Consent Agenda
Juvenile Services

Jefferson County
Board of County Commissioners

Agenda Request

To:	Board of County Commissioners
From:	Barbara L. Carr, Juvenile Court Administrator
Date:	Week of November 12, 2013
Subject:	**Interagency Agreement** Memorandum of Understanding WSP and Juvenile Court Contract #C130725GSC

Statement of Issue:
This MOU authorizes our relationship with the Washington State Patrol to provide background checks on all our volunteer guardian ad litem (CASA's) pursuant to statute. Historically, the Sheriff's Office performed these duties, but the WSP has assumed responsibility for all these checks and have set forth substantial requirements for participating programs.

Analysis:
Pursuant to RCW 13.34.100, a criminal background check is required annually of all volunteer GAL's. This includes a WSP and FBI background check, which is available to us through the attached MOU. This document is the Washington State Patrol's first step in formalizing this process. I will be meeting with WSP staff to discuss issues such as appropriate dissemination and sharing of such records (which is extremely limited).

Alternatives:
None – statutorily required.

Fiscal Impact:
This will ultimately have some fiscal impact on my budget but at this point I am not sure to what degree. These costs will be tracked this year and if of consequence, will be included in my budget separately for 2015.

Recommendation:
That the Board approves the agreement and sign 3 originals. A fully executed original will be returned to the BOCC office upon final execution by AOC.

11/6/13

Reviewed by:
Philip Morley, County Administrator

MEMORANDUM OF UNDERSTANDING

Between the

WASHINGTON STATE PATROL

And the

JEFFERSON COUNTY
JUVENILE AND FAMILY COURT

I. PURPOSE

The parties to this Memorandum of Understanding (MOU) are the Washington State Patrol, Identification and Criminal History Section (WSP) and the Jefferson County Juvenile and Family Court, a non criminal justice agency (NCJA). This MOU sets forth the policy to ensure the protection of criminal history record information (CHRI) between the WSP, the NCJA, and the Federal Bureau of Investigation (FBI). This MOU provides guidance for the creation, viewing, modification, transmission, dissemination, storage, and destruction of CHRI data. This policy applies to the NCJA and its contractors with access to, or who operate in support of, non-criminal justice services and information.

II. ADMINISTRATIVE RESPONSIBILITIES

As participants in this MOU, the parties will develop mutually and separately appropriate procedures for transmission, dissemination, storage, and destruction of CHRI data.

a. The Washington State Patrol. WSP shall ensure the NCJA complies with the Criminal Justice Information Services (CJIS) Security Policy (See Exhibit B) which includes authorized use of CHRI, dissemination of CHRI, statute authorization for civil applicant background checks conducted by noncriminal justice agencies, applicant notification and record challenge, security of CHRI, storage of CHRI, outsourcing of noncriminal justice administrative functions, and user fees. WSP will conduct regional audits of all agencies working under this MOU to ensure compliance to all state and federal standards.

b. NCJA. The NCJA shall be responsible for ensuring:

1. NCJA responds to requests for information by the FBI CJIS Division or the WSP in the form of questionnaires, surveys, or similar methods, to the maximum extent possible, consistent with any fiscal, time, or personnel constraints of the agency.
2. NCJA has formalized written procedures for the following, if applicable: criminal history use and dissemination, misuse, background checks, password management, storage, and destruction of CHRI.
3. CHRI received as a result of licensing or employment purposes, pursuant to Public Law 92-544 is solely used for the purpose for which the record was requested. Subject fingerprints shall be submitted with all requests for CHRI for noncriminal justice purposes. Access to the FBI CJIS using name-based inquiry and record request messages is not permitted for noncriminal justice purpose, unless otherwise approved by the FBI.
4. Access to CHRI by authorized officials is subject to cancellation if dissemination is made outside the receiving departments, related agencies, or other authorized entities.

5. All fingerprint based applicant submissions must include in the reason fingerprinted field an accurate representation of the purpose and/or authority for which the CHRI is to be used.
6. NCJA must notify the applicants fingerprinted that the fingerprints will be used to check the criminal history records of the FBI. 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 an FBI identification record are set forth in Title 28, C.F.R. 16.34. Official 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.
7. Appropriate administrative, technical, and physical safeguards to insure the security and confidentiality of records and to protect against any anticipated threats or hazards to their security or integrity.
8. NCJA shall seek WSP permission prior to outsourcing noncriminal justice functions.
9. Outsourcing of noncriminal justice administrative functions requiring access to CHRI to either another governmental agency or a private contractor acting as an agent for the authorized receiving agency complies with the security and management control outsourcing standard for non-channelers (see Exhibit A).
10. NCJA is responsible for compliance to technical standards set forth by WSP and the CJIS Security Policy.
11. NCJA will conduct periodic self audits to ensure compliance with CJIS Security Policy.
12. NCJA will participate in WSP and FBI audits, provide plans for any compliance issues, and follow through to resolution within identified timeframes.
13. NCJA will ensure all appropriate staff members are trained according to the state and federal requirements.

III. CRIMINAL HISTORY RECORD INFORMATION RESPONSBILITIES

NCJA shall conform to system policies, as established by the FBI CJIS Division and WSP, before access to CHRI is permitted. This will allow for control over the data and give assurance of system security.

1. The rules and procedures governing access to CHRI shall apply equally to all participants in the system.
2. All noncriminal justice agencies with access to CHRI data must designate a specific unit, position, or personnel to access CHRI; noncriminal justice agencies must advise WSP of such personnel and changes to such designation.
3. All noncriminal justice agencies with access to CHRI data from the system shall permit an FBI CJIS Division or WSP audit team to conduct appropriate audits. NCJA must cooperate with these audits and respond promptly.

IV. SECURITY RESPONSIBILITIES

Technical Roles and Responsibilities

NCJA must comply with and enforce system security. NCJA must have someone designated as the security point of contact (POC). Security POC's shall be responsible for the following:

1. Identifying the user of the hardware/software and ensuring that no unauthorized users have access to the same.
2. Identifying and documenting how the equipment is connected to the state system.

3. Ensuring that personnel security screening procedures are being followed as stated in the CJIS Security Policy.
4. Ensuring that appropriate hardware security measures are in place.
5. Supporting policy compliance and keeping the WSP informed of security incidents.
6. If the technical POC changes at your agency, notify WSP immediately.

Security Enforcement
NCJA is responsible for enforcing system security standards for their agency, in addition to all of the other agencies to which the NCJA provides CHRI information. Authorized users shall access and disseminate the CHRI data only for the purpose for which they are authorized. NCJA shall have a written policy for the discipline of policy violators.

Technical Security Training
All Information Technology (IT) employees who have access to and those who have direct responsibility to configure and maintain FBI CJIS systems must review security awareness training within six months of their appointment or assignment. Documentation pertaining to the materials used and those employees which receive security awareness training shall be maintained in a current status.

Physical Security
A physically secured location in a noncriminal justice facility, an area, a room, a group of rooms, that is/are subject to criminal justice agency management control security addendum and which contain hardware, software, and/or firmware (e.g., information system servers, controlled interface equipment, associated peripherals or communications equipment, wire closets, patch panels, etc.) that provide access to the CJIS sensitive facilities and restricted/controlled areas shall be prominently posted and separated from non-sensitive facilities and non-restricted/controlled areas by physical barriers that restrict unauthorized access.

All personnel with access to computer centers, CHRI, or areas where CHRI information is housed shall either be escorted by authorized personnel at all times or receive a fingerprint-based background check. All personnel must review security awareness training within six months of their appointment or assignment.

Personnel Security
To verify identification, state of residency and national fingerprint-based record checks shall be conducted within 30 days of initial employment or assignment for all personnel who have authorized access to FBI CJIS information and those who have direct responsibility to configure and maintain computer systems and networks with access to FBI CJIS information. All requests from system access shall be made as specified by the CJIS Systems Officer (i.e. WSP Identification and Criminal History Section).

c. NCJA shall use the data supplied by WSP and the FBI under this MOU only for the authorized purpose intended. NCJA shall not use this data for any other purpose and shall not disseminate this data with any other parties unless required by law. NCJA shall share any public disclosure requests regarding this data with the WSP.

Storage
Please see 'Security and Management Control Outsourcing Standard for Non-Channelers' (Exhibit A).

V. LIAISON REPRESENTATIVES

For the Washington State Patrol:

Jim Anderson, Administrator
Criminal Records Division
PO Box 42619
Olympia WA 98504-2619
Phone: (360) 534-2101
Fax:(360) 534-2070
E-mail: jim.anderson@wsp.wa.gov

For the Jefferson County Juvenile and Family Court:

Barbara Carr
PO Box 120
Port Townsend WA 98368
360-385-9190
bcarr@co.jefferson.wa.us

VI. INDEMNIFICATION

Each party shall defend, protect and hold harmless the other party from and against all claims, suits and/or actions arising from any negligent or intentional act or omission of that party's employees, agents, and/or authorized subcontractor(s) while performing this MOU.

VII. PERIOD OF MOU

This MOU becomes effective on the date of the last signature and continues for three years and may be renewed. It may be modified by mutual written consent of the two agencies. Liaison Representatives may modify Exhibit A by mutual written consent of the two agencies without changing the general conditions of this MOU.

VIII. TERMINATION

Except as otherwise provided in this MOU, either party may terminate this MOU upon ninety (90) days' written notification to the other party. If this MOU is so terminated, the terminating party shall be liable only for performance in accordance with the terms of this MOU for performance prior to the effective date of termination.

IX. DISPUTES

In the event that a dispute arises under this MOU, it shall be determined in the following manner: The Chief of WSP, or designee, shall appoint one member to the Dispute Board. NCJA shall appoint one member to the Dispute Board. The Chief of WSP, or designee, and the NCJA shall jointly appoint an additional member to the Dispute Board. The Dispute Board shall evaluate the dispute and make a determination of the dispute. The determination of the Dispute Board shall be final and binding on the parties hereto. If applicable and as an alternative to this process, either of the parties may request intervention by the Governor, as provided by RCW 43.17.330, in which event the Governor's process will control.

X. EXHIBITS

The exhibits listed below are incorporated into and made a part of this MOU:

Exhibit A - 'Security and Management Control Outsourcing Standard for Non-Channelers'

Exhibit B - Federal Bureau of Investigation – Criminal Justice Information Services (CJIS) Security Policy, Version 5.2, published 8/9/2013 which is available at the following link: www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center. WSP will provide a copy of the manual upon request.

XI. ORDER OF PRECEDENCE

In the event of any inconsistency in the terms of this MOU, unless otherwise provided herein, the inconsistency shall be resolved by giving precedence in the following order:

a. Applicable federal and state statutes and regulations;
b. The Terms and Conditions contained in this MOU;
c. The Exhibits attached to this MOU;
d. Any other provisions of the MOU, whether incorporated by reference or otherwise.

XII. ALL WRITINGS CONTAINED HEREIN

This MOU contains all the terms and conditions agreed upon by the parties. No other understandings, oral or otherwise, regarding the subject matter of this MOU shall be deemed to exist or to bind any of the parties hereto.

STATE OF WASHINGTON
WASHINGTON STATE PATROL

_____
John R. Batiste, Chief

_____
Date

JEFFERSON COUNTY
JUVENILE AND FAMILY COURT

_____

_____
Date

Approved as to form only
11/4/13
Jefferson Co. Prosecutor's Office
David Alvarez, Chief Civil DPA

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELERS

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 without 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 *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.

1.04 *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.

1.05 *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.

1.06 *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.

1.07 *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 noncriminal justice administrative functions requiring access to CHRI.

1.08 *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.

1.09 *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:

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

1.10 *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.

1.11 *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.

1.12 *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.

1.13 *Positive Identification,* as provided in Article I(20) of the Compact, means a determination, based upon a comparison of fingerprints[1] 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.

1.14 *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.

1.15 *Security Violation* means the failure to prevent or failure to institute safeguards to prevent access, use, retention, or dissemination of CHRI in

[1] 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.

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 (1) the State Compact Officer/Chief Administrator[2] or (2) the FBI Compact Officer[3]; (b) provide the Compact Officer/Chief Administrator copies of the specific authority for the outsourced work, criminal history record check requirements, and/or a copy of relevant portions of the contract as requested; and (c) inquire of the FBI Compact Officer whether a prospective Contractor has any security violations (See Section 8.04). The FBI Compact Officer will report those findings to the Authorized Recipient and, when applicable, to the State Compact Officer/Chief Administrator.

2.02 The Authorized Recipient shall execute a contract or agreement prior to providing a Contractor access to CHRI. The contract shall, at a minimum, incorporate by reference and have appended thereto this Outsourcing Standard.

2.03 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI, specify the terms and conditions of such access; limit the use of such information to the purposes for which it is provided; limit retention of the information to a period of time not to exceed that period of time the Authorized Recipient is permitted to retain such information; prohibit dissemination of the information except as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General; ensure the security and confidentiality of the information to include confirmation that the intended recipient is authorized to receive CHRI; provide for audits and sanctions; provide conditions for termination of the contract; and ensure that Contractor

---

[2]The 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.

[3]State or local Authorized Recipients based on State or Federal Statutes shall contact the State Compact Officer/Chief Administrator. Federal or Regulatory Agency Authorized Recipients shall contact the FBI Compact Officer.

personnel comply with this Outsourcing Standard.

a. The Authorized Recipient shall conduct criminal history record checks of Contractor personnel having access to CHRI if such checks are required or authorized of the Authorized Recipient's personnel having similar access.[4] The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI and update those records within 24 hours when changes to that access occur and, if a criminal history record check is required, the Authorized Recipient shall maintain a list of Contractor personnel who successfully completed the criminal history record check.

b. The Authorized Recipient shall ensure that the Contractor maintains site security.

c. The Authorized Recipient shall ensure that the most current version of both the Outsourcing Standard and the CJIS Security Policy are incorporated by reference at the time of contract, contract renewal, or within 30 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or CJIS Security Policy, whichever is sooner. The Authorized Recipient shall notify the Contractor within 30 calendar days (unless otherwise directed) of FBI notification regarding changes or updates to the Outsourcing Standard and/or CJIS Security Policy.

2.04 The Authorized Recipient shall understand the communications and record capabilities of the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient. The Authorized Recipient shall maintain an updated topological drawing which depicts the interconnectivity of the Contractor's network configuration.

2.05 The Authorized Recipient is responsible for the actions of the Contractor and shall monitor the Contractor's compliance to the terms and conditions of the Outsourcing Standard. The Authorized Recipient shall certify to the Compact Officer/Chief Administrator that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

---

[4] If a national criminal history record check of Authorized Recipient personnel having access to CHRI is mandated or authorized by a federal statute, executive order, or state statute approved by the Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel having similar access are either covered by the existing law or that the existing law is amended to include such Contractor personnel prior to authorizing outsourcing initiatives. The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.06 The Authorized Recipient shall provide written notice of any early voluntary termination of the contract to the Compact Officer/Chief Administrator or the FBI Compact Officer.

3.0 *Responsibilities of the Contractor*

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJIS Security Policy) as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

3.02 The Contractor shall develop, document, administer, and maintain a Security Program (Physical, Personnel, and Information Technology) to comply with the most current Outsourcing Standard and the most current FBI *CJIS Security Policy*. The Security Program shall describe the implementation of the security requirements described in this Outsourcing Standard and the FBI *CJIS Security Policy*. In addition, the Contractor is also responsible to set, maintain, and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. The Authorized Recipient shall provide the written approval of a Contractor's Security Program.

3.03 The requirements for a Security Program should include, at a minimum:

a) Description of the implementation of the security requirements described in this Outsourcing Standard and the *CJIS Security Policy*.

b) Security Training.

c) Guidelines for documentation of security violations.

d) Standards for the selection, supervision, and separation of personnel with access to CHRI.

**If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the *CJIS Security Policy*. If the corporate policy is not this specific, it must flow down to a level where the documentation supports these requirements.

3.04 Except when the training requirement is retained by the Authorized Recipient, the Contractor shall develop a Security Training Program for all Contractor personnel with access to CHRI prior to their appointment/assignment. The Authorized Recipient shall review and provide to the Contractor written approval of the Security Training Program. Training shall be provided upon receipt of notice from the Compact Officer/Chief Administrator on any changes to federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General. Annual refresher training shall also be provided. The Contractor shall annually, not later than the anniversary date of the contract, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access

to CHRI.

3.05 The Contractor shall make its facilities available for announced and unannounced audits performed by the Authorized Recipient, the state, or the FBI on behalf of the Compact Council.

3.06 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI CJIS Division. During this review, provision will be made to update the Security Program to address security violations and to ensure changes in policies and standards as well as changes in federal and state law are incorporated.

3.07 The Contractor shall maintain CHRI only for the period of time necessary to fulfill its contractual obligations but not to exceed the period of time that the Authorized Recipient is authorized to maintain and does maintain the CHRI.

3.08 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of 365 days.

4.0 *Site Security*

4.01 The Authorized Recipient shall ensure that the Contractor site(s) is a physically secure location to protect against any unauthorized access to CHRI.

5.0 *Dissemination*

5.01 The Contractor shall not disseminate CHRI without the consent of the Authorized Recipient, and as specifically authorized by federal and state laws, regulations, and standards as well as with rules, procedures, and standards established by the Compact Council and the United States Attorney General.

5.02 An up-to-date log concerning dissemination of CHRI shall be maintained by the Contractor for a minimum one year retention period. This log must clearly identify: (A) The Authorized Recipient and the secondary recipient with unique identifiers, (B) the record disseminated, (C) the date of dissemination, (D) the statutory authority for dissemination, and (E) the means of dissemination.

5.03 If CHRI is stored or disseminated in an electronic format, the Contractor shall protect against unauthorized access to the equipment and any of the data. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent contract requirements.

6.0 *Personnel Security*

6.01 If a local, state, or federal written standard requires or authorizes a criminal history record check of the Authorized Recipient's personnel with access to

CHRI, then a criminal history record check shall be required of the Contractor's (and approved Sub-Contractor's) employees having access to CHRI. Criminal history record checks of Contractor and approved Sub-Contractor employees, at a minimum, will be no less stringent than criminal history record checks that are performed on the Authorized Recipient's personnel performing similar functions. Criminal history record checks must be completed prior to accessing CHRI under the contract.

6.02 The Contractor shall ensure that each employee performing work under the contract is aware of the requirements of the Outsourcing Standard and the state and federal laws governing the security and integrity of CHRI. The Contractor shall confirm in writing that each employee has certified in writing that he/she understands the Outsourcing Standard requirements and laws that apply to his/her responsibilities. The Contractor shall maintain the employee certifications in a file that is subject to review during audits. Employees shall make such certification prior to performing work under the contract.

6.03 The Contractor shall maintain updated records of personnel who have access to CHRI, update those records within 24 hours when changes to that access occur, and if a criminal history record check is required, maintain a list of personnel who have successfully completed criminal history record checks. The Contractor shall notify Authorized Recipients within 24 hours when additions or deletions occur.

7.0 *System Security*

7.01 The Contractor's security system shall comply with the CJIS Security Policy in effect at the time the Outsourcing Standard is incorporated into the contract and with successor versions of the CJIS Security Policy.

a. If CHRI can be accessed by unauthorized personnel via Wide Area Network/Local Area Network or the Internet, then the Contractor shall protect the CHRI with firewall-type devices to prevent such unauthorized access. These devices shall implement a minimum firewall profile as specified by the CJIS Security Policy in order to provide a point of defense and a controlled and audited access to CHRI, both from inside and outside the networks.

b. Data encryption shall be required throughout the network passing CHRI through a shared public carrier network.

7.02 The Contractor shall provide for the secure storage and disposal of all hard copy and media associated with the system to prevent access by unauthorized personnel.

a. CHRI shall be stored in a physically secure location.

b. The Authorized Recipient shall ensure that a procedure is in place for

sanitizing all fixed storage media (e.g., disks, drives, backup storage) at the completion of the contract and/or before it is returned for maintenance, disposal, or reuse. Sanitization procedures include overwriting the media and/or degaussing the media.

c. The Authorized Recipient shall ensure that a procedure is in place for the disposal or return of all non-fixed storage media (e.g., hard copies, print-outs).

7.03 To prevent and/or detect unauthorized access to CHRI in transmission or storage, each Authorized Recipient, Contractor, or sub-Contractor must be assigned a unique identifying number.

8.0 *Security Violations*

8.01 Duties of the Authorized Recipient and Contractor

a. The Contractor shall develop and maintain a written policy for discipline of Contractor employees who violate the security provisions of the contract, which includes this Outsourcing Standard that is incorporated by reference.

b. Pending investigation, the Contractor shall, upon detection or awareness, suspend any employee who commits a security violation from assignments in which he/she has access to CHRI under the contract.

c. The Contractor shall immediately (within four hours) notify the Authorized Recipient of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. Within five calendar days of such notification, the Contractor shall provide the Authorized Recipient a written report documenting such security violation, any corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the prior notification.

d. The Authorized Recipient shall immediately (within four hours) notify the State Compact Officer/Chief Administrator and the FBI Compact Officer of any security violation or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The Authorized Recipient shall provide a written report of any security violation (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator, if applicable, and the FBI Compact Officer, within five calendar days of receipt of the written report from the Contractor. The written report must include any corrective actions taken by the Contractor and the Authorized Recipient to resolve such security violation.

8.02 Termination of the contract by the Authorized Recipient for security violations

a. The contract is subject to termination by the Authorized Recipient for security violations involving CHRI obtained pursuant to the contract.

b. The contract is subject to termination by the Authorized Recipient for the Contractor's failure to notify the Authorized Recipient of any security violation or to provide a written report concerning such violation.

c. If the Contractor refuses to or is incapable of taking corrective actions to successfully resolve a security violation, the Authorized Recipient shall terminate the contract.

8.03 Suspension or termination of the exchange of CHRI for security violations

a. Notwithstanding the actions taken by the State Compact Officer, if the Authorized Recipient fails to provide a written report notifying the State Compact Officer/Chief Administrator or the FBI Compact Officer of a security violation, or refuses to or is incapable of taking corrective action to successfully resolve a security violation, the Compact Council or the United States Attorney General may suspend or terminate the exchange of CHRI with the Authorized Recipient pursuant to 28 CFR §906.2(d).

b. If the exchange of CHRI is suspended, it may be reinstated after satisfactory written assurances have been provided to the Compact Council Chairman or the United States Attorney General by the Compact Officer/Chief Administrator, the Authorized Recipient and the Contractor that the security violation has been resolved. If the exchange of CHRI is terminated, the Contractor's records (including media) containing CHRI shall be deleted or returned in accordance with the provisions and time frame as specified by the Authorized Recipient.

8.04 The Authorized Recipient shall provide written notice (through the State Compact Officer/Chief Administrator if applicable) to the FBI Compact Officer of the following:

a. The termination of a contract for security violations.

b. Security violations involving the unauthorized access to CHRI.

c. The Contractor's name and unique identification number, the nature of the security violation, whether the violation was intentional, and the number of times the violation occurred.

8.05 The Compact Officer/Chief Administrator, Compact Council and the United States Attorney General reserve the right to investigate or decline to investigate any report of unauthorized access to CHRI.

8.06 The Compact Officer/Chief Administrator, Compact Council, and the United

States Attorney General reserve the right to audit the Authorized Recipient and the Contractor's operations and procedures at scheduled or unscheduled times. The Compact Council, the United States Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the contract.

9.0 *Miscellaneous Provisions*

9.01 This Outsourcing Standard does not confer, grant, or authorize any rights, privileges, or obligations to any persons other than the Contractor, the Authorized Recipient, Compact Officer/Chief Administrator (where applicable), and the FBI.

9.02 The following document is incorporated by reference and made part of this Outsourcing Standard: (1) The CJIS Security Policy.

9.03 The terms set forth in this document do not constitute the sole understanding by and between the parties hereto; rather they provide a minimum basis for the security of the system and the CHRI accessed therefrom and it is understood that there may be terms and conditions of the appended contract which impose more stringent requirements upon the Contractor.[5]

9.04 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. Conformance to such security measures may not be less stringent than stated in this Outsourcing Standard without the consent of the Compact Council in consultation with the United States Attorney General.

9.05 This Outsourcing Standard may only be modified by the Compact Council and may not be modified by the parties to the appended contract without the consent of the Compact Council.

9.06 Appropriate notices, assurances, and correspondence to the FBI Compact Officer, Compact Council, and the United States Attorney General required by Section 8.0 of this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer
1000 Custer Hollow Road
Module D-3
Clarksburg, WV 26306

10.0 *Exemption from Above Provisions*

---

[5] Such conditions could include additional audits, fees, or security requirements. The Compact Council, Authorized Recipients, and the Compact Officer/Chief Administrator have the explicit authority to require more stringent standards than those contained in the Outsourcing Standard.

10.01 An Information Technology (IT) contract need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the IT contractor's personnel is limited solely for the development and/or maintenance of the Authorized Recipient's computer system;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the IT contractor;
3. The computer system resides within the Authorized Recipient's facility;
4. The Authorized Recipient's personnel supervise or work directly with the IT contractor personnel;
5. The Authorized Recipient maintains complete, positive control of the IT contractor's access to the computer system and CHRI contained therein; and
6. The Authorized Recipient retains all of the duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard.

10.02 An Authorized Recipient's contract where access to CHRI is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient need only include Sections 1.0, 2.01, 2.02, 2.03, 3.01, 4.0, 6.0, 8.0, and 9.0 of this Outsourcing Standard for Non-Channelers when all of the following conditions exist:

1. Access to CHRI by the Contractor is limited solely for the purposes of: (A) storage (referred to as archiving in some states) of the CHRI at the Contractor's facility; (B) retrieval of the CHRI by Contractor personnel on behalf of the Authorized Recipient with appropriate security measures in place to protect the CHRI; and/or (C) destruction of the CHRI by Contractor personnel when not observed by the Authorized Recipient;
2. Access to CHRI is incidental, but necessary, to the duties being performed by the Contractor;

3. The Contractor is not authorized to disseminate CHRI to any other agency or contractor on behalf of the Authorized Recipient;
4. The Contractor's personnel are subject to the same criminal history record checks as the Authorized Recipient's personnel;
5. The criminal history record checks of the Contractor personnel are completed prior to work on the contract or agreement;
6. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate contract to perform such noncriminal justice administrative functions, subject to all applicable requirements, including the Outsourcing Standard; and
7. The Contractor stores the CHRI in a physically secure location.