MARTY J. JACKLEY
ATTORNEY GENERAL

STATE OF SOUTH DAKOTA
DIVISION OF CRIMINAL INVESTIGATION
OFFICE OF ATTORNEY GENERAL
GEORGE S. MICKELSON CRIMINAL JUSTICE CENTER
PIERRE, SOUTH DAKOTA 57501-8505
PHONE (605) 773-3331
FAX (605) 773-4629

Law Enforcement Training
State Forensic Laboratory

To Whom it May Concern:

Per federal requirements, the South Dakota Division of Criminal Investigation is implementing a Non-Criminal Justice Agency User Agreement for all non-criminal justice agencies which have obtained enabling legislation allowing them to request and receive fingerprint-based national criminal history information (CHRI).

Please read through the User Agreement carefully and complete all required documents. Maintain a copy for your records and return the original to:

Division of Criminal Investigation
Attn: Jami Oakland
1302 E Hwy 14 Ste 5
Pierre SD 57501

Enclosed is a sample of the Audit Questionnaire. Per federal requirements, your agency will be audited once every three years. The agency will first receive an Audit Questionnaire via mail. Once the Audit Questionnaire is complete and received by DCI, an on-site audit will be conducted.

If you have any questions, please feel free to contact me at (605) 773-4614.

Sincerely,

Jami Oakland

Jami Oakland, Identification Specialist

Enclosures

SOUTH DAKOTA
DIVISION OF CRIMINAL INVESTIGATION

GUIDE FOR NONCRIMINAL JUSTICE AGENCY

Table of Contents

Acronym Glossary

CHRI	Criminal History Record Information
CJI	Criminal Justice Information
CJIS	Criminal Justice Information Services
FBI	Federal Bureau of Investigation
III	Interstate Identification Index
LASO	Local Agency Security Officer
NAC	Noncriminal Agency Coordinator
NCJA	Noncriminal Justice Agency
NSA	Nation Security Agency
ORI	Originating Agency Identifier
POC	Point of Contact
SDDCI	South Dakota Division of Criminal Investigation
SDCL	South Dakota Codified Law
SIB	State Identification Bureau

Introduction

This guide sets forth procedures and guidelines for noncriminal justice agencies that access criminal history record information (CHRI) through fingerprint submissions. It is designed to be a reference for agencies regarding the access, maintenance, dissemination, and audit requirements for CHRI.

South Dakota Codified Law §23-5-12. Examination of own criminal history information--Written request--Authorization of release to others--Waiver of liability. Any person may examine criminal history information filed with the attorney general that refers to that person. The person requesting such information shall supply the attorney general with a written request together with fingerprint identification. The person may also authorize the attorney general to release his criminal history information to other individuals or organizations. The attorney general may require the person to sign a waiver releasing the state, its employees or agents from any liability before releasing criminal history information.

Agency User Agreement

Each agency authorized to receive CHRI must sign a user agreement. A user agreement (see appendix A) is a contractual agreement between the authorized receiving agency and the SDDCI; it must be signed by SDDCI and the appropriate authority at the user agency. The user agreement contains Terms and Conditions which include the following:

The user agreement states the nature of the requesting organization, the purpose for which CHRI is requested, and the specific authorization granting access to the information. It is prohibited for noncriminal justice agencies to use CHRI for any purpose other than that for which it was requested.

The chief official of each noncriminal justice agency will designate a Noncriminal Agency Coordinator (NAC) to act as the primary contact person for that agency. The NAC should complete SDDCI training requirements and shall serve as liaison between the agency and SDDCI. The NAC should ensure all employees are current on training and assist SDDCI personnel in the audit process. (see appendix B)

The user agreement requires the appointment of a Local Agency Security Officer (LASO) to act as liaison with SDDCI to ensure the agency is in compliance with security procedures. (see appendix C) This individual must be knowledgeable in CHRI, policies and mandated rules and regulations as well as knowledge of IT security procedures.

Agencies are responsible for complying with mandatory training requirements. SDDCI will provide training or instruction on fingerprint handling and submission for all agencies accessing CHRI. All agency personnel who view or handle CHRI must complete the

standard online training (CJIS Online) and undergo agency internal training on CHRI security and handling based on the required policies/procedures.

As part of privacy and security, agencies are required to develop and implement policies and procedures which provide for the security and proper handling of the CHRI. Agencies should also have rules for fingerprint submissions which include proper applicant identification and protecting the fingerprint card from tampering.

The user agreement is subject to cancellation by either party with 30 days written notice. SDDCI reserves the right to suspend service for violations or for investigations of apparent/alleged violations of the User Agreement or requirements for access. State and federal civil and/or criminal penalties may apply for misuse of CHRI.

What is CHRI

CHRI includes information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, information, or other criminal charges, any dispositions arising therefrom, sentencing, correctional supervision, and release. SDDCI is the state central repository for the collection, maintenance, and dissemination of CHRI.

CHRI does not include driver history records.

The FBI CHRI could contain more or less information than is on the South Dakota response.

Use of CHRI

The FBI is authorized to exchange CHRI with, and for the official use of, authorized officials of the federal government, states, cities, and other institutions. CHRI may be made available for use in connection with licensing or employment, pursuant to SDCL 23-15-21.1 or other federal legislation and for other uses for which dissemination is authorized by federal law. CHRI obtained under such authority may be used solely for the purpose for which the record was requested. When CHRI is needed for a subsequent authorized use, a new record request must be conducted to obtain current information. Subject fingerprints or other approved forms of positive identification shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the Interstate Identification Index (III) using name-based inquiry and record request messages is not permitted for noncriminal justice purposes, unless otherwise approved by the FBI and/or the Compact Council pursuant to applicable authority. To review the State and Federal regulations regarding the use of CHRI (see appendix D)

Agencies must have an Originating Agency Identifier (ORI) number assigned to them as a prerequisite to obtaining a fingerprint-based criminal history record.

Misuse of CHRI

The exchange of the CHRI is subject to cancellation if dissemination is made outside the receiving departments or related agencies and if CHRI is used for any other reason not stated in the South Dakota state law. Furthermore, depending upon the nature of the offense and the identity of the offender, federal or state crimes may be charged for the willful, unauthorized disclosure of CHRI. Misuse of the CHRI is a misdemeanor or felony depending on the circumstances.

Penalties For Unauthorized Disclosure

Title 28, U.S.C., Section 534, Pub. L. 92-544 and Title 28, CFR, 20.33(b), provide that the exchange of records and information is subject to CANCELLATION if dissemination is made outside the receiving departments or related agencies. Furthermore, depending upon the nature of the offense and the identity of the offender, federal or state crimes may be charged for the willful, unauthorized disclosure of CHRI. Depending on the authority to which the CHRI was authorized for dissemination, penalties may be different according to the authority.

SDCL Ch. 23-5 and SDCL Ch. 23-6 makes reference that all criminal history record information is confidential and any person who discloses the information beyond the scope allowed is guilty of a Class 2 misdemeanor.

Applicant Notification and Record Challenge

Applicants who are the subject of a national fingerprint-based criminal history record check for a noncriminal justice purpose, have certain rights which are discussed below.

Applicants must be provided written notification that the applicant's fingerprints will be used to check the criminal history records of the FBI. They are allowed a reasonable opportunity to challenge the accuracy of the CHRI. (ALL applicants must be advised of this, not just those who dispute an employment/license denial or who feel their CHRI is incorrect). If the applicant elects to challenge the CHRI, the agency must provide the applicant a reasonable period of time to do so before final denial. The agency should also establish and document what constitutes a reasonable period of time for the review and challenge and any appeals process that is available to the applicant.

Information on how to review and challenge an FBI Identity History check can be found on the FBI website at: http://www.fbi.gov/about-us/cjis/identity-history-summary-checks/challenge-ofan-identity-history-summary.

Dissemination Of Criminal History Record Information

With all authorized dissemination, a dissemination log shall be maintained from the time of authorized dissemination until the agency receives a successful Policy Compliance Review. AUDITs are conducted on a triennial basis; therefore, all dissemination logs shall be maintained from the time of the initial AUDIT until the next AUDIT cycle.
A dissemination log may be kept in different formats. Some of the general dissemination logs are maintained on a Microsoft Excel spreadsheet. However, a copy of the correspondence that accompanies the record dissemination also may serve as a dissemination log if kept in the applicant file or is accessible to the auditor upon request.

The CHRI Secondary Dissemination log should contain two forms of information for all authorized dissemination (see appendix E). A CHRI secondary dissemination Record must be completed and kept for Audit. (see appendix F).

The first part should identify the record being disseminated and should include:
- The name of the subject of record (last, first, middle initial);
- The date of birth of the subject of record;
- The social security number (optional) of the subject of record;
- The agency name (qualified entity) releasing the record; and,
- The date released.

The second part of the log should indicate to whom the record is being provided and should include:
- The name of the person requesting the record;
- The requesting agency and address of the requesting agency;
- The purpose for the record request; and,
- Signature of the person signing for the record (if mailing the record, the name, title and address of the authorized recipient).

If the dissemination is for the subject of record, only the subject of record may pick up his/her record.

A valid photo ID should be shown prior to release.

Violations and associated penalties for misuse of dissemination practices are stated in SDCL Ch. 23-5 and SDCL Ch. 23-6.

Security of CHRI

Physical media shall be securely disposed of when no longer required, using formal procedures. Formal procedures for the secure disposal or destruction of physical media shall minimize the risk of sensitive information compromised by unauthorized individuals. Physical media shall be destroyed by shredding or incineration.

Agencies shall ensure the disposal or destruction is witnessed or carried out by authorized personnel.

Agencies shall sanitize, by overwriting at least three times or delete electronic media prior to disposal or release for reuse by unauthorized individuals. Inoperable electronic media shall be destroyed (cut up, shredded, etc.). Agencies shall maintain written documentation of the steps taken to sanitize or destroy electronic media. Agencies shall ensure the sanitization or destruction is witnessed or carried out by authorized personnel. Agencies must have these procedures written in the agency's policy.

Physical Security: Agencies are required to establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity. The agencies must have these procedures written in the agency's policy. This includes maintaining CHRI in a secure location that is not readily accessible to individuals not authorized to see it.

Physical Security includes:

1. Protection of information subject to confidentiality;
2. Limitation of visitor access to controlled areas;
3. Prevention of social engineering;
4. Positioning of computer and system devices (lap tops, cellular phones, I-pads, or any kind of hand held devices used to access, process or store CHRI media) in such a way that prevents unauthorized personal gaining physical or visual access; and
5. Locking of rooms, areas, or storage containers where CHRI media is accessed, processed and/or stored.
6. CHRI shall not be stored in individual's personnel file.

Personnel Security: The training shall provide employees with a working knowledge of federal and state regulations and laws governing the security and processing of CHRI.

Maintenance (Retention and) Of Criminal History Record Information

Criminal history record information may be retained in hard copy format and electronic format. Criminal history record information needs to be retained only for the length of time it is needed. Pursuant to the CJIS Security Policy, the records shall be stored for extended periods of time only when they are key elements for the integrity and/or utility of case files. Therefore, if it is not an agency requirement, the hard copy record information may be destroyed.

It is recommended that an agency conduct in-house shredding of criminal history record information or that agency personnel supervise the destruction of the records if an agency uses a contracted vendor. If criminal history record information is allowed

outside the controls of the authorized agency, it becomes an outsourcing standard requirement.

Example 1: The agency has a contracted destruction service and provides locked bins for the housing of criminal history records to be destroyed. The contractor picks up the bins, and leaves new, empty bins.

Is this acceptable? No. This would require an outsourcing standard.

Example 2: The agency has a contracted destruction service that provides locked bins for the housing of criminal history records for destruction. The contractor picks up the bins and shreds in view of agency personnel.

Is this acceptable? Yes.

Example 3: The agency destroys all criminal history record information in-house. The Agency keeps the shredded information in a bin for pick up by a contracted vendor.

Is this acceptable? Yes.

Training

Agencies are responsible for mandatory training requirements. All persons directly associated with the accessing, maintaining, processing, dissemination or destruction of CHRI shall be trained. Training must be completed within six (6) months of initial assignment, and biennially thereafter. The CJIS Security Training has a two (2) year recertify training for noncriminal justice agencies and one (1) year recertify training for outsourced vendors.
The CJIS Security Training can be located at www.cjisonline.com.

There are three Levels of CJIS Security Training:

Level 1 – All personnel with access to Criminal Justice Information (CJI). This level is designed for people who do not have physical and logical access to CJI but may encounter it in their duties.
Level 2 – All personnel with both physical and logical access to CJI.
Level 3 - All personnel with Information Technology Roles. This level is designed for all information technology personnel including system administrators, security administrators, network administrator, etc.

Security Training Minimums: At a minimum, the following topics shall be addressed as baseline security awareness training for all authorized personnel with access to CHRI:

1. Rules that describe responsibilities and expected behavior with regard to CHRI usage;
2. Implications of noncompliance;
3. Incident response (points of contact; individual actions);
4. Media protection;
5. Visitor control and physical access to spaces—discuss applicable physical security policy and procedures, e.g., challenge strangers, report unusual activity;
6. Protect information subject to confidentiality concerns — hardcopy through destruction;
7. Proper handling and marking of CHRI;
8. Threats, vulnerabilities, and risks associated with handling of CHRI;
9. Social engineering; and
10. Dissemination and destruction.

Outsourcing of Noncriminal Justice Administrative Function

The Compact Council published a Final Rule in the Federal Register regarding a Security and Management Control Outsourcing Standard, (see appendix G) which became effective December 15, 2005. The goal of the Outsourcing Standard is to permit the outsourcing (delegation of non-core operations from internal production to an external entity specializing in the management of that operation) of noncriminal justice functions related to processing CHRI obtained from the III. The Outsourcing Standard permits a governmental agency or other authorized recipient of CHRI to select a private or governmental agency to perform these noncriminal justice administrative functions on behalf of the governmental or authorized agency, subject to appropriate controls. The NCJA should provide SDDCI written permission to outsource and SDDCI will notify the agency whether the outsourced vendor is approved or denied.

The Outsourcing Standard establishes minimum standards to ensure that security and privacy requirements are satisfied while CHRI obtained from the III is under the control or management of a third party. The contracting parties may not reduce these minimum standards; however, they may adopt more strict standards than required.

The Outsourcing Standard identifies duties and responsibilities for adequate security controls between the authorized recipient and the Vendor in order to maintain the security, accuracy, and reliability of the III system and CHRI.

South Dakota governmental agencies that obtain national CHRI for noncriminal justice purposes under an approved Public Law 92-544 statute may utilize the Compact Council's Outsourcing Standard to permit a Vendor or Vendors to perform the administration of noncriminal justice functions associated with national criminal history records on behalf of the authorized government recipient. The Outsourcing Standard may require additional stricter requirement on the Vendors performing noncriminal

justice functions. This includes forwarding the FBI record to a third party subcontractor to determine employment or licensing eligibility at the lowest agency level.

IT Security and Responsibilities of CHRI

1. Password use and management;
2. Appropriate use and management of e-mail, spam and attachments;
3. Appropriate web use;
4. Use of encryption; for transmission of sensitive/confidential information through electronic means; and
5. Provide data backup and storage through centralized and decentralized approaches, when applicable;
6. Provide timely application of system patches as part of configuration management;
7. Provide access control measures; and
8. Provide protection measures for agency network infrastructure.

Configuration Management

Access Restrictions for Changes: Planned or unplanned changes to the hardware, software, and/or firmware components of the information system can have significant effects on the overall security of the system. The goal is to allow only qualified and authorized individuals access to information system components for purposes of initiating changes, including upgrades, and modifications.

The agency shall ensure that a complete topological drawing depicting the interconnectivity of the agency network, to criminal justice information, systems and services is maintained in a current status.

The network topological drawing shall include the following:

1. All communications paths, circuits, and other components used for the interconnection, beginning with the agency-owned system(s) and traversing through all interconnected systems to the agency end-point;
2. The logical location of all components (e.g., firewalls, routers, switches, hubs, servers, encryption devices, and computer workstations). Individual workstations (clients) do not have to be shown; the number of clients is sufficient;
3. "For Official Use Only" markings; and
4. The agency name and date (day, month, and year) drawing was created or updated.

As IT security personnel you are required to sign a User Rules of Behavior Acknowledgment Form. (see appendix H)

Encryption:

1. Encryption shall be a minimum of 128 bit.
2. When CJI is transmitted outside the boundary of the physically secure location, the data shall be immediately protected via cryptographic mechanisms (encryption).

EXCEPTIONS: See Sections 5.5.7.3.2 and 5.10.2 of the CJIS Security Policy.

1.When CJI is at rest (i.e. stored electronically) outside the boundary of the physically secure location, the data shall be protected via cryptographic mechanisms (encryption).

a.When agencies implement encryption on CJI at rest, the passphrase used to unlock the cipher shall meet the following requirements:

I. Be at least 10 characters.
II. Not be a dictionary word.
III. Include at least one (1) upper case letter, one (1) lower case letter, one (1) number, and one (1) special character.
IV. Can't use the last 24 passwords in history
V. Be changed when previously authorized personnel no longer require access.

b.Multiple files maintained in the same unencrypted folder shall have separate and distinct passphrases. A single passphrase may be used to encrypt an entire folder or disk containing multiple files. All audit requirements found in Section 5.4.1 Auditable Events and Content (Information Systems) shall be applied.

2.When encryption is employed, the cryptographic module used shall be certified to meet FIPS 140-2 standards.

Note 1: Subsequent versions of approved cryptographic modules that are under current review for FIPS 140-2 compliancy can be used in the interim until certification is complete.

Note 2: While FIPS 197 (Advanced Encryption Standard) certification is desirable, a FIPS 197 certification alone is insufficient as the certification is for the algorithm only vs. the FIPS 140-2 standard which certifies the packaging of an implementation.

EXCEPTION: When encryption is used for CJI at rest, agencies may use encryption methods that are FIPS 197 certified, 256 bit as described on the National Security Agency (NSA) Suite B Cryptography list of approved algorithms.

3.For agencies using public key infrastructure technology, the agency shall develop and implement a certificate policy and certification practice statement for the issuance of public key certificates used in the information system. Registration to receive a public key certificate shall:

a. Include authorization by a supervisor or a responsible official.
b. Be accomplished by a secure process that verifies the identity of the certificate holder.
c. Ensure the certificate is issued to the intended party.

Incident Response

There has been an increase in the number of accidental or malicious computer attacks against both government and private agencies, regardless of whether the systems are high or low profile.

LASOs are the designated point of contact for security-related issues for their agency. LASOs are responsible for incident response reporting procedures at their agency as needed. (see appendix J) Each agency shall establish:

1. Information security reporting procedures outlining who to report to and how reporting happens through the agency chain of command upon discovery of any information security incident to CHRI; and

2. Incident handling capability procedures that includes adequate preparation, detection, and analysis, containment, eradication, recovery, and user response activities.

Agency AUDIT Preparation

An auditor with the SDDCI will be assigned to oversee the agency review process and is the POC between the SDDCI and the agency (LASO and NAC) during the current review cycle.

A notification letter along with a questionnaire will be mailed to the agency approximately 45- 60 days prior to the estimated on-site AUDIT. The agency should review, complete, and return the questionnaire to the SDDCI in a timely manner. The information provided from the completed questionnaire will assist the auditor in ascertaining the internal processes of the agency regarding the use, dissemination, maintenance, destruction, and security of the criminal history record information provided to the entity. Upon receipt of the questionnaire, the auditor reviews and contacts the agency POC to schedule an on-site AUDIT. It is important to note that any specific areas that an agency may wish to address during the AUDIT process should be conveyed to the auditor during this time. The auditor has the flexibility to alter the process at this point in order to address various CHRI-related concerns and/or questions from the agency.

Agency Administrative Interview (On-Site Visit)

During the administrative interview, the auditor will meet with the agency LASO and NAC and review the responses provided on the questionnaire. Generally, any concerns or points of interest that the auditor may need addressed will be covered during this time.

The following topics are discussed during the AUDIT:

1. Point of Contact
2. Use of criminal history information
   - Legal authority;
   - Fingerprint submission information;
3. Dissemination of criminal history record information
   - Outsourcing;
   - User Agreement, if applicable;
   - Waiver Agreement and Statement, if applicable.
4. Security of criminal history record information.
   - Physical security
   - Personnel (personnel having access to CHRI)
5. Maintenance of criminal history record information
6. Destruction process, if applicable, of criminal history records

Agency Criminal History Record Review

The auditor reviews a predetermined random number of CHRI received by an agency based on a statistical sampling method. The auditor will document each discrepancy found during the CHRI quality review, if any, using a standard record form.

Examples of error types include:

1. *Unauthorized* — CHRI should not have been requested and/or received — no Substantiating documentation as to employment or volunteer status, dissemination error, disseminated or shared with unauthorized entities.
2. *Unsecured* — CHRI filed or maintained in a non-secure location.
3. *Undocumented* — CHRI missing, dissemination log missing, waiver missing.

Agency Exit Briefing

The purpose of the exit briefing is to present a summary of findings to the agency at the conclusion of the AUDIT. The agency LASO and NAC or other designated agency representative must be present for the exit briefing. The summary will be an overview of the general findings of the review and should not be considered the official outcome of the AUDIT. Any communications between the agency LASO and NAC and auditor during the summary exit briefing will be well documented for inclusion into the official findings.

The official findings and recommendations will be compiled upon the auditor's return. Generally, the final AUDIT results will be mailed to the agency LASO and NAC within 30 days after the on-site visit. All discrepancies noted by the auditor, along with cumulative and discrepancy totals, will be included. The agency will have an opportunity to review the audit findings and either agree or disagree.

Each agency satisfying the state compliance standards will be scheduled for future AUDITs on a triennial basis.

If an agency has failed compliance standards, a follow up AUDIT will be conducted within 30 to 90 days of the initial AUDIT. The follow up AUDIT will include a new sampling of records and will generally address the previous areas of non-compliance.

AUDIT Survey Form

Along with the final report, the agency will receive an AUDIT survey form. The survey form provides the agency with the opportunity to rate the AUDIT process and provide any suggestions or comments.

The completion of the survey will assist the CJIS Division in accomplishing the following goals:

- Obtain information and/or opinions from the evaluated agency of the AUDIT process.
- Establish and maintain a line of communication between MSHP and non-criminal justice
- Entities/agencies regarding CHRI.
    - Identify areas in the AUDIT process that may need improvement.

NONCRIMINAL JUSTICE AGENCY USER AGREEMENT FOR RELEASE OF CRIMINAL HISTORY RECORD INFORMATION Between the SOUTH DAKOTA DIVISION OF CRIMINAL INVESTIGATION

Agency Name (Please Print or Type):

Agency Address:

City, State, Zip:

Point of Contact (POC) Name (Please Print or Type):

POC Title:

Telephone Number: FAX Number:

Email Address:

This agency hereinafter shall be known as "Authorized Recipient (AR)"
The AR's Originating Agency Identifier (ORI) and OCA, if applicable, is:

For SDDCI use

I.PURPOSE

This User Agreement is used to provide criminal history record information (CHRI) to authorized employers, licensing agencies, and other agencies requesting fingerprint-based criminal history record information.

Fingerprint-based criminal history record information must be explicitly mandated or allowed by law. National criminal history record information must be authorized by federal law or a state statute approved by the U.S. Attorney General. The applying AR is seeking background checks for:

Provide description of purpose to receive criminal history record information (include description of job and customers/clients served):

_____

_____

_____

_____

Enter law(s) requiring or allowing the receipt of criminal history record information, if known:

_____

II.THE PARTIES AGREE AS FOLLOWS

The SDDCI will:

1. Provide CHRI in response to fingerprint-based background checks, either to the AR or to the appropriate agency that reviews criminal history results for the AR pursuant to an approved Outsourcing Standard.
2. Provide assistance to the AR in interpreting CHRI.
3. Work to ensure the completeness and accuracy of the CHRI.
4. Conduct audits to assure compliance with this Agreement, state and federal laws and pursuant to the Federal Bureau of Investigation (FBI) CJIS Security Policy.
5. Cease providing information to the AR if this Agreement is violated or if the AR is
6. suspected of violating this Agreement.

The AR will:

1. Abide by the terms and conditions identified in this Agreement.
2. Comply with state and federal laws, rules, procedures, and policies, including those adopted by the state, the SDDCI, and the National Crime Prevention and Privacy Compact (42 U.S.C. 14611-16) regarding the receipt, use and dissemination of CHRI.
3. Use CHRI only for the purpose for which it was requested.
4. Provide for the security of any CHRI received. This includes, but is not limited to:
    a. Designate a security officer who is responsible for ensuring compliance with security procedures and this User Agreement.
    b. Ensure that all personnel with access to CHRI are aware of the rules and responsibilities with regard to CHRI, pursuant to the most current version of the CJIS Security Policy.
    c. Restrict access to physical or electronic copies of CHRI to authorized personnel. Physical copies shall be maintained in a controlled, secure environment such as a locked cabinet in a room not accessible to all staff and visitors. Electronic copies shall be protected with at least 128-bit encryption or individually password protected. The relevant federal encryption standard is FIPS 140-2.
    d. Restrict dissemination of criminal history record information unless explicitly allowed by law and log all authorized dissemination. Logs shall

include, at a minimum, the date, the name of sending agency, name of receiving agency or applicant, record shared, means of dissemination, and name of person who disseminated.

e. Track and report information security incidents such as the theft/loss of physical records or the penetration of electronic systems.
f. Dispose of records securely. Physical media should be cross-shredded at aminimum, and electronic records should be deleted and repeatedly over-written with random 0s and 1s.

5. Understand that this data is based on CHRI received at the state repository and through the systems of the FBI. If a person could be adversely affected by this data, the person must be given the opportunity to challenge and correct a record. Challenge and/or appeal procedures are referenced in SDCL Ch. 23-5, Ch. 23-6 and Title 28, Code of Federal Regulations (CFR) 16.30-34.
6. Retain audit records for at least three (3) years or until AR has received a favorable compliance rating from a SDDCI Policy Compliance Review. Once the minimum retention time period has passed, the AR shall continue to retain audit records until they are no longer needed for administrative, legal, audit, or other operational purposes such as Freedom of Information Act requests or legal actions.
7. Allow the SDDCI to conduct audits to assure compliance with this Agreement.
8. Pay all fees for criminal history record information provided by the SDDCI and FBI in accordance with SDCL Ch. 23-5, Ch. 23-6 and Title 28 Code of Federal Regulations (CFR) 20.31(e)(3).

III.CRIMINAL HISTORY RECORD INFORMATION LIMITATIONS

The AR understands the CHRI has the following limitations:

1. CHRI is defined and has three parts as follows:
   a. The arresting agency's name and crime class under which the person was arrested. The arrest data submitted includes the mandatory field of name, race, sex, and date of birth. All arrests are accompanied by fingerprints.
   b. The charge(s) issued by the prosecutor.
   c. The name of the court that tried the case and the ultimate disposition of the case.

2. CHRI and custody information is compiled from information submitted to the SDDCI. from law enforcement agencies, prosecutors, courts, Department of Mental Health and Department of Corrections (hereinafter referred to as contributing agencies). Although the SDDCI makes reasonable efforts to ensure all information is submitted as required by law, it is not responsible for omissions from contributing agencies.
3. Before releasing information on individuals or taking adverse action against an individual listed on the CHRI, the person in question must be afforded the opportunity to dispute and correct the record.

4. CHRI is constantly being updated as new arrests and other information are entered into the system by contributing agencies. The record released is only valid as of the date the criminal history record check was performed.
5. Certain statutes allow for the suppression or deletion of records, and this information is not provided.
6. The SDDCI retains records for State of South Dakota only. Most fingerprinting reasons include a check through the FBI, which the SDDCI will request on the AR's behalf as a normal part of the criminal history record check, if allowed by law.

This Agreement commences on the date the last signature is obtained below and continues until terminated by either party. This Agreement may be terminated sooner by one or both parties upon 30-days written notice or immediately upon violation of the terms of the Agreement.

Compliance with this Agreement is voluntary; however, failure to complete this Agreement may result in denial of request.

NONCRIMINAL JUSTICE AGENCY

_____

Signature of Agency Representative Date

_____

Print or Type Name

SOUTH DAKOTA DIVISION OF CRIMINAL INVESTIGATION

_____

Signature of Director, South Dakota Division of Criminal Investigation Date
Bryan Gortmaker, Director

_____

Print or Type Name

Submit completed Agreement via United States mail or Fax as follows:
ATTENTION: Jami Oakland
SOUTH DAKOTA DIVISION OF CRIMINAL INVESTIGATION
1302 E HWY 14, STE 5
PIERRE SD 57501

Office: (605) 773-4614
FAX: (605) 773-2235

Noncriminal Agency Coordinator (NAC)

The NAC is expected to be the primary liaison between the agency and SDDCI (SD Division of Criminal Investigation).

Send Completed Hard-Copy
Form To:

South Dakota Division of Criminal Investigation
Attn: Jami Oakland
1302 E Hwy 14, Ste. 5
Pierre SD 57501
Phone: 605-773-4614
Fax: 605-773-2235
Email: jami.oakland@state.sd.us

I.NAC Information

Appointed NAC (First Name, Last Name, and M.I.)

Agency Name Agency ORI

Agency Address City State Zip Code

Work Phone Number Fax Number

Email Address Agency Director Name (First Name, Last Name, and M.I.)

Has this person received CJIS Training? Yes No

II. Approval – I further agree to submit a new designation form to SDDCI at any time there is a change in the above name NAC.

Signature of Agency Director Date

For Additional Information please visit:
www.fbi.gov/about-us/cjis/cjis-security-policyresource-center/view for FBI CJIS SECURITY POLICY

Questions / Comments:
Phone: (605) 773-4614

ORI/_____

Designation Of
Local Agency Security Officer
(LASO)

I hereby designate _____ to serve as Local Agency Security Officer (LASO) for the _____.

I understand that a LASO is expected to be the primary point of Information Security contact between my department and SDDCI, to actively represent my department in all matters pertaining to Information Security, to disseminate Information Security alerts and other material to my department, to be available for basic and refresher training conducted by SDDCI, to maintain Information Security documentation (including system configuration data), to assist with Information Security audits of hardware and procedures, and to keep SDDCI informed as to specific agency Information Security needs and problems.

I further agree to submit a new designee from to SDDCI any time there is a change in LASO assignments.

_____

Chief Official

_____

Agency

_____

Date

State and Federal Regulations Regarding the Use Of Criminal History Record Information (CHRI)

The non-criminal justice use of criminal history record information AUDIT is based on the following federal guidelines, where applicable:

• Title 5, United States Code (U.S.C.), Section 552, the Freedom of Information Act, requires the records to be accurate, complete, timely, and relevant.

• Title 28, U.S.C., Section 534, authorizes dissemination of CHRI, and provides that access to CHRI is subject to cancellation if dissemination is made outside of the authorized recipient.

• Title 5, U.S.C., Section 552a, the Privacy Act, requires that agencies maintain a system of records which establish appropriate administrative, technical, and physical safeguards to ensure the security and confidentiality of records.

• Title 42, U.S.C., Chapter 140, Subchapter II, Section 14616, the National Crime Prevention and Privacy Compact (Compact), established the Compact Council, which is authorized to establish rules, procedures, and standards for the use of Interstate Identification Index (III) for non-criminal justice purposes. Determining compliance includes, but is not limited to, assessing participation requirements, the continual maintenance, and the security of CHRI.

• Title 28, Code of Federal Regulations (CFR), 20.30, cites the administration of criminal justice shall include criminal identification activities, and the collection, storage, and dissemination of CHRI.

• Title 28, CFR, 20.33 (a) (2), authorizes the dissemination of CHRI contained in the III to federal agencies authorized to receive it pursuant to federal statute or Executive Order (E.O.)

• Title 28, CFR, 20.33 (a)(3), authorizes the dissemination of CHRI contained in the III for use in connection with licensing or employment, pursuant to Public Law (Pub.L.) 92-544, 86 Stat. 1115, or other federal legislation, and for other uses for which dissemination is authorized by federal law.

• Title 28, CFR, 20.33(d), cites that criminal history records received from the III System or the FIRS shall be used only for the purpose requested and a current record should be requested when needed for a subsequent authorized use.

• Title 28, CFR, 50.12 (b), references the exchange of FBI identification records obtained under this authority may be used solely for the purpose requested and cannot be disseminated outside the receiving departments, related agencies, or other authorized entities.

• Title 28, CFR, 50.12 (b), references that officials at the governmental institutions and other entities authorized to submit fingerprints and receive FBI identification records under this authority must notify the individuals fingerprinted that the fingerprints will be used to check the criminal history records of the FBI.

• Title 28, CFR, 50.12 (b), references that the officials making the determination of suitability for licensing or employment shall provide the applicants the opportunity to complete, or challenge the accuracy of, the information contained in the FBI identification record. These officials also must advise the applicants that procedures for obtaining a change, correction, or updating of a Policy Compliance Review Reference Manual 17 FBI identification record are set forth in Title 28, CFR, 16.34. Officials making such determinations should not deny the license or employment based on information in the record until the applicant has been afforded a reasonable time to correct or complete the record, or has declined to do so.

• Title 28, CFR, Part 906, Outsourcing of Non-criminal Justice Administrative Functions, amends the dissemination restrictions of 28 CFR 50.12 (b), by permitting the outsourcing of non-criminal justice criminal history record checks to either another governmental agency or a private Vendor acting as an agent for the authorized receiving agency. Published as a final rule on December 15, 2005, this rule also established the standards, entitled the Security and Management Control Outsourcing Standard (Outsourcing Standard), that must be followed for an agency to outsource these functions.

• Title 28, CFR, Part 906, the Outsourcing Standard, requires Vendors to maintain a security program consistent with federal and state laws, regulations, and standards, as well as, rules, procedures, and standards established by the Compact Council and the United States Attorney General. The Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship, so that the security and integrity of the III System and criminal history information are not compromised. The security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

• Title 28, CFR, Section 16.34, if, after reviewing his/her identification record, the subject thereof believes that it is incorrect or incomplete in any respect and wishes changes, corrections, or updating of the alleged deficiency, he/she should make application directly to the agency which contributed the questioned information. The subject of a record may also direct his/her challenge as to the accuracy or completeness of any entry on his/her record to the FBI, Criminal Justice Information Services (CJIS) Division, ATTN: SCU, Mod. D-2, 1000 Custer Hollow Road, Clarksburg, WV 26306. The FBI will forward the challenge to the agency which submitted the data requesting that agency to verify or correct the challenged entry. Upon the receipt of an official communication directly from the agency which contributed the original information, the FBI CJIS Division will make any changes necessary in accordance with the information supplied by that agency.

• Title 42, U.S.C., Section 14611-14616, Congress finds that -- (1) both the Federal Bureau of Investigation and state criminal history record repositories maintain fingerprint-based criminal history records; (2) these criminal history records are shared and exchanged for criminal justice purposes through a federal-state program known as the Interstate Identification Index System; (3) although these records also are exchanged for legally authorized, noncriminal justice uses, such as governmental licensing and employment background checks, the purposes for and procedures by which they are exchanged vary widely from state to state; (4) an interstate and federal-state compact is necessary to facilitate authorized interstate criminal history record exchanges for noncriminal justice purposes on a uniform basis, while permitting each state to effectuate its own dissemination policy within its own borders; and (5) such a compact will allow federal and state records to be provided expeditiously to governmental and nongovernmental agencies that use such records in accordance with pertinent federal and state law, while simultaneously enhancing the accuracy of the records and safeguarding the information contained therein from unauthorized disclosure or use.

Pursuant to Public Law (Pub.L.) 92-544, the FBI is empowered to exchange identification records with officials of state and local governments for purposes of licensing and employment if authorized by a state statute which has been approved by the Attorney General of the United States.

The Attorney General's approval authority is delegated to the FBI by Title 28, CFR, Section 0.85(j).

The standards employed by the FBI in approving Pub. L. 92-544 purposes have been established by a series of memoranda issued by the Department of Justice (DOJ), Office of the General Counsel (OGC), Access Integrity Unit (AIU). The standards are:

• The authorization must exist as the result of legislative enactment or its functional equivalent;
• The authorization must require fingerprinting of the applicant;
• The authorization must, expressly or by implication, authorize use of FBI records for screening of the applicant;
• The authorization must not be against public policy; and,
• The authorization must not be overly broad in its scope and must identify the specific category of applicants and/or licensees.
Additionally,
• The fingerprint submission must be channeled through the State Identification Bureau (SIB) for forwarding to the FBI (South Dakota Division of Criminal Investigation);

• The states must designate a governmental agency to be responsible for receiving and screening the results of the record check to determine an applicant's suitability for employment and/or licensing;

• The results of the record check cannot be released outside the receiving governmental

department or related governmental agency; and,

• Processing fees are either by direct payment or billed to the SIB (South Dakota Division of Criminal Investigation) depending on arrangements made between the FBI and the SIB, such as the execution of a Memorandum of Understanding (MOU) for billing.

Policy Compliance Review Reference Manual 19
Emergency III Name-based Background Checks Approved By The Compact Counsel (Non-User Fee)

• Officials of state or local governmental with a child-placement statute approved under Pub. L. 92-544 and officials of a federal law enforcement agency for a federal agency responsible for the placement of children to conduct background checks on the temporary custodian with whom a child is being placed and all adults residing in the home of the custodian. (The III name-based checks must be followed by non-criminal justice user-fee fingerprint submissions within a time frame specified by the Compact Council.) [Pub. L. 92-544; Title 28, U.S.C., Section 534, Note; the Compact, Title 42, U.S.C., Section 14611-14616; Title 28, CFR, Part 901]

• Officials of the DHS, Federal Emergency Management Agency (FEMA) to conduct pre-employment background checks on emergency workers hired by FEMA to assist in recovery efforts as a result of national disasters or other catastrophic emergencies. (The III name-based checks must be followed by non-criminal justice user-fee fingerprint submissions within a time frame specified by the Compact Council.) [Title 28, U.S.C., Section 534; E.O. 10450; The Compact, Title 42, U.S.C., Section 14611-14616; Title 28, CFR, Part 901] Privacy Statement The responsibility of notification (authority to collect and potential use of the information) lies with the agency collecting the fingerprints. Civil information is often collected on FBI applicant cards (FD-258), which are provided to authorized agencies in support of federal criminal history checks. The FD-258 fingerprint card is generally used for civil purposes, and the Privacy Act statement on the back of the card has been updated (June 2, 2010) as follows: Authority: The FBI's acquisition, preservation, and exchange of information requested by this form is generally authorized under 28 U.S.C. 534. Depending on the nature of your application, supplemental authorities include numerous federal statutes, hundreds of state statutes pursuant to Pub.L. 92-544, presidential executive orders, regulations, and/or orders of the attorney general of the United States, or other authorized authorities. Examples include, but are not limited to: 5 U.S.C. 9101; Pub.L. 94-29; Pub.L. 101-604; and Executive Orders 10450 and 12968. Providing the requested information is voluntary; however, failure to furnish the information may affect timely completion or approval of your application.

Social Security Account Number (SSAN): Your SSAN is needed to keep records accurate, because other people may have the same name and birth date. Pursuant to the Federal Privacy Act of 1974 (5 USC 552a), the requesting agency is responsible for informing you whether disclosure is mandatory or voluntary, by what statutory or other

authority your SSAN is solicited, and what uses will be made of it. Executive Order 9397 also asks federal agencies to use this number to help identify individuals in agency records. 20 Policy Compliance Review Reference Manual Principal Purpose: Certain determinations, such as employment, security, licensing, and adoption, may be predicated on fingerprint-based checks. Your fingerprints and other information contained on (and along with) this form may be submitted to the requesting agency, the agency conducting the application investigation, and/or the FBI for the purpose of comparing the submitted information to available records in order to identify other information that may be pertinent to the application. During the processing of this application, and for as long hereafter as may be relevant to the activity for which this application is being submitted, the FBI may disclose any potentially pertinent information to the requesting agency and/or to the agency conducting the investigation.

The FBI may also retain the submitted information in the FBI's permanent collection of fingerprints and related information, where it will be subject to comparisons against other submissions received by the FBI. Depending on the nature of your application, the requesting agency and/or the agency conducting the application investigation also may retain the fingerprints and other submitted information for other authorized purposes of such agency (ies). Routine Uses: The fingerprints and information reported on this form may be disclosed pursuant to your consent, and also may be disclosed by the FBI without your consent as permitted by the Federal Privacy Act of 1974 (5 USC 552a (b)) and all applicable routine uses as may be published at any time in the Federal Register, including the routine uses for the FBI Fingerprint Identification Records System (Justice/FBI-009) and the FBI's Blanket Routine Uses (Justice/FBI-BRU). Routine uses include, but are not limited to, disclosures to: appropriate governmental authorities responsible for civil or criminal law enforcement, counterintelligence, national security, or public safety matters to which the information may be relevant; to state and local governmental agencies and nongovernmental entities for application processing as authorized by federal and state legislation, executive order, or regulation, including employment, security, licensing, and adoption checks; and as otherwise authorized by law, treaty, executive order, regulation, or other lawful authority.

If other agencies are involved in processing this application, they may have additional routine uses. Additional Information: The requesting agency and/or the agency conducting the application investigation will provide you additional information pertinent to the specific circumstances of this application, which may include identification of other authorities, purposes, uses, and consequences of not providing requested information. In addition, any such agency in the federal executive branch also has published notice in the Federal Register describing any system(s) of records in which that agency may also maintain your records, including the authorities, purposes, and routine uses for the system(s).

SECONDARY DISSEMINATION LOG

Requirement

As set forth in the Criminal Justice Information Services (CJIS) Security Policy, Secondary Dissemination Section 5.1.3, a Noncriminal Justice Agency (NCJA) releasing Criminal History Record Information (CHRI) to another agency that was not part of the original information exchange, then the sending NCJA is required to log and maintain such transactions. A "log" is to consist of the following fields: Date Shared, Disseminated Record, Requesting Agency (whom the response was shared with), Method of Sharing, and Agency Personnel that shared the CHRI.

Purpose

The purpose of this document is to provide your agency with a sample tool in order to meet the federal requirement. Your agency is in no way obligated to use the Secondary Dissemination Log.

Instructions

The Secondary Dissemination Log is provided. All fields listed in this log are compliant with the secondary dissemination requirement. This log is to be used in any instance where CHRI is being shared with another agency outside the original request and this log should be maintained indefinitely. A NCJA may individually create documents to "log" such dissemination. However, they are to meet the same required fields, whether physically or electronically maintained.

Disseminated Record: Enter the TCN or full name assigned to the individual CHRI record that is to be disseminated.

Date Shared: The date the CHRI is actually provided to the other agency.

Requesting Agency: The name of the qualified agency that is receiving the CHRI.

Recipient Name: The name of the authorized recipient for the Requesting Agency.

Method of Sharing: The method used to exchange the CHRI (e.g. e-mail, fax, U.S. Postal Service, etc.) *Note: Any requested CHRI record that is a "hit" record, meaning a record was found, then the agency can only disseminate the found, or hit record, by U.S. Postal Service.*

Agency Personnel (Operator) that shared the CHRI: The name or initials of the individual within your agency that actually forwarded the CHRI record with the other qualified entity.

NCJA means – A governmental agency authorized by federal statute, executive order, or state statute and approved by the U.S. Attorney General to be able to receive state and federal fingerprint based CHRI, directly or indirectly from the South Dakota Division of Criminal Investigation (SDDCI). Examples of services include, but are not limited to, employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD

The goal of this document is to provide adequate security and integrity for criminal history record information (CHRI) while under the control or management of an outsourced third party, the Contractor. Adequate security is defined in Office of Management and Budget Circular A-130 as "security commensurate with the risk and magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."

The intent of this Security and Management Control Outsourcing Standard (Outsourcing Standard) is to require that the Contractor maintain a security program consistent with federal and state laws, regulations, and standards (including the FBI Criminal Justice Information Services (CJIS) Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

This Outsourcing Standard identifies the duties and responsibilities with respect to adequate internal controls within the contractual relationship so that the security and integrity of the Interstate Identification Index (III) System and CHRI are not compromised. The standard security program shall include consideration of site security, dissemination restrictions, personnel security, system security, and data security.

The provisions of this Outsourcing Standard are established by the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. They apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI with a direct connection to the FBI CJIS Wide Area Network (WAN).

1.0 **Definitions**

1.01 Access to CHRI means to view or make use of CHRI obtained from the III System but excludes direct access to the III System by computer terminal or other automated means by Contractors other than those that may be contracted by the FBI or state criminal history record repositories or as provided by title 42, United States Code, section 14614(b).

1.02 Authorized Recipient means (1) a nongovernmental entity authorized by federal statute or federal executive order to receive CHRI for noncriminal 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 noncriminal justice purposes.

1.03 Authorized Recipient's Information Security Officer means the individual who shall ensure technical compliance with all applicable elements of this Outsourcing Standard.

1.04 Chief Administrator means the primary administrator of a Nonparty State's criminal history record repository or a designee of such administrator who is a regular full-time employee of the repository, which is also referred to as the State Identification Bureau (SIB) Chief.

1.05 CHRI, as referred to in Article I (4) of the Compact, means information collected by criminal justice agencies on individuals consisting of identifiable descriptions and notations of arrests, detentions, indictments, or other formal criminal charges, and any disposition arising therefrom, including acquittal, sentencing, correctional supervision, or release; but does not include identification information such as fingerprint records if such information does not indicate involvement of the individual with the criminal justice system.

1.06 Criminal History Record Check, for purposes of this Outsourcing Standard only, means an authorized noncriminal justice fingerprint-based search of a state criminal history record repository and/or the FBI system.

1.07 CJIS Systems Agency, as provided in Section 1.4 of the FBI Criminal Justice Information Services (CJIS) Division's Advisory Policy Board Bylaws, means a criminal justice agency which has overall responsibility for the administration and usage of CJIS Division Programs within a state, district, territory, or foreign country. This includes any federal agency that meets the definition and provides services to other federal agencies and/or whose users reside in multiple states or territories.

1.08 CJIS Systems Officer, as provided in Section 1.5 of the CJIS Advisory Policy Board Bylaws, means the individual employed by the CJIS Systems Agency who is responsible for monitoring system use, enforcing system discipline and security, and assuring that CJIS operating procedures are followed by all users as well as other related duties outlined by the user agreements with the FBI's CJIS Division. (This title was formerly referred to as the Control Terminal Officer or the Federal Service Coordinator).

1.09 Compact Officer, as provided in Article I (2) of the Compact, means (A) with respect to the Federal Government, an official [FBI Compact Officer] so designated by the Director of the FBI [to administer and enforce the compact among federal agencies], or (B) with respect to a Party State, the chief administrator of the State's criminal history record repository or a designee of the chief administrator who is a regular full-time employee of the repository.

1.10 Contractor means a government agency, a private business, non-profit organization or individual, that is not itself an Authorized Recipient with respect to the particular noncriminal justice purpose, who has entered into a contract with an Authorized Recipient to perform channeler functions requiring access to CHRI. Under this Outsourcing Standard, a Contractor serves as a Channeler and has direct connectivity to the CJIS Wide Area Network (WAN) for the purpose of electronic submission of fingerprints to and the receipt of CHRI from the FBI on behalf of an Authorized Recipient.

1.11 Contractor's Security Officer means the individual accountable for the management of the Contractor's security program.

1.12 Dissemination means the disclosure of III CHRI by an Authorized Recipient to an authorized Contractor, or by the Contractor to another Authorized Recipient consistent with the Contractor's responsibilities and with limitations imposed by federal and state laws, regulations, and standards as well as rules, procedures, and standards established by the Compact Council and the United States Attorney General.

1.13 Noncriminal Justice Administrative Functions means the routine noncriminal justice administrative functions relating to the processing of CHRI, to include but not limited to the following

a. Making fitness determinations/recommendations
b. Obtaining missing dispositions
c. Disseminating CHRI as authorized by Federal statute, Federal Executive Order, or State statute approved by the United States Attorney General
d. Other authorized activities relating to the general handling, use, and storage of CHRI

1.14 Noncriminal Justice Purposes, as provided in Article I (18) of the Compact, means uses of criminal history records for purposes authorized by federal or state law other than purposes relating to criminal justice activities, including employment suitability, licensing determinations, immigration and naturalization matters, and national security clearances.

1.15 Outsourcing Standard means a document approved by the Compact Council after consultation with the United States Attorney General which is to be incorporated by reference into a contract between an Authorized Recipient and a Contractor. This Outsourcing Standard authorizes access to CHRI for noncriminal justice purposes, limits the use of the information to the purposes for which it is provided, prohibits retention and/or dissemination except as specifically authorized, ensures the security and confidentiality of the information, provides for audits and sanctions, provides conditions for termination of the contract, and contains such other provisions as the

Compact Council may require.
1.16 Physically Secure Location means 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 CHRI and associated information systems.

1.17 Positive Identification, as provided in Article I (20) of the Compact, means a determination, based upon a comparison of fingerprints1 or other equally reliable biometric identification techniques, that the subject of a record search is the same person as the subject of a criminal history record or records indexed in the III System. Identifications based solely upon a comparison of subjects' names or other non-unique identification characteristics or numbers, or combinations thereof shall not constitute positive identification.

1.18 Public Carrier Network means a telecommunications infrastructure consisting of network components that are not owned, operated, and managed solely by the agency using that network, i.e., any telecommunications infrastructure which supports public users other than those of the agency using that network. Examples of a public carrier network include but are not limited to the following: Dial-up and Internet connections, network connections to Verizon, network connections to AT&T, ATM Frame Relay clouds, wireless networks, wireless links, and cellular telephones. A public carrier network provides network services to the public; not just to the single agency using that network.

1.19 Security Violation means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in violation of: (A) Federal or state law, regulation, or Executive Order; or (B) a rule, procedure, or standard established by the Compact Council and the United States Attorney General.

2.0 **Responsibilities of the Authorized Recipient**

2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions, the Authorized Recipient shall: (a) Request and receive written permission from the State Compact Officer. The Compact Council currently defines positive identification for noncriminal justice purposes as identification based upon a qualifying ten-rolled or qualifying ten-flat fingerprint submission. Further information concerning positive identification may be obtained from the FBI Compact Council office.

2.02The Compact Officer/Chief Administrator may not grant such permission unless he/she has implemented a combined state/federal audit program to, at a minimum, triennially audit a representative sample of the Contractors and Authorized Recipients engaging in outsourcing with the first of such audits to be conducted within one year of the date the Contractor first receives CHRI under the approved outsourcing agreement. A representative sample will be based on generally accepted statistical sampling methods.

User Rules of Behavior Acknowledgment Form

As a user of an IT system, I acknowledge my responsibility to conform to the following requirements and conditions as directed by all relevant Information Assurance and Information Security Policies, Procedures and Guidelines. These conditions apply to all personnel who have access to FBI CJIS systems and all appropriate IT personnel.

1. I understand that failure to sign this acknowledgment will result in denial of access to FBI
CJIS systems, terminal areas, and facilities that have FBI CJIS network equipment.

2. I acknowledge my responsibility to use the network only for official business except for
such personal use involving negligible cost to the agency and no interference with official business as may be permissible under the acceptable use policy.

3. I understand that the network operates at a Sensitive but Unclassified level. I have all clearance necessary for access to the network, and will not introduce or process data that the network is not specifically designed to handle as specified by the Security Policy.

4. I understand the need to protect my password at the highest level of data it secures. I will NOT share my password and/or account. I understand that neither the Security Administrator/System Administrator, nor the Network Operations Center (NOC) will request my password. I will change my password at least every 90 days or as requested for security reasons.

5. I understand I am responsible for all actions taken under my account. I will not attempt to "hack" the network or any connected automated information system (AIS), or attempt to gain access to data for which I am not specifically authorized.

6. I understand my responsibility to appropriately protect all output generated under my account, to include printed material, magnetic tapes, floppy disks, CD-ROMs, and downloaded hard disk files. I understand that I am required to ensure all hard copy material and magnetic media is properly labeled as required by policies and regulations.

7. I understand my responsibility to report all AIS or network problems to my security point of contact. I will NOT install, remove, or modify any hardware or software.

8. I acknowledge my responsibility to not introduce any software or hardware not acquired and approved through the IT Security group. I also acknowledge my responsibility to have all official electronic media virus-scanned by the IT Security group before introducing it into the AIS or network.
9. I acknowledge my responsibility to conform to the requirements of the Rules of Behavior, Acceptable Use Policy, and Security Policies and Procedures. I also acknowledge that failure to comply with these policies and procedures may constitute a security violation resulting in denial of access to the AIS, network, or facilities, and that such violations will be reported to appropriate authorities for further actions as deemed appropriate to include disciplinary, civil, or criminal penalties.

10. I agree that I have no expectation of privacy in any equipment or media I use. I consent to inspections by authorized agency personnel, at any time and agree to make any equipment available for audit and review by FBI personnel upon request.

11. I further consent that my use of FBI CJIS systems within agency owned or leased space is subject to system monitoring.

12. I have completed the required triennial Security Awareness Training required by the CJIS Security Policy for individuals managing or accessing FBI CJIS systems and/or data.

_____ _____

User (Print Name): Date:

_____ _____

User Signature: Date:

_____ _____

ISO/Security Officer: Date:

DISCIPLINARY POLICY

In support of SD Division of Criminal Investigation's mission of public service to the city of/county of [city or county name] citizens, the SD Division of Criminal Investigation' provides the needed technological resources needed to personnel to access FBI CJIS systems and information in support of the agency's mission. All agency personnel, with access to FBI Criminal Justice Information (CJI) or any system with stored FBI CJI, have a duty to protect the system and related systems from physical and environmental damage and are responsible for correct use, operation, care and maintenance of the information. All technology equipment: computers, laptops, software, copiers, printers, terminals, MDTs, mobile devices, live scan devices, fingerprint scanners, software to include RMS/CAD, operating systems, etc., used to process, store, and/or transmit FBI CJIS is a privilege allowed by SD Division of Criminal Investigation state CSO, and the FBI. To maintain the integrity and security of the SD Division of Criminal Investigation's and FBI's CJIS systems and data, this computer use privilege requires adherence of relevant federal, state and local laws, regulations and contractual obligations. All existing laws and SD Division of Criminal Investigation regulations and policies apply, including not only those laws and regulations that are specific to computers and networks, but also those that may apply to personal conduct.

Misuse of computing, networking or information resources may result in temporary or permanent restriction of computing privileges up to employment termination. In some misuse situations, account privileges will be suspended to prevent ongoing misuse while under investigation. Additionally, misuse can be prosecuted under applicable statutes. All files are subject for search. Where follow-up actions against a person or agency after an information security incident involves legal action (either civil or criminal), the evidence shall be collected, retained, and presented to conform to the rules for evidence laid down in the relevant jurisdiction(s). Complaints alleging misuse of SD Division of Criminal Investigation's computing and network resources and FBI CJIS systems and/or data will be directed to those responsible for taking appropriate disciplinary action.

Examples of Misuse with access to FBI CJI

1. Using someone else's login that you are not the owner.
2. Leaving computer logged in with your login credentials unlocked in a physically unsecure location allowing anyone to access SD Division of Criminal Investigation systems and/or FBI CJIS systems and data in your name.
3. Allowing unauthorized person to access FBI CJI at any time for any reason. Note: Unauthorized use of the FBI CJIS systems is prohibited and may be subject to criminal and/or civil penalties.

4. Allowing remote access of SD Division of Criminal Investigation issued computer equipment to FBI CJIS systems and/or data without prior authorization by SD Division of Criminal Investigation.
5. Obtaining a computer account that you are not authorized to use.
6. Obtaining a password for a computer account of another account owner.
7. Using the SD Division of Criminal Investigation's network to gain unauthorized access to FBI CJI.
8. Knowingly performing an act which will interfere with the normal operation of FBI CJIS systems.
9. Knowingly propagating a computer virus, Trojan horse, worm and malware to circumvent data protection or compromising existing security holes to FBI CJIS systems.
10. Violating terms of software and / or operating system licensing agreements or copyright laws.
11. Duplication of licensed software, except for backup and archival purposes that circumvent copyright laws for use in SD Division of Criminal Investigation, for home use or for any customer or contractor.
12. Deliberately wasting computing resources to include streaming audio, videos for personal use that interferes with SD Division of Criminal Investigation network performance.
13. Using electronic mail or instant messaging to harass others.
14. Masking the identity of an account or machine.
15. Posting materials publicly that violate existing laws or SD Division of Criminal Investigation's codes of conduct.
16. Attempting to monitor or tamper with another user's electronic mail or files by reading, copying, changing, or deleting without explicit agreement of the owner.
17. Using SD Division of Criminal Investigation's technology resources to advance unwelcome solicitation of a personal or sexual relationship while on duty or through the use of official capacity.
18. Unauthorized possession of, loss of, or damage to SD Division of Criminal Investigation's technology equipment with access to FBI CJI through unreasonable carelessness or maliciousness.
19. Maintaining FBI CJI or duplicate copies of official SD Division of Criminal Investigation files in either manual or electronic formats at his or her place of residence or in other physically non-secure locations without express permission.
20. Using SD Division of Criminal Investigation's technology resources and/or FBI CJIS systems for personal or financial gain.
21. Deliberately failing to report promptly any known technology-related misuse by another employee that may result in criminal prosecution or discipline under this policy.
22. Using personally owned devices on SD Division of Criminal Investigation's network to include personally-owned thumb drives, CDs, mobile devices, tablets on wifi, etc. Personally owned devices should not store SD Division of Criminal Investigation data, State data, or FBI CJI.

The above listing is not all-inclusive and any suspected technology resource or FBI CJIS system or FBI CJI misuse will be handled by Agency Name on a case by case basis. Activities will not be considered misuse when authorized by appropriate Agency Name officials for security or performance testing.

Privacy Policy

All agency personnel utilizing agency-issued technology resources funded by SD Division of Criminal Investigation expressly acknowledges and agrees that such service, whether for business or personal use, shall remove any expectation of privacy. Use of SD Division of Criminal Investigation systems indicates consent to monitoring and recording. The SD Division of Criminal Investigation reserves the right to access and audit any and all communications including electronic and physical media at rest, in transit and at end of life. SD Division of Criminal Investigation personnel shall not store personal information with an expectation of personal privacy that are under the control and management of SD Division of Criminal Investigation.

Personal Use of Agency Technology

The computers, electronic media and services provided by SD Division of Criminal Investigation are primarily for business use to assist personnel in the performance of their jobs. Limited, occasional, or incidental use of electronic media (sending or receiving) for personal, non-business purposes is understandable and acceptable, and all such use should be done in a manner that does not negatively affect the systems' use for their business purposes. However, employees are expected to demonstrate a sense of responsibility and not abuse this privilege.

Misuse Notification

Due to the increase in the number of accidental or malicious computer attacks against both government and private agencies, SD Division of Criminal Investigation shall: (i) establish an operational incident handling capability for all information systems with access to FBI CJIS systems and data. This includes adequate preparation, detection, analysis, containment, recovery, and user response activities; (ii) track, document, and report incidents to appropriate agency officials and/or authorities.

ISOs have been identified as the POC on security-related issues for their respective agencies and shall ensure LASOs institute the CSA incident response reporting procedures at the local level.

All SD Division of Criminal Investigation personnel are responsible to report misuse of SD Division of Criminal Investigation technology resources to appropriate SD Division of Criminal Investigation officials.

Local contact-LASO: firstnamelast@agencyname.com Phone:
State contact-CSA ISO: jami.oakland@state.sd.us Phone: 605-773-4614

I have read the policy and rules above and I will abide in the SD Division of Criminal Investigation's Disciplinary policy.

Signature: _____

Date: _____/20____

ACKNOWLEDGEMENT STATEMENT OF MISUSE

All Authorized Personnel are made aware of the guidelines, consequences and liabilities that could occur from unauthorized use of criminal justice information and criminal history record information. Employees are advised of the following:

- Give a criminal history record information (CHRI) to someone who is not authorized to receive it.
- Allowing unauthorized access to criminal history record information (CHRI).
- Using criminal history record information (CHRI) for any other purpose other than stated in the South Dakota statute.
- Access to criminal justice information (CJI) and criminal history record information (CHRI) via submitted fingerprints could be suspended or cancelled for violation of security and/or violation of the terms and conditions in the User Agreement.
- Misuse of the CHRI is a misdemeanor or felony depending on the circumstances of the release
- *Penalties for Misuse of CHRI*

I acknowledge that I have been advised of the consequences of misuse of criminal justice and criminal history record information.

_____

Employee Name (Print)

_____ _____

Employee Signatures Date

SD DIVISION OF CRIMINAL INVESTIGATION
INFORMATION SECURITY OFFICER (ISO)

SECURITY INCIDENT REPORTING FORM

NAME OF PERSON REPORTING THE INCIDENT: _____

DATE OF REPORT: _____ (mm/dd/yyyy)

DATE OF INCIDENT: _____ (mm/dd/yyyy)

POINT(S) OF CONTACT (Include Phone/Extension/Email): _____

LOCATION(S) OF INCIDENT:

_____

_____

INCIDENT DESCRIPTION:

_____

_____

_____

SYSTEM(S) AFFECTED:

_____

_____

SYSTEM(S) AFFECTED (e.g. CAD, RMS, file server, etc.):

_____

_____

METHOD OF DETECTION:

_____

ACTIONS TAKEN/RESOLUTION:

_____

_____

_____

Copies To:

Jami Oakland
SD Division of Criminal Investigation
1304 E Hwy 14, Ste 5
Pierre SD 57501

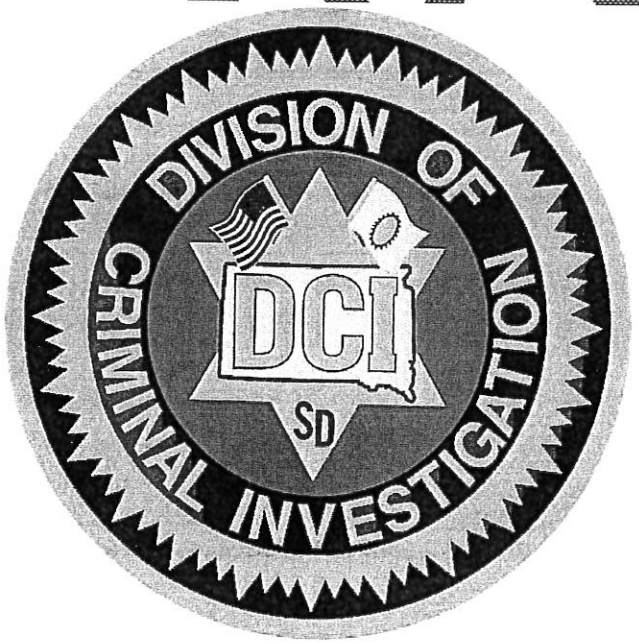
Noncriminal Justice Agency

(NCJA)

Information Technology

Security Audit

Correspondence Questionnaire



Agency Contact Information

Please complete the following, where applicable only.

Audit Information:

Agency Name/Department Name: _____

ORI/Unique Identifier: _____

Name of Agency Head: _____ Title: _____

Mailing Address: _____

Primary Point of Contact (POC):

Name: _____ Title: _____

Street Address: _____ City: _____ State: _____ Zip: _____

Phone: _____ Alt. Phone: _____ Email: _____

Local Agency Security Officer (LASO) (technical POC, if applicable):

Name: _____ Title: _____

Street Address: _____ City: _____ State: _____ Zip: _____

Phone: _____ Alt. Phone: _____ Email: _____

Physical Address (main address where CHRI/CJI is accessed):

Contact Name: _____ Title: _____

Street Address: _____ City: _____ State: _____ Zip: _____

Phone: _____ Alt. Phone: _____ Email: _____

Data Center (if different from physical address):

Contact Name: _____ Title: _____

Street Address: _____ City: _____ State: _____ Zip: _____

Phone: _____ Alt. Phone: _____ Email: _____

Offsite Media Storage (where media containing CJI is stored outside of the agency):

Contact Name: _____ Title: _____

Street Address: _____ City: _____ State: _____ Zip: _____

Phone: _____ Alt. Phone: _____ Email: _____

Back-up Recovery Site (disaster recovery site/where system back-ups are stored):

Contact Name: _____ Title: _____

Street Address: _____ City: _____ State: _____ Zip: _____

Phone: _____ Alt. Phone: _____ Email: _____

AUTHORIZED USE/ACCESS TO CRIMINAL JUSTICE INFORMATION

*****Please note criminal history record information (CHRI) is a subset of criminal justice information (CJI) and are interchangeable for the purposes of this document.*****

1. Under what authority does the agency have access to national CHRI/CJI?

   - ☐ State statute: _____
   - ☐ NCPA/VCA
   - ☐ Adam Walsh Act
   - ☐ HUD (Housing and Urban Development) / PHA (Public Housing Authority)
   - ☐ Real ID Act
   - ☐ Other: _____

2. Does the agency have access to CHRI/CJI by means other than fingerprint submission?
   ☐ YES ☐ NO ☐ N/A

3. Describe the process for the submission of civil fingerprint transactions to include method of submission to the state Repository.

   _____
   _____
   _____
   _____
   _____

4. How does the agency receive or retrieve the national CHRI response from the state Repository?

   - ☐ mail (hard copy)
   - ☐ fax
   - ☐ email
   - ☐ website
   - ☐ livescan device
   - ☐ other: _____

RETENTION OF CRIMINAL JUSTICE INFORMATION

1. Does the agency retain the results (hard copies or electronic) of the criminal history record check or documents containing CHRI/CJI?
   ☐ YES ☐ NO ☐ N/A

   - ☐ hard copy (case files, filing cabinet, etc.)
   - ☐ e-mail (kept on email server/archive)
   - ☐ scanned/saved to network share (more than one person can access)
   - ☐ Excel spreadsheet (yes/no indicators kept, etc.)
   - ☐ scanned/saved to desktop (not on network file share)
   - ☐ website/internet application (records management system/personnel database, etc.)
   - ☐ other: _____

2. Is the CHRI/CJI commingled (kept in same location) with any other records (such as in a personnel file with tax information, etc.)? ☐ YES ☐ NO ☐ N/A

DISSEMINATION OF CRIMINAL JUSTICE INFORMATION

1. Does the agency disseminate CHRI/CJI results to the individual of record or applicant? ☐ YES ☐ NO ☐ N/A

   a. How is the information disseminated?

   - ☐ mail (hard copy)
   - ☐ courier service
   - ☐ hand carried by authorized personnel
   - ☐ email
   - ☐ website/internet
   - ☐ verbal (face to face or by phone)
   - ☐ fax
   - ☐ other: _____

2. Does the agency disseminate CHRI/CJI to any other entity/individual? ☐ YES ☐ NO ☐ N/A

   a. Who?

   - ☐ private contractors (for outsourcing – additional questions below)
   - ☐ another similar agency (e.g. one school to another school)
   - ☐ grant funded positions (give results to grant provider)
   - ☐ accreditations (providing CHRI to accreditation company for review/proof)
   - ☐ licensing
   - ☐ audit (other than FBI/State Repository)
   - ☐ other: _____
   - ☐ other: _____

   b. How is the CHRI/CJI shared?

   - ☐ mail (hard copy)
   - ☐ courier service
   - ☐ hand carried by authorized personnel
   - ☐ email
   - ☐ website/internet
   - ☐ Verbal (face to face or by phone)
   - ☐ fax
   - ☐ other: _____

   c. What information is sent?

   _____

   _____

d. Why is the information sent/for what purposes would you disclose the results?

_____

_____

_____

3. How is the information protected during dissemination?

- ☐ encryption (if via email, accessed via an internet website or application)
- ☐ tamper-proof container (sealed envelope, locked container, etc.)
- ☐ hand carried by authorized personnel
- ☐ certified mail
- ☐ other: _____

a. If CHRI/CJI is sent via email or accessed from an internet based application or website, please describe methods (bit level such as 128, hardware/software, etc.) of encryption and the National Institute of Standards and Technology (NIST) Federal Information Processing Standard (FIPS) 140-2 certification number.

_____

_____

_____

b. Does the agency protect the information using a passphrase (to unlock encryption)? Please describe.

_____

_____

_____

ADMINISTRATION OF NONCRIMINAL JUSTICE ADMINISTRATIVE FUNCTIONS

PRIVATE CONTRACTORS

1. Does the agency outsource (use private contractor personnel/vendors) for any noncriminal justice administrative functions that provides private contractor personnel with access to CHRI/CJI?

☐ YES ☐ NO ☐ N/A

a. If **YES**, what noncriminal justice administrative functions are private contractors performing?

- ☐ data destruction (paper shredding, hard drives, etc.)
- ☐ IT services (network/system administrations, desktop support, etc.)
- ☐ off-site media storage (data centers, backup, paper storage archives, etc.)
- ☐ dispositions (obtains additional information from court of jurisdiction)
- ☐ hiring decisions (mails offer letters, generates security badges/credentials, etc.)
- ☐ scanning services (scans results into database or electronic file)
- ☐ other: _____

b. Has the agency obtained state/repository level approval for private contractor access to CHRI/CJI?

☐ YES ☐ NO ☐ N/A

c. Has the agency designated someone as an Agency Coordinator to ensure all private contractor personnel have completed a fingerprint based record check (if applicable), completed the appropriate level security awareness training, and abide by all policies within the CJIS Security Policy? ☐ YES ☐ NO ☐ N/A

d. Does the agency have a contract/agreement with the private contractor(s), which incorporates or references the CJIS Security Policy and Outsourcing Standard? ☐ YES ☐ NO ☐ N/A

PERSONNEL SECURITY

1. Has the state passed legislation authorizing or requesting civil fingerprint-based record checks for personnel with access to CHRI/CJI for the purposes other than the administration of criminal justice functions *(e.g., licensing and employment)*? ☐ YES ☐ NO ☐ N/A

   a. If **YES**, has the agency ensured all personnel with unescorted access to CHRI/CJI have completed a state and national fingerprint-based record check within 30 days of access to CHRI/CJI? *(should include agency personnel, IT staff, private contractors, cleaning/maintenance personnel with physical access to secure locations)* ☐ YES ☐ NO ☐ N/A

SECURITY AWARENESS TRAINING

1. Does the agency ensure all personnel with unescorted access to CHRI/CJI have completed security awareness training within 6 months of assignments and at least every two years after? *(should include agency personnel, IT staff, private contractors, cleaning/maintenance personnel with physical access to information)* ☐ YES ☐ NO ☐ N/A

   a. If **YES**, is documentation of individual security awareness training maintained in a current status, to include private contractors if applicable? ☐ YES ☐ NO ☐ N/A

   b. Is the agency using the state provided training curriculum? (If **NO**, please provide training materials for review) ☐ YES ☐ NO ☐ N/A

SECURITY INCIDENTS AND VIOLATIONS

1. Does the agency provide and enforce the CJIS Security Policy to all authorized users, to include private contractor personnel? ☐ YES ☐ NO ☐ N/A

2. Does the agency have a written policy for the discipline of CJIS policy violators? ☐ YES ☐ NO ☐ N/A

3. What are the procedures when a security violation or incident is detected?

   _____

   _____

   _____

   a. Does the agency report the security violation or incident to anyone? Who? ☐ YES ☐ NO ☐ N/A

      _____

      _____

      _____

b. Are all employees and/or private contractors made aware of the reporting procedures? ☐ YES ☐ NO ☐ N/A

c. Are the procedures described above written in agency policy? ☐ YES ☐ NO ☐ N/A

4. Has the agency reported/had any security violations or incidents in the last 3 years? (incidents in which security of CHRI/CJI was compromised or put at risk) ☐ YES ☐ NO ☐ N/A

_____

_____

_____

_____

INFORMATION PROTECTION

*****Please note, if the agency does not retain criminal history record information or criminal justice information, the following sections are not applicable. Please skip each section that is not applicable and complete the signature block on the last page of this questionnaire before returning as indicated.*****

FOR HARD COPY STORAGE AND ACCESSIBILITY

The following questions apply to noncriminal justice agencies retaining all or part of the national criminal history record in paper (hard copy) form.

1. Describe all locations where and how criminal history record information is retained. (e.g. locked file cabinet, locked office, off-site storage facility, records archive, etc.)

_____

_____

_____

_____

2. Is the storage location physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, within a locked file with limited access, in a locked office, in a safe, etc.) ☐ YES ☐ NO ☐ N/A

   a. Does the agency house files that contain CHRI/CJI in an off-site record storage facility? ☐ YES ☐ NO ☐ N/A

   b. Who owns/manages the facility? (i.e. who controls access)

   _____

   c. How are records transported to the off-site facility?

   _____

   d. How are the records stored at the off-site facility?

   _____

3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) ☐ YES ☐ NO ☐ N/A

4. Are visitors escorted by authorized personnel in physically secure locations at all times (in all access and storage areas to include off-site facilities if designated physically secure)? ☐ YES ☐ NO ☐ N/A

5. How does the agency dispose of physical (hard copy/paper) media containing CHRI/CJI?

_____
_____
_____
_____

   a. Does the agency have written procedures for paper destruction? ☐ YES ☐ NO ☐ N/A

   b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel? ☐ YES ☐ NO ☐ N/A

FOR SINGLE DESKTOP STORAGE AND ACCESSIBILITY

The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record on a single computer (desktop, laptop, tablet, etc.) that is not part of a larger shared network. (i.e. one user/one desktop)

1. What information is kept? (i.e. scanned copies, excel spreadsheet with CHRI/CJI indicators, word documents with descriptors, email account, etc.)

_____
_____
_____
_____

2. Describe the physical location where the computer with access to CHRI/CJI is housed. (e.g., locked office, reception area, etc.)

_____
_____
_____
_____

   a. Is the computer's location physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, computer is not left unattended, visitors are escorted while in area, etc.) ☐ YES ☐ NO ☐ N/A

   b. Is the CHRI/CJI encrypted at rest? ☐ YES ☐ NO ☐ N/A

   c. If encryption is used, please describe methods (bit level, hardware/software, etc.) of encryption. (e.g. Adobe Pro, WinZip, TrueCrypt, etc.)

_____
_____
_____

d. Does the agency protect the information using a passphrase (to unlock encryption)? Please describe.

_____

_____

_____

3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) ☐ YES ☐ NO ☐ N/A

4. When a computer reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

_____

_____

_____

_____

a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)? ☐ YES ☐ NO ☐ N/A

b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel? ☐ YES ☐ NO ☐ N/A

5. When logging onto the computer or before accessing CHRI/CJI does the user enter a password that utilizes secure password attributes? (at least 8 characters, numbers/letters, expires every 90 days, cannot reuse 10 previous passwords, and does not display when entered) ☐ YES ☐ NO ☐ N/A

6. Do users ever share their usernames, password, or passphrase (if applicable)? ☐ YES ☐ NO ☐ N/A

7. Does the computer initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity? ☐ YES ☐ NO ☐ N/A

a. If a user leaves the computer, do they log out of the computer or lock the screen? ☐ YES ☐ NO ☐ N/A

8. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, virus protection patches, etc.) ☐ YES ☐ NO ☐ N/A

9. Does the computer storing CHRI/CJI have access to the internet? ☐ YES ☐ NO ☐ N/A

a. If **YES**, describe the boundary protection used to protect the computer. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

_____

_____

b. Does the agency enable virus protection at start-up and employ automatic scanning and updates? Please describe. ☐ YES ☐ NO ☐ N/A

_____

10. Does someone within the agency stay up to date with relevant security alerts and advisories?
☐ YES ☐ NO ☐ N/A

FOR SHARED NETWORK STORAGE AND ACCESSIBILITY

The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record on a shared closed-network platform (not accessible from internet webpage).

1. What information is kept? (i.e. scanned copies, excel spreadsheet with CHRI/CJI indicators, word documents with descriptors, emails, etc.)

2. Identify all locations where CHRI/CJI is either maintained (stored) or can be accessed (e.g., servers, offsite backups, primary offices, secondary locations, third party cloud storage, etc.)

   a. Are all locations where CHRI/CJI is either maintained/stored or accessed considered physically secured? (i.e. unauthorized personnel cannot access CHRI/CJI, computer is not left unattended, visitors are escorted while in area, etc.)
   ☐ YES ☐ NO ☐ N/A

   b. Describe physical security measures. (i.e. key card access, locked doors, etc.)

   c. Is the CHRI/CJI encrypted at rest?
   ☐ YES ☐ NO ☐ N/A

   d. Is the CHRI/CJI encrypted in transit? (accessed from secondary location, emailed, remotely accessed)
   ☐ YES ☐ NO ☐ N/A

   e. If encryption is used, please describe methods (bit level, hardware/software, etc.) of encryption. (e.g. Adobe Pro, WinZip, TrueCrypt, etc.)

   f. Does the agency protect the information using a passphrase (to unlock encryption)? Please describe.
   ☐ YES ☐ NO ☐ N/A

3. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) ☐ YES ☐ NO ☐ N/A

4. Is the CHRI/CJI backed up to off-site storage or a disaster recovery location? ☐ YES ☐ NO ☐ N/A

   a. Who owns/manages the facility? (i.e. who controls access)

   _____

   b. How are backup records transported to the secondary facility? (i.e. disc to disc with encryption or physical tapes encrypted or in locked box, etc.)

   _____

   c. How are the records stored at the off-site facility?

   _____

5. When a computer reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

   _____
   _____
   _____
   _____

   a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)? ☐ YES ☐ NO ☐ N/A

   b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel? ☐ YES ☐ NO ☐ N/A

6. Before logging into the computer or before accessing CHRI/CJI, does the agency display a system use notification, a warning to the user that they are accessing sensitive information and informing of the possible consequences for misuse? ☐ YES ☐ NO ☐ N/A

7. When logging onto the computer or before accessing CHRI/CJI does the user enter a password that utilizes secure password attributes? (at least 8 characters, numbers/letters, expires every 90 days, cannot reuse 10 previous passwords, and does not display when entered) ☐ YES ☐ NO ☐ N/A

8. Do users ever share their usernames, passwords, or passphrase (if applicable)? ☐ YES ☐ NO ☐ N/A

9. Describe the agency's process for issuing user accounts, deleting/disabling user accounts, and periodic validation of user accounts:

   _____
   _____
   _____
   _____

   a. Are these procedures written? ☐ YES ☐ NO ☐ N/A

10. Does the information system initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity? ☐ YES ☐ NO ☐ N/A

    a. If a user leaves the computer, do they log out of the computer or lock the screen? ☐ YES ☐ NO ☐ N/A

11. Does the information system log: ☐ YES ☐ NO ☐ N/A

    - ☐ successful and unsuccessful log on attempts
    - ☐ successful and unsuccessful password changes
    - ☐ successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.)
    - ☐ successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.)

    a. Does each logged event include: date, time, component (where it occurred), type of event, user, outcome (success or failure)? ☐ YES ☐ NO ☐ N/A

    b. Does the agency check logs (who accessed CHRI/CJI, logged in, etc.) at least weekly? ☐ YES ☐ NO ☐ N/A

    c. How long are logs kept?

    _____

12. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, firewall patches, etc.) ☐ YES ☐ NO ☐ N/A

13. Describe the boundary protection used to protect the network. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

    _____

    _____

    _____

    a. Is CHRI/CJI separated from non-CHRI/CJI related access? (i.e. can unauthorized users access shared folder or location of CHRI/CJI or is it separated in some way, such as a VLAN?) Please describe. ☐ YES ☐ NO ☐ N/A

    _____

    _____

    _____

14. Does the agency utilize intrusion detection (IDS) or intrusion protection (IPS) tools? ☐ YES ☐ NO ☐ N/A

    _____

15. Can users access CHRI/CJI remotely? (i.e., access network from outside physically secure location, etc.) Please describe. (i.e. method/application, encryption used, etc.) Include details. (e.g., Citrix, VPN, GoToMyPC, LogMeIn, TeamViewer, etc.) ☐ YES ☐ NO ☐ N/A

    _____

    _____

    _____

16. Does the agency enable virus protection at start-up and employ automatic scanning and updates on all computers and servers storing or accessing CHRI/CJI? Please describe. (i.e. type and version)
☐ YES ☐ NO ☐ N/A

_____

17. Does someone within the agency stay up to date with relevant security alerts and advisories?
☐ YES ☐ NO ☐ N/A

18. Does the agency host any CHRI/CJI in a virtualized environment? ☐ YES ☐ NO ☐ N/A

    a. Please describe how CHRI information is protected in a virtual environment. (i.e. how is CHRI protected from unauthorized access – partitions, separate virtual NICs, different hosts from non-CHRI related systems or internet facing applications, etc.?)

_____
_____
_____
_____

FOR RECORD MANAGEMENT SYSTEMS/DATABASE STORAGE AND INTERNET ACCESSABILITY

The following questions apply to noncriminal justice agencies retaining all or part of the criminal history record in a records management system or database that is accessible through the internet.

1. What information is kept? (i.e. scanned copies, entered descriptor data, etc.)

_____
_____
_____
_____

2. What is the name of the application/website/database housing CHRI/CJI? (i.e. HR database, etc.)

_____

3. Identify all locations where criminal history information/CJI is maintained/stored. (e.g., application/web servers, database storage, offsite backups, primary offices, secondary locations, third party cloud storage, etc.)

_____
_____
_____
_____

    a. Are all locations where CHRI is either maintained/stored considered physically secured? (i.e. unauthorized personnel cannot access CHRI, computer is not left unattended, visitors are escorted while in area, etc.)
☐ YES ☐ NO ☐ N/A

    b. Describe physical security measures. (i.e. key card access, locked doors, etc.)

_____
_____
_____

c. Is the CHRI or CJI encrypted at rest? ☐ YES ☐ NO ☐ N/A

d. If encryption is used for data at rest, please describe methods (bit level, hardware/software, etc.) of encryption.

_____

_____

_____

4. Does the agency have a written policy that describes physical protections? (i.e. how and where the information/equipment must be stored, who can access, restricts unauthorized access, requires visitors to be escorted, etc.) ☐ YES ☐ NO ☐ N/A

5. Is the CHRI/CJI backed up to off-site storage or a disaster recovery location? ☐ YES ☐ NO ☐ N/A

a. Who owns/manages the facility? (i.e. who controls access)

_____

b. How are backup records transported to the secondary facility? (i.e. disc to disc with encryption or physical tapes encrypted or in locked box, etc.)

_____

c. How are the records stored at the off-site facility?

_____

6. When a computer/server, etc. reaches end of life (no longer works) or is to be replaced/upgraded, how does the agency destroy the hard drive?

_____

_____

_____

_____

a. Does the agency have written procedures for the sanitization and/or destruction of electronic media (hard drive, thumb drive, CDs, etc.)? ☐ YES ☐ NO ☐ N/A

b. If the agency personnel does not conduct the sanitization or destruction of the media and it is performed by another entity, is the process witnessed by authorized personnel? ☐ YES ☐ NO ☐ N/A

7. Before logging into the application or website to access CHRI/CJI, does the agency display a system use notification, a warning to the user that they are accessing sensitive information and informing of the possible consequences for misuse? ☐ YES ☐ NO ☐ N/A

8. When logging onto the application or website and accessing CHRI/CJI does the user and/or administrator enter a password that utilizes secure password attributes that includes all of the following characteristics? ☐ YES ☐ NO ☐ N/A

   - ☐ length must be at least eight characters
   - ☐ must contain letters and numbers or special characters
   - ☐ not be the same as the user ID
   - ☐ expire within a maximum of 90 days
   - ☐ not allow the reuse of the last 10 passwords
   - ☐ not display when entered

9. Do users or IT administrators ever share their usernames or passwords or have generic group accounts? ☐ YES ☐ NO ☐ N/A

10. Describe the agency's process for issuing user accounts, deleting/disabling user accounts, and periodic validation of user accounts:

    _____
    _____
    _____
    _____

    a. Are these procedures written? ☐ YES ☐ NO ☐ N/A

11. Does the information system or application initiate a session lock (require the user to re-enter password) after a maximum of 30 minutes of inactivity? ☐ YES ☐ NO ☐ N/A

    a. If a user leaves the computer, do they log out of the computer or lock the screen? ☐ YES ☐ NO ☐ N/A

12. Are the following events logged: ☐ YES ☐ NO ☐ N/A

    - ☐ successful and unsuccessful log on attempts
    - ☐ successful and unsuccessful password changes
    - ☐ successful and unsuccessful actions by privileged accounts (adding users, deleting users, etc.)
    - ☐ successful and unsuccessful actions related to CHRI (delete records, edits of information, access to the record, etc.)

    a. Does each logged event include: date, time, component (where it occurred), type of event, user, outcome (success or failure)? ☐ YES ☐ NO ☐ N/A

    b. If a security incident happened in relation to the release or misuse of CHRI/CJI, could you identify the individual who carried out the action and when? ☐ YES ☐ NO ☐ N/A

    c. Does the agency check logs (who accessed CHRI/CJI, logged in, etc.) at least weekly? ☐ YES ☐ NO ☐ N/A

    d. How long are logs kept?

    _____

13. Does the agency apply routine patches and updates to all software and components? (i.e. Windows updates, firewall patches, etc.) ☐ YES ☐ NO ☐ N/A

14. Describe the boundary protection used to protect the network. (i.e., hardware/software firewalls, proxies, gateways, guards, routers, etc.)

    a. Is CHRI/CJI separated from non-CHRI/CJI related access? (i.e. can unauthorized users access application or locations of CHRI/CJI or is it separated in some way, such as a VLAN?) Please describe. ☐ YES ☐ NO ☐ N/A

15. Does the agency utilize intrusion detection (IDS) or intrusion protection (IPS) tools? ☐ YES ☐ NO ☐ N/A

16. How is CHRI/CJI encrypted when transmitted outside the physically secure location where it is stored? (i.e., how is the data encrypted when a user is accessing from an internet connection, etc.) Include details. (e.g., methods of encryption, bit level, hardware/software/application, FIPS certificate numbers, etc.)

17. Does the agency enable virus protection at start-up and employ automatic scanning and updates on all computers and servers storing or accessing CHRI/CJI? Please describe. (i.e. type and version) ☐ YES ☐ NO ☐ N/A

18. Does someone within the agency stay up to date with relevant security alerts and advisories? ☐ YES ☐ NO ☐ N/A

19. Does the agency host any CHRI/CJI in a virtualized environment? ☐ YES ☐ NO ☐ N/A

    a. Please describe how CHRI information is protected in a virtual environment. (i.e. how is CHRI protected from unauthorized access – partitions, separate virtual NICs, different hosts from non-CHRI related systems or internet facing applications, etc.)

Before returning this audit, please complete the following information:

Questionnaire Completed By (signed name): _____

Questionnaire Completed By (print name): _____

Phone Number: _____ Date Completed: _____

E-mail address: _____

After completed, please attach all supporting documentation and send to the following:

Attention: _____

Phone: _____ Fax: _____

Email: _____

Mailing Address: Street: _____

City: _____ State: _____ Zip: _____

********* **FOR OFFICIAL USE ONLY*********

Auditor Review

Auditor Name: _____ Date of Review: _____

Comments/Documents Provided/Notes: _____

Secondary Reviewer: _____ Date of Review: _____

Additional Comments: _____

Non-Criminal Justice Agency User Guide Questions and Answers

1. **Why am I receiving this?**

    a. All agencies who receive Finger print based FBI background checks from DCI are required to complete the User Agreement. (pages 17-20)

2. **Is my agency being audited?**

    a. No, the enclosed Sample audit is what will be sent to your agency when DCI schedules an on-site audit. Per the FBI recommendation we will be using a more in depth audit. DCI sent the sample so your agency will know what will be expected to filled out at the time of your audit.

    b. Your agency will be audited at some point over the next 3 years.

3. **Will my agency need training? (pages 9-10)**

    a. Yes – anyone who has access to the FBI background results will be required to take an online training. DCI is requiring email addresses of the individuals who will have access to the FBI results. DCI will then email a link to those individuals to complete the CJIS security training.

4. **Why do I need to take security training? (pages 9-10)**

    a. Per FBI regulations anyone who has access to the FBI result is required to complete the CJIS security training.

5. **What is a LASO? (page 21)**

    a. Local Agency Security officer, this can be anyone in your agency that will be the responsible party for documenting and notifying DCI if there is any misconduct or misuse of the FBI criminal history result.

6. **What is a NAC? (page 22)**

    a. The Non-Criminal Agency Coordinator, this can be anyone in your agency who will be the contact person or liaison between your agency and DCI.

    b. This individual will receive the pre-audit packet prior to the on-site audit.

7. **What is a Secondary Dissemination Log? (page 7)**

    a. School Districts are allowed (if they chose) to share FBI results with another school district. The FBI and DCI are requiring those agencies to keep a secondary dissemination log for auditing purposes.

8. **What is Outsourcing? (pages 10-11 and pages 30-33)**

    a. Examples of outsourcing are: (also see page 33; 1.18 for more examples)

        i. Hiring an agency to shred FBI results

        ii. Any outside IT support agencies (if you keep FBI result electronically)

    b. All outsourcing entities need prior approval from DCI

9. **Who needs to sign the Rules of Behavior Acknowledgment form?)page 34-35)**

    a. Anyone who has access to the FBI background information received from DCI is required to complete this form (you may need to make copies depending how many individuals have access to the Criminal history).

        i. Examples:

            1. Secretary opens the mail, passes it on to the Superintendent and the then it is given to the Business Manager.

                a. In this case all three individuals will need to complete a Behavior Acknowledgment form.

10. **Who needs to read and sign the Disciplinary policy and rules? (pages. 36-39)**

    a. Anyone who has access to the FBI background information received from DCI is required to complete this form (you may need to make copies depending how many individuals have access to the Criminal history).

        i. Examples:

            1. Secretary opens the mail, passes it on to the Superintendent and the then it is given to the Business Manager.

                a. In this case all three individuals will need to complete a Disciplinary form.

11. Who needs to read and complete the Acknowledgment statement of Misuse?

a. Anyone who has access to the FBI background information received from DCI is required to complete this form (you may need to make copies depending how many individuals have access to the Criminal history).

i. Examples:

1. Secretary opens the mail, passes it on to the Superintendent and the then it is given to the Business Manager.

a. In this case all three individuals will need to complete an Acknowledgment of Misuse form.

12. What is the Security Incident Reporting Form on page 41?

a. This form is what the LASO would complete and send to DCI if there has been misuse of the criminal history.

13. What forms do I need to complete and return to DCI?

a. Agency User Agreement (pages 17-20)

b. Noncriminal Agency Coordinator (page 21)

c. Local Agency Security Officer (page 22)

d. User Rules of Behavior Acknowledgment Form (pages 34-35)

i. You may need to make additional copies

e. Disciplinary Policy (pages 36-39)

i. You may need to make additional copies

Thank you,

Jami Oakland – 605-773-4614

Jami.oakland@state.sd.us