>. *Any exceptions to the use of Purpose Code E must be granted access from the state CSO and maintain written approval on file for audit purposes.*

3. All inquiries into NCJIS, NCIC, Nlets or CLETS to obtain CHRI must include a unique identifier of the authorized person that requested the inquiry in the Attention Field. A division name, department name or a reason for the inquiry without a unique identifier of the authorized requestor is <u>not acceptable</u>. Users are required to provide the reason for the inquiry and supporting documentation for all CHRI transactions upon request by the audit staff. Including the reason for inquiry in the attention field, such as case numbers may help in retrieving supporting documents for audit purposes.

NOTE: Example of a unique identifier: Full Name, Badge Number or Employee Number.

~~4.2~~ *5.2* Security and Confidentiality

Any electronic device that uses wireless or radio technology to transmit voice data may be used for the transmission of CHRI when an authorized requestor determines that there is an immediate need for this information to further an investigation or there is a situation affecting the safety of an officer or the general public.

~~4.3~~ *5.3* Dissemination

1. TACs must establish IWEITS specific to ~~his or her~~ *their* agency regarding dissemination of CHRI. A current list of the agency's authorized personnel must be referenced in the IWP and made available to the agency's terminal operators.

Primary Dissemination

1. Disseminating CHRI from any system on NCJIS to any unauthorized source is prohibited.

2. If the requesting agency's ORI is being used for the inquiry, it is considered primary dissemination and the transaction is electronically logged at the state level.

NOTE: It is at the discretion of individual agencies whether or not to log primary dissemination. [KM39]

Example #1: A Sheriff's Office uses their terminal and their own ORI to request information for their own use.

Example #2: A Sheriff's Office has a User Agreement/Letter of Understanding with the District Attorney's Office. The Sheriff's Office agrees to run transactions for the District Attorney using the appended District Attorney's ORI.

Secondary Dissemination

1. If the requesting agency's ORI cannot be used for the inquiry, or if the requesting agency ran the transaction for their purposes and later shared the information with another authorized agency, this is considered secondary dissemination and is not logged at the state level.

Example #3: A Sheriff's Office has a User Agreement/Letter of Understanding with the District Attorney's Office. The Sheriff Office agrees to run transactions for the District Attorney but is not able to use the District Attorney's ORI to run the transaction.

Example #4: A Sheriff's Office uses their terminal and their own ORI to run a transaction for their own use. Later the District Attorney requests a copy of the transaction to be used in a criminal case. The Sheriff's Office shares the information with the District Attorney's Office.

2. Secondary dissemination transactions must be maintained on a secondary dissemination log for one NCJIS audit cycle. The logs must contain the following:

   a. The date which the information was provided.

   b. The person who is the subject of the information.

   c. To what agency and person the information was provided to.

   d. A brief description of the information provided.

3. If a secondary agency is disseminating CHRI to another authorized Criminal Justice Agency, a log must be maintained containing the above information.

Example #5: A Sheriff's Office uses their terminal and their own ORI to run a transaction for their own use. Later the District Attorney requests a copy of the transaction to be used in a criminal case. The Sheriff's Office shares the information with the District Attorney's Office. The District Attorney's Office later disseminates the information to a court.

~~**NOTE: It is at the discretion of individual agencies whether or not to log primary dissemination.**~~ ***NOTE: If your agency does not practice secondary dissemination it must be specified in your agency's Internal Written Procedures (IWP).***

4. Information obtained from the III is considered CHRI. Its use shall be consistent as described in Title 28, Part 20, CFR, and the NCIC Operating Manual.

5. Further information regarding proper use, dissemination, storage and penalties for misuse can be obtained in the CJIS Security Policy.

~~**4.4 *5.4* Personally Identifiable Information (PII)**~~

~~For the purpose of this document, PII is information which can be used to distinguish or trace an~~

~~individual's identity as outlined in the CJIS Security Policy.~~

~~5.1~~ *6.0* General[KM40]

Procedures regarding the NCJIS Wanted Person File, including validations, entry, modification, clear, Nevada Offense Codes (NOC), etc. are outlined in detail in the NCJIS Operating Guide. Procedures regarding the NCIC Wanted Person File are contained in the current NCIC Operating Manual.

~~5.2~~ *6.1* Requirements for Warrant Entry into NCJIS

1. For a warrant(s) to be entered into the NCJIS Wanted Person File, the warrant(s) must be criminal in nature, be issued by a court, meet minimum mandatory field requirements pursuant to NCJIS Operating Guide and the entering agency must have the original or a copy of the warrant(s) on file. A fax copy or electronic form is permissible. The following rules apply:

    a. The entry of parking citations and/or civil infractions is prohibited.

    b. The NCJIS Wanted Person File is not to be used to "locate" persons.

    c. A valid warrant must exist to be entered into the NCJIS.

    d. The transportation field must contain accurate and true limitations.

    e. Packing the record with all available information at the time of entry is optimal for officer safety. Packing the record at a minimum includes:

        1. Scars, marks and tattoos.

        2. AKAs.

        3. Additional dates of birth.

        4. Additional social security numbers.

    f. The juvenile flag must be set when entering juvenile warrants.

~~5.3~~ 6.2 Double Entry (NCJIS & NCIC)

When the entry criteria for both NCJIS and NCIC are met, agencies may elect to enter a warrant(s) into both systems. Agencies who exercise this option must be aware that separate record validation requirements exist for each system.

NOTE: A second party check must be completed ***by an individual other than the original person entering the warrant.*** ~~**has been completed by an individual other than the individual entering the warrant.**~~

~~5.4~~ *6.3* Day Service Only Warrants

Courts may issue warrants for "Day Service Only" in accordance with NRS 171.136 (2). Any "Day Service Only" warrant must be reflected in the NCJIS entry pursuant to the NCJIS Operating Guide.

~~5.5~~ *6.4* NCJIS Hit Confirmation

1. Prior to taking any action on a state warrant for liability reasons, the investigating agency MUST confirm the validity of the warrant with the confirming agency.

2. Agencies with state warrants or an agency providing hit confirmation services must be available 24 hours a day, seven days a week.

3. Upon receipt of a hit confirmation request, the confirming agency must furnish a response of either positive, negative or indicate the specific amount of time necessary to confirm or reject.

    a. Response timeframes are as follows:
    Urgent: Within ten minutes
    Routine: Within one hour

4. Failing to respond to a hit confirmation request from another agency may result in NCJIS sanctions in the form of the record(s) being purged from NCJIS by the CSA.

5. Hit confirmation for an NCJIS Electronic warrant is not required unless the warrant hit states otherwise.

6. NCJIS Warrant hit confirmation procedures follow NCIC procedure which can be found in the Introduction, Section 3 #3.5 of the NCIC 2000 Operating Manual. EXCEPT that an AM should be sent to the confirming ORI in place of an YQ or YR. Agencies should retain paperwork for audit purposes.
When a YQ or YR is sent via Nlets, notices are generated to NCIC. Notices for *an* NCJIS warrant do not need to be sent to NCIC.

~~5.6~~ *6.5* Served Warrants

1. NCJIS warrants must immediately be removed once the wanted person has been served, arrested or no longer wanted. When the individual is booked on the warrant, it is the booking facility's responsibility to remove the warrant from the system.

2. When a wanted person is in custody for local charges and it is determined that an additional warrant(s) exists from another jurisdiction, the subject may be held on a detainer. The outside warrant(s) from another jurisdiction must not be cleared from NCJIS until the local charges have been satisfied and the warrant(s) is actually served.

~~5.7~~ *6.6* Validation of NCJIS Records

1. Agencies that enter a warrant(s) into the NCJIS Wanted Person file are responsible for ensuring that the information has been entered accurately and completely. Within 90 days after the initial entry of each warrant, the validating and/or entering agency will receive a list of warrant(s) they have entered in the NCJIS Wanted Person File.

2. Although a quality control review is not required during the above verification process, agencies are encouraged to provide accurate and complete information and to provide supplemental data when necessary to increase the effectiveness of the file.

~~5.8~~ *6.7* Validation of NCIC Records

All terminal or non-terminal agencies with entries in NCIC must abide by the validation procedures and schedule as established in Section 3.4 of the NCIC Operating Manual.

NOTE: Ultimate responsibility lies with the validating agency to ensure warrants are promptly removed from the system.

~~5.9~~ *6.8* NCJIS Retention Policy

Warrants will remain indefinitely until the warrant is removed or cleared.

~~Section 6~~ *Section 7* ELECTRONIC WARRANTS

~~6.1~~ *7.0* General

The Electronic Warrant File provides for a system-to system exchange of information. Electronic warrant submission requires a state issued ORI. All electronic warrants entered into the NCJIS Wanted Person file will remain indefinitely until they are either removed or cleared.

~~6.2~~ *7.1* Requirements for Electronic Warrant Entry into NCJIS

1. For a warrant(s) to be entered into the NCJIS Wanted Person file, the warrant(s) must be criminal in nature, be issued by a court, meet minimum mandatory field requirements pursuant to the NCJIS Operating Guide and the entering agency must have the original or a copy of the warrant(s) on file. An electronic form is permissible.

2. The entry of parking citations and/or civil infractions is prohibited.

3. The NCJIS Wanted Person file is not to be used to "locate" persons. A valid warrant must exist to be entered into NCJIS.

4. The transportation field must contain accurate and true limitations.

5. Packing the record with all available information ~~at the time of entry~~ is optimal for officer safety. Packing the record at a minimum includes:

    a. Scars, marks and tattoos.

    b. AKAs.

    c. Additional dates of birth.

    d. Additional social security numbers.

6. The juvenile flag must be set when entering juvenile warrants.

~~6.3~~ *7.2* Double Entry (NCJIS & NCIC)

When the entry criteria for both NCJIS and NCIC are met, agencies may elect to enter the warrant(s) into both systems. Agencies who exercise this option, however, must be aware that

separate record validation requirements exist for each system.

~~6.4~~ *7.3* Day Service Only Warrants

Courts may issue warrants for "Day Service Only" in accordance with NRS 171.136 (2). Any "Day Service Only" warrant must be reflected in the NCJIS entry, pursuant to the NCJIS Operating Guide.

~~6.5~~ *7.4* Hit Confirmation Requirements

Hit confirmation is not required for state electronic warrants. The ~~validity of the warrants is guaranteed by the~~ process of synchronization~~, thus~~ eliminat~~ing~~*es* the ~~need~~ *requirement* for law enforcement personnel to contact the agency of record prior to serving the warrant.

NOTE: Hit confirmation of the NCJIS electronic warrant is only required when noted on the warrant.

~~6.6~~ *7.5* NCJIS Warrant Synchronization

1. Electronic synchronization of state electronic warrant records must be completed nightly. The electronic synchronization will compare fields in the agency's warrant database with nightly files provided by DPS. On a monthly basis, the requesting agency will submit to their auditor a document verifying that the errors found through synchronization have been corrected. This document must include:
2.
   a. Date of the synchronization.
   b. Exact name on the warrant.
   c. Social Security number or case number.
   d. Warrants found in the agency's record management system (RMS) but not found as a State warrant file.
   e. Warrants in the NCJIS Wanted Person file, but not in the agency's RMS.
   f. Any differences between the NCJIS Wanted Person file and the agency's RMS.
   g. Date discrepancy was resolved.
3. In the case that the submitting agency is inquiry only, that agency must have an

agreement with an entering agency to perform emergency recall/clear/cancel functions.

NOTE: The CSA has the option to purge electronic warrant records upon approval by the Director of DPS, if an agency fails to follow NCJIS Policies and/or the NCJIS Operating Guide. Due to officer safety, liability and system integrity concerns the CSO is not bound by the "Sanction Process" but may immediately remove all unsynchronized or non validated records from the State system.

~~6.7~~ *7.6* NCJIS Electronic Warrant Audit

1. The CSA will monitor the new courts coming on-line to determine an acceptable error rate for a period of not less than six months and every ~~two~~ *three* years thereafter.

2. Terminal agencies that electronically submit warrant records to NCJIS will be audited every ~~two~~ *three* years in accordance with the NCJIS Audit Plan.

3. Courts submitting electronic warrants must retain the most recent twelve months of synchronization error reports for audit purposes.

~~7.0~~ *8.0* General

1. IWEITS must be in place for NCIC administrative messages and CSA quality control messages that relate to the agency.

2. Cross checks through DMV for vehicle registration, driver's license and NCJIS/NCIC criminal history files to find additional information to enhance a record entry is optimal for officer safety.

3. Records that contain errors or incorrect information must be promptly modified or removed to ensure maximum system accuracy and effectiveness.

~~7.1~~ *8.1* Quality Control Messages

Administrative Messages (AM) that are sent through Nlets are reviewed by the CSA for conformity to Nlets standards. See the Nlets User and Technical Guide for further information. Messages that do not conform will be returned to the agency by the *EITS* Helpdesk or the CSA.

~~Section 8~~ Section 9 AUDIT PLAN

~~8.0~~ *9.0* General

1. Agencies with ~~NCJIS~~ *state approved CJI* access will be audited every ~~two~~ *three* years by the CSA. The purpose of the audit will be to confirm compliance with ~~NCJIS and CJIS~~ *any CJIS Criminal Justice Information System* policy and procedures. ~~Agencies that access N-DEx will also be audited on N-DEx policies and procedures.~~

2. Directed audits will be conducted as necessary. A directed audit is defined as an audit that is conducted as a result of a complaint or request received by the CSA.

3. New terminal agencies will be audited within the first six months of coming on-line.

NOTE: Internal Written Procedures (IWP) must be specific to your agency's practices.

~~8.1~~ *9.1* Audit Plan

The Audit Plan focuses on nine areas of agency accountability which are as follows:

1. Administrative Responsibilities.

2. Security Requirements.

3. Personnel Training Standards.

4. Criminal History Record Information.

5. Wanted Person Files.

6. Electronic Warrants.

7. Data Integrity.

8. N-DEx.

9. Technical ~~Security~~ *Compliance*

NOTE: Internal Written Procedures (IWP) must be made available to audit staff upon request.

~~8.2~~ *9.2* System Discipline and Sanction Policies

The CSA has developed a three-phase sanction plan that will be initiated whenever an agency is not in compliance with NCJIS and CJIS policies and procedures. This process will enhance system integrity and security through increased user compliance.

PHASE 1

1. An audit report will be sent to the attention of the AA and the TAC for review and immediate corrective action.

2. A written formal response detailing the compliance resolution from the AA shall be directed to the assigned auditor from EITS, General Services Division within 30 business days of the audit report. The ~~following issues will be addressed:~~ *agency's formal response must include the following issues:*

    a. noncompliance issues cited in the scheduled audit

    b. documentation of corrective measures

    c. plans implemented to eliminate future noncompliance

3. If noncompliance remains an issue, Phase 2 will be initiated.

PHASE 2

1. A letter from the CSA will be forwarded to the AA outlining the result of the NCJIS audit and the agency's failure to implement corrective measures. This letter will request a meeting regarding implementation of limited NCJIS services for the subject agency and will be submitted via the DPS chain of command.

2. Limited sanctions that may be initiated at this time are:

    a. Suspended access to NCJIS.

    b. All other NCJIS services restricted to one terminal and one printer.

c. 60 days probation, which may include requirements to provide additional documentation.

d. Electronic warrants failing compliance issues will be required to perform hit confirmations and monthly validation procedures.

2. If noncompliance remains an issue, Phase 3 will be initiated.

PHASE 3

1. A formal letter from the Director of the DPS will be forwarded to the AA advising that NCJIS services to that agency have been terminated. This letter will address the noncompliance issue(s), failure to implement appropriate corrective measures and previously imposed sanctions.

2. Termination of the ability to submit electronic warrants.

3. All action taken by the DPS will be documented and maintained at the General Services Division.

REINSTATEMENT OF NCJIS SERVICES

1. To regain access to NCJIS services, a formal letter from the AA must be submitted to the CSA. All of the following issues must be addressed:

a. Noncompliance issues that initiated the enforced sanctions.

b. Implemented plans to ensure compliance in the future.

c. Documentation of retraining agency personnel, if applicable and

d. Requested date for re-inspection by General Services Division personnel.

2. Upon completion of a satisfactory re-inspection by General Services Division personnel, the agency's original level of access will be restored.

3. The agency will be placed on probation for a period of one year and areas of non-compliance will be monitored.

ADMINISTRATIVE RESPONSIBILITIES

10.1.0 General

The Nevada Central Repository is housed within the Nevada Department of Public Safety, General Services Division. The Central Repository is responsible for Non-criminal Justice Agencies (NCJA) requesting access to Criminal History Record Information (CHRI), as authorized by legislative enactment or federal executive order to request civil fingerprint-based background checks for licensing, employment, or other noncriminal justice purposes.

The National Crime Prevention and Privacy Compact Council works in partnership with criminal history record custodians, end users, and policy makers to regulate and facilitate the sharing of complete, accurate, and timely CHRI to noncriminal justice users in order to enhance public safety, welfare, and security of society while recognizing the importance of individual privacy rights. This is facilitated in part through the development of resource materials for use in protecting criminal justice information from unauthorized and inappropriate access, collection, maintenance and disclosure.

Within the Central Repository, the Nevada Criminal Justice Information System (NCJIS) Compliance Unit (NCU) performs several duties in regard to compliance with the federal and state regulations for noncriminal justice access to CHRI:

- *Training on the use of CHRI*
- *Conducting audits*
- *Researching/investigating security breaches*

Note: This does not include civil applicant agencies that are granted access to the Nevada Applicant Background Check System (NABS) in regards to Nevada Revised Statute (NRS) Chapter 449.

10.1.1 Requirements for receiving an account

1. *For initial access to receive CHRI, the NCJA must submit its defining statutory or federal authority for review to the Central Repository through the application process.*

2. *Certain statutory and/or federal authority guidelines require training prior to being granted access to CHRI. For example, if the NCJA is applying for the National Child Protection Act of 1993, as amended by, Volunteers for Children Act (NCPA/VCA).*

10.1.2 Contract between Public Agencies

(Interlocal Contracts, User Agreements, Letters of Understanding, Security Addendums)

1. *All agencies that have been approved for access to CJI must enter into an Interlocal Contract between Public Agencies with the Department of Public Safety (DPS), General Services Division and are legally bound thereby and agree to abide by all provisions contained therein. The contract serves to identify the responsibilities between the CJIS Systems Agency (CSA) and the noncriminal justice agency.*

- *Authority and Purpose: It is prohibited for noncriminal justice agencies to use CHRI for any purpose other than that for which it was requested.*
- *Authorized Recipient (AR): Agencies must appoint an AR within the agency that is responsible for viewing or handling CHRI.*
- *Training: Agency contact is responsible to train on the security and handling of CHRI for any additional personnel based on the required policies/procedures.*
- *Destruction: Authorized recipient (AR) is responsible for the destruction of all CHRI*
- *Policies/ Procedures: Agencies must implement policies and procedures which provide for the security and proper handling of the CHRI. As a best business practice agencies should also have rules for fingerprint submissions which include proper applicant identification and protecting the fingerprint card from tampering.*

2. *Agreement shall be reviewed at the next compliance audit by the NCJIS Audit staff. The agreement shall remain in force until:*

   a. *Authorized Recipient violates any portion of the agreement or policies which result in the termination of said access; OR*

   b. *Authorized Recipient advises the Central Repository in writing of the agency's wish to cancel access; OR*

   c. *Until renewed by the Central Repository*

10.1.3 Responsibilities of the Authorized Recipient (AR)

The AR is designated as the primary liaison between their agency and the Central Repository, and is responsible for coordinating agency compliance pertaining to the access, use, handling, dissemination and destruction of CHRI.

1. *Must complete mandatory training set by the Central Repository.*

2. *Serves as the central contact point to DPS NCJIS Compliance Unit (NCU).*

3. *The AR must immediately notify the Central Repository of any intentional misuse of CHRI.*

4. *Maintain an Authorized Personnel List of agency personnel who are part of the determination group. A determination group is defined as any agency personnel who plays a part in making the determination for suitability or eligibility to work or volunteer for your agency.*

5. *Ensure their agency determination group has been properly trained as determined by the Central Repository.*

6. *Ensure all personnel who are a part of the determination group have a signed a Training Acknowledgment understanding the penalties for misuse of the information. This must be maintained on file as long as they are in a determination role.*

7. *As defined in Title 28 Code of Federal Regulations, the Fingerprint Background Waiver must be signed and dated prior to submission of fingerprints. This waiver advises the applicant of the background check, and of their rights regarding challenging the accuracy of the record. This waiver must be maintained on file for one complete audit cycle (3 years).*

8. *As defined in Title 28 Code of Federal Regulations, the Notice to Applicant Waiver must be signed and dated prior to submission of fingerprints. This waiver advises the applicant of the background check, and of their rights regarding challenging the accuracy of the record.*

9. *Cooperate and give assistance to the NCJIS Compliance Staff with required or directed compliance audits.*

10. *Must always have an appointed Agency Contact Person. The AR must notify the Central Repository within 10 days when changes occur in the agency name, contact person, mailing address, and/or phone number.*

In addition the following is highly recommended for the AR:

- *The AR must be available during hours that are conducive to communicating with DPS NCU personnel.*

10.1.4 Termination of access to State and FBI Responses

1. *At the recommendation of the CSO and approval by the Director of the DPS, the Central Repository may suspend or terminate access to CHRI for a violation of a specific term of the*

Interlocal Contract between Public Agencies. In addition, any violation of NCJIS, state or federal statutes, regulations or rules incorporated in the Noncriminal Justice Agency shall be deemed a breach of terms. Suspension or termination shall commence upon 30 days advance written notice to the user from the CSO.

2. *Any agency may terminate access to CHRI with written notice from the AR to the CSO/ Central Repository.*

SECURITY AND TRAINING REQUIREMENTS

10.2.0 General

1. *The AR of the agency must establish and maintain Internal Written Procedures (IWP) specific to their agency including the following CHRI privacy and security areas and ensure all personnel deemed part of the determination group are aware of them:*
2.

a. *Purpose:*
i. *The specific use for CHRI*
ii. *Restricting use to the specific purpose for which CHRI was requested*

b. *Security*
i. *Access:*
1. *Defining who is authorized to access CHRI*
2. *Restricting access to only those who are authorized to handle CHRI.*
3. *Responsible to maintain CHRI in a secure records environment at all times.*
ii. *Unauthorized Access:*
iii. *Logging/Tracking Procedures*
iv. *Extraction, refer to section on Dissemination of CHRI.*

c. *Storage*
i. *CHRI must be maintained in a secure records environment at all times.*
1. *Secure Records Environment is defined as a secure file, safe or other security device, such as a locked file cabinet only accessible by the AR. This includes securing the area to be out of public view.*
ii. *Where is CHRI maintained?*
iii. *Is CHRI stored electronically?*
iv. *Who has access to CHRI? (This includes but is not limited to maintenance or outside personnel)*
v. *Proper security of CHRI from receipt through destruction.*
d. *Dissemination:*
i. *Agencies obtaining information from CHRI are responsible for maintaining the security and confidentiality of the CHRI. The Nevada Central Repository prohibits dissemination of any information received from CHRI to any unauthorized person or unauthorized agency.*
ii. *Logging/Tracking procedures*
iii. *Extraction*
e. *Destruction:*

i. *Retention/destruction rules and process*
ii. *Agency AR must destroy CHRI or any information derived from CHRI by either shredding or burning.*

f. *Penalties for misuse:*
i. *If the unauthorized use or dissemination includes CHRI, the person may be subject to criminal charges pursuant to NRS 179A.900.*

3. *Training Acknowledgments must be signed and dated, then maintained on file as set by the Central Repository.*

Note: Training will be provided by the CSO/Central Repository or by designee.

10.2.1 Dissemination

Secondary Dissemination

1. *Disseminating CHRI to any unauthorized source is prohibited.*

2. *If an agency is disseminating CHRI to the applicant for the applicant to challenge his/her criminal history record, a secondary dissemination log must be maintained, and the log must contain the following information:*

    a. *The date the information was provided.*

    b. *The subject of the record*

    c. *The Information is being disseminated (State Background Check or National Background Check).*

    d. *To whom the record is being disseminated to (only the applicant).*

Note: It is considered best business practice to include the steps your agency took to validate the applicant's identity if you are disseminating the record to the subject of the record in person. If the record is being mailed using the US Postal Service, this should also be indicated.

~~*3. If applicant is challenging, must be within 90 days from when the response was generated.*~~

AUDIT

10.3.0 General

1. *Civil Applicant agencies that receive CHRI directly from the Central Repository will be audited every three years by the CSA.*

2. *Directed audits will be conducted as necessary. A directed audit is defined as an audit that is conducted as a result of an incident/allegation or request received by the CSA.*

3. *New agencies will be audited within the first six months of receiving CHRI.*

10.3.1 Audit Plan

The Audit Plan focuses on five areas of agency accountability which are as follows:

1. *Use of CHRI.*
2. *Dissemination of CHRI.*
3. *Personnel Training Standards.*
4. *Applicant Notification and Record Challenge.*
5. *Privacy and Security of CHRI.*
6. *Outsourcing of Noncriminal justice Administrative Functions.*

OUTSOURCING RESPONSIBILITES

10.4.0 General

1. *Outsourcing is available to all agencies excluding the NCPA/VCA accounts. If an agency chooses to outsource their duties or store CHRI offsite then Attachment A: Security and Management Control Outsourcing Standard for Non-Channelers, and Attachment B: Responsibility Table for Non-Channeling must be followed.*

DISCIPLINE AND SANCTION POLICIES

10.5.0 General

The CSA has developed a three-phase sanction plan that will be initiated whenever an agency is not in compliance with the Intrastate Interlocal Contract.

PHASE 1

2. *An audit report will be sent to the attention of the AR for review and immediate corrective action.*
3. *A written formal response detailing the compliance resolution from the AR shall be directed to the assigned auditor from DPS, General Services Division within 30 business days of the audit report. The following issues will be addressed*

    a. *noncompliance issues cited in the scheduled audit*

b. *documentation of corrective measures*
c. *plans implemented to eliminate future noncompliance*

3. *If noncompliance remains an issue, Phase 2 will be initiated.*

PHASE 2

1. *A letter from the CSA will be forwarded to the AR outlining the result of the NCJIS audit and the agency's failure to implement corrective measures. This letter will request a meeting regarding implementation of limited access to CJI for the subject agency and will be submitted via the DPS chain of command.*

2. *Limited sanctions that may be initiated at this time are:*

a. *Suspended access to CHRI.*
b. *60 days probation, which may include requirements to provide additional documentation.*

2. *If noncompliance remains an issue, Phase 3 will be initiated.*

PHASE 3

a. *A formal letter from the Director of the DPS will be forwarded to the AR advising that NCJIS services to that agency have been terminated. This letter will address the noncompliance issue(s), failure to implement appropriate corrective measures and previously imposed sanctions.*

b. *All action taken by the DPS will be documented and maintained at the General Services Division.*

REINSTATEMENT OF NCJIS SERVICES

1. *To regain access to CJI, a formal letter from the AR must be submitted to the CSA. All of the following issues must be addressed:*

a. *Noncompliance issues that initiated the enforced sanctions.*
b. *Implemented plans to ensure compliance in the future.*
c. *Requested date for re-inspection by General Services Division personnel*

2. *Upon completion of a satisfactory evaluation of submitted documentation to the General Services Division personnel, the agency's original level of access will be restored.*

3. *The agency will be placed on probation for a period of one year and areas of non-compliance will be monitored.[KM41]*

APPENDIX A TERMS AND DEFINITIONS

Access to Criminal Justice Information – The physical or logical (electronic) ability, right or privilege to view, modify or make use of Criminal Justice Information.

Agency Administrator (AA) – An individual located within an agency that is ultimately responsible for security and compliance requirements.

Administrative Messages (AM) – A secure and documentable means of interagency communication. An AM may be used for any type of official law enforcement or public safety purpose as approved by Nlets and NCIC.

Assistant Terminal Agency Coordinator (ATAC) – An individual located within an agency designated to assist the terminal agency coordinator as liaison between the agency and the CSA.

Authorized Personnel/Criminal Justice Practitioner – A non-sworn or non-terminal operator that could receive or view hard copy NCJIS/NCIC record information.

AUTHORIZED RECIPIENT (Civil Accounts) - (1) A non-governmental entity authorized by federal statute or federal executive order to receive CHRI for non-criminal justice purposes, or (2) a government agency authorized by federal statute, federal executive order, or state statute which has been approved by the United States Attorney General to receive CHRI for non-criminal justice purposes.

AUTHORIZED RECIPIENT (NCPA/VCA accounts) - A governmental, public, private, for-profit, or not-for-profit entity operating within the State of Nevada authorized to submit fingerprint cards and review resultant CHRI as part of the screening process for current and/or prospective employees, volunteers, contractors and vendors who have or may have unsupervised access to children, the elderly or disabled persons for whom AUTHORIZED RECIPIENT provides services or care.

Authorized User/personnel – An individual, or group of individuals, who have been appropriately vetted (national fingerprint-based record check, a wants/warrant check and received appropriate training) and have been granted access to CJI.

CJIS Security Officer (CSO) – An individual located within the CSA responsible for the administration of CJIS for the CSA.

CJIS Security Policy – The FBI CJIS Security Policy document as published by the FBI CJIS ISO.

CJIS System Agency (CSA) – A state criminal justice agency providing access to its criminal justice users with respect to CJIS data. There can only be one CSA per state.

California Law Enforcement Telecommunications System - (CLETS)

Confidentiality – The concept of ensuring that information is observable only to those who have been granted authorization to do so.

Contractor – A private business, agency or individual which has entered into an agreement for the administration of criminal justice or noncriminal justice functions with a Criminal Justice or a Noncriminal Justice Agency.

Criminal History Record Information (CHRI) – A subset of CJI. Any notations or other written or electronic evidence of an arrest, detention, complaint, indictment, information or other formal criminal charge relating to an identifiable person that includes identifying information regarding the individual as well as the disposition of any charges.

Criminal Justice Information (CJI) – Criminal Justice Information is the abstract term used to refer to all of the NCJIS and FBI CJIS provided data necessary for law enforcement agencies to perform their mission and enforce the laws, including but not limited to: biometric, identity history, person, organization, property, and case/incident history data. In addition, CJI refers to the NCJIS and FBI CJIS-provided data necessary for civil agencies to perform their mission; including but not limited to data used to make hiring decisions.

~~**Criminal Justice Information Services (CJIS) –** *CJIS is a system within, and* administrated by the FBI that provides law enforcement with timely and secure access to services that provide data wherever and whenever needed for stopping and reducing crime.~~

Criminal Justice Information Services Division (FBI CJIS or CJIS) *— The FBI division responsible for the collection, warehousing, and timely dissemination of relevant CJI to the FBI and to qualified law enforcement, criminal justice, civilian, academic, employment, and licensing agencies.*

Direct Access – (1) Having the authority to access systems managed by NCJIS and the FBI CJIS Division, whether by manual or automated methods, not requiring the assistance of, or intervention by, any other party or agency (28 CFR, Chapter 1, Part 20). (2) Having the authority to query or update national databases maintained by NCJIS and the FBI CJIS Division including national queries and updates automatically or manually generated by the CSA.

Dissemination – ~~The transmission/distribution of CJI to authorized recipients.~~ *Disclosing records of criminal history or the absence of records of criminal history to a person or agency outside the organization which has control of the information.*

Escorting – An unauthorized person ~~being escorted~~ in a physically secure area must be escorted by a person who is sufficiently familiar with the equipment in the area and the tasks being performed. The escort must be able to identify an unauthorized act and alert security personnel. If the escort does not have this set of knowledge and skills, then the ~~unauthorized person is not considered escorted.~~ person cannot be an escort.

Federal Bureau of Investigation (FBI)

Information Security Officer (ISO) – An individual designated by the CSO who has the responsibilities to establish and maintain information security policy, assesses threats and vulnerabilities, performs risk and control assessments, oversee the governance of security operations and establishes information security training and awareness programs. The ISO interfaces with security operations to manage implementation details and with

auditors to verify compliance to established policies.

Internal Written Procedures (IWP) – An Agency's written procedures detailing how a policy will be implemented.

Interstate Identification Index (III) – The CJIS service that manages automated submission and requests for CHRI that is warehoused subsequent to the submission of fingerprint information. Subsequent requests are directed to the originating state as needed.

Law Enforcement National Data Exchange (N-DEx) – FBI CJIS division system providing law enforcement agencies with a shared investigative tool. For further reference see the Audit Section of this Manual.

Local Agency Security Officer (LASO) – A point-of-contact designated as the liaison between their agency and the ISO who has access to the NCJIS network and provides any needed technical systems assistance to help assure the confidentiality, integrity and availability of criminal justice information on the network.

National Crime Information Center (NCIC) – ~~An~~ *FBI* information system which stores CJI which can be queried by appropriate Federal, state and local law enforcement, criminal justice and certain noncriminal justice agencies.

Nevada Criminal Justice Information System (NCJIS) - The primary function of the Nevada Criminal Justice Information System is to provide an efficient and effective system for the expeditious exchange of criminal justice or related information.

Nlets – ~~Powers~~ The International Justice and Public Safety Network.

Non terminal Agency (NTA) – An agency having access to NCJIS/NCIC information through a terminal agency.

Non-Terminal Agency Coordinator - *An individual located within an agency designated as the liaison between his or her agency and the CSA. The TAC administers NCJIS/CJIS systems programs within the local agency and oversees the agency's compliance with those policies.*

NRS – Nevada Revised Statutes

Originating Agency Identifier (ORI) – A unique alpha numerical identifier authorized by the CSA.

~~**Program Development and**~~ ***NCJIS*** **Compliance Unit (~~PD& C~~ *NCU*) -** Manages, trains and audits Users of the NCIC/NCJIS systems, Civil Applicant, Civil Name Check and the Uniform Crime Reporting (UCR) program. Serves as the CJIS Systems Agency (CSA) for the State which includes the National Crime Information Center (NCIC), Interstate Identification Index (III), Nlets and California Law Enforcement Telecommunications System (CLETS).

~~***Personally Identifiable Information (PII)*** ~~ ~~is any information maintained by an agency that is derived from CJI. PII includes, but is not limited to: any information which can be used to distinguish or trace and individual's identity (to include at least two items from the provided list), such as their name, social security number, date and place of birth, mother's maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.~~

Physically Secure Location – A facility or an area, a room, or a group of rooms, within a facility with both the physical and personnel security controls sufficient to protect CJI and associated information systems.

Secondary Dissemination – The release of CHRI from one agency to an authorized recipient agency when the recipient agency's ORI was not used to run the transaction.

Terminal Agency (TA) – An agency that has direct computer access to the NCJIS/NCIC system.

Terminal Agency Coordinator (TAC) – An individual located within an agency designated as the liaison between his or her agency and the CSA. The TAC administers NCJIS/CJIS systems programs within the local agency and oversees the agency's compliance with those policies.

Terminal Operator – An individual, ~~whom~~ *that* transmits, receives and coordinates information through direct communication to the NCJIS system (NCJIS, NCIC, Nlets and CLETS in compliance with state and federal regulations.