National Crime Prevention and Privacy Compact Council

Security and Management Control Outsourcing Standard for Non-Channelers

Approved by the Council on
May 16, 2018

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 34, United States Code (U.S.C.), Section 40314 (b), (formally cited as 42 U.S.C. § 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 *Identity History Summary (IdHS)*, for the purposes of this Outsourcing Standard, means the report of all identification, demographic, and event information (criminal and/or civil) within a Next Generation Identification (NGI) Identity record which may be disseminated to an Authorized Recipient contingent upon legislation and federal regulations. The IdHS contains the criminal justice information associated with criminal fingerprint (i.e., "rap sheets") and/or noncriminal justice information associated with the civil fingerprints, therefore the existence of an IdHS

alone does not reflect criminal history events on that NGI Identity. This term is unique to NGI and is not intended to affect other agencies' use of the term "rap sheet" to describe reports of information in their identification repositories.

1.10 *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

1.11 *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.

1.12 *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.

1.13 *Personally Identifiable Information (PII)* means information which can be used to distinguish or trace an individual's identity, such as name, social security number, or biometric records, alone or when combined with other personal or identifying information which is linked or linkable to a specific individual, such as date and place of birth, or mother's maiden name.

1.14 *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.

1.15 *PII Breach* means the loss of control, compromise, unauthorized disclosure, unauthorized acquisition, unauthorized access or any similar term referring to situations where persons other than the authorized users, and for other

than authorized purposes, have access or potential access to PII, whether physical or electronic.

1.16 *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.

1.17 *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.

1.18 *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 (1) the State Compact Officer/Chief Administrator[2] or (2)

[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.

[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.

the FBI Compact Officer[3]; and (b) provide the State Compact Officer/Chief Administrator or the FBI Compact Officer 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.

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 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 of the Authorized Recipient's personnel are required or authorized under an existing federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544.[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

[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.

[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 United States Attorney General under Public Law 92-544, the State Compact Officer/Chief Administrator and/or the FBI Compact Officer must ensure Contractor personnel accessing CHRI 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.

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. (See the current CJIS Security Policy [www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view])

c. The State Compact Officer/Chief Administrator or the FBI Compact Officer shall make available the most current versions of both the Outsourcing Standard and the CJIS Security Policy to the Authorized Recipient within 60 calendar days (unless otherwise directed) of notification of successor versions of the Outsourcing Standard and/or the CJIS Security Policy. The Authorized Recipient shall notify the Contractor within 60 calendar days of the FBI/state notification regarding changes or updates to the Outsourcing Standard and/or the CJIS Security Policy. The Authorized Recipient shall be responsible to ensure the most updated versions are incorporated by reference at the time of contract, contract renewal, or within the 60 calendar day notification period, whichever is sooner.

d. The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.

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 request and approve a topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced function(s). The Authorized Recipient shall understand and approve any modifications to the Contractor's network configuration as it relates to the outsourced function(s). For approvals granted through the State Compact Officer/Chief Administrator, the Authorized Recipient, if required, shall coordinate the approvals with the State Compact Officer/Chief Administrator.

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. For approvals granted through the FBI Compact Officer, the Authorized Recipient shall certify to the FBI Compact Officer that an audit was conducted with the Contractor within 90 days of the date the Contractor first receives CHRI under the approved

outsourcing agreement. For approvals granted through the State Compact Officer/Chief Administrator, the Authorized Recipient, in conjunction with the State Compact Officer/Chief Administrator, will conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement. The Authorized Recipient shall certify to the State Compact Officer/Chief Administrator that the audit was conducted.

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.

2.07 The Authorized Recipient shall appoint an Information Security Officer. The Authorized Recipient's Information Security Officer shall:

a. Serve as the security POC for the FBI CJIS Division Information Security Officer.
b. Document technical compliance with this Outsourcing Standard.
c. Establish a security incident response and reporting procedure to discover, investigate, document, and report on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the CJIS Systems Officer, State Compact Officer/Chief Administrator and the FBI CJIS Division Information Security Officer.

2.08 The Authorized Recipient shall immediately (within one hour) notify the State Compact Officer/Chief Administrator or the FBI of any PII breach. The Authorized Recipient shall also provide a written report of any PII breach (to include unauthorized access to CHRI by the Contractor) to the State Compact Officer/Chief Administrator or the FBI within five calendar days of receipt of the initial report of the PII breach. The written report must include corrective actions taken by the Authorized Recipient and, if necessary, the Contractor to resolve such PII breach.

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 CJIS Security Policy. The Security Program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the 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 to the State Compact Officer/Chief Administrator or the FBI Compact Officer of a Contractor's Security Program. For approvals granted through the State Compact Officer/Chief Administrator, it is the responsibility of the State Compact Officer/Chief Administrator to ensure the Authorized Recipient is in compliance with the CJIS Security Policy.

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 to include:

i) Develop and maintain a written incident reporting plan to address security events, to include violations and incidents. (See the CJIS Security Policy {www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view}).

ii) A process in place for reporting 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 and security inspections 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.

3.09 The Authorized Recipient and/or Contractor shall make available to the State Compact Officer/Chief Administrator or the FBI Compact Officer the relevant portions of the current and approved contract relating to CHRI, upon request.

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 with unique identifiers to include the FBI assigned Originating Agency Idenifiers to include the FBI assigned Originating Agency Identifier (ORI)/Originating Agency Case (OCA) number, (B) the Transaction Control Number (TCN), (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. Devices shall be implemented 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 for data in transit pursuant to the requirements in the CJIS Security Policy.

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.

See the current CJIS Security Policy to address:

[www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view]

a. Physically secure location.
b. Sanitization procedures for all fixed and non-fixed storage media.
c. Storage procedures for all fixed and non-fixed storage media.

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 Authorized Recipient 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. The Authorized Recipient shall develop and maintain a written incident reporting plan for security events, to include violations and incidents. (See also Sections 2.07 and 3.03)
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 one hour of discovery) notify the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI of any security violation to include unauthorized access to CHRI. Within five calendar days of such discovery, the Contractor shall provide the Authorized Recipient, the State Compact Officer/Chief Administrator or the FBI a written report documenting such security violation, corrective actions taken by the Contractor to resolve such violation, and the date, time, and summary of the violation.
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 and Contractor 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 *PII*

9.01 The Contractor is responsible for protecting all PII in its possession and control when handling, using, or storing CHRI.

9.02 The Contractor shall notify authorized individuals of their right to report PII breaches directly to the FBI should they believe their information has been mishandled or compromised.

9.03 The Contractor shall immediately (within one hour of discovery) notify the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI of any PII breach or potential PII breach. Within five calendar days of such discovery, the Contractor shall provide the Authorized Recipient, the State Compact Officer/Chief Administrator, or the FBI a written report documenting such violation and corrective actions taken to resolve such violation, to include the date, time, and summary of the notification to resolve such breach.

10.0 *Miscellaneous Provisions*

10.01 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.

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

10.03 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]

[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.

10.04 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.

10.05 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.

10.06 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

11.0 *Exemption from Above Provisions*

11.01 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.

11.02 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.

12.0 *Duties of the State Compact Officer/Chief Administrator*

12.01 The State Compact Officer/Chief Administrator shall review legal authority and respond in writing to the Authorized Recipient's request to outsource noncriminal justice administrative functions.

12.02 The State Compact Officer/Chief Administrator reserves the right to review relevant portions of the outsourcing contract relating to CHRI throughout the duration of the contract approval.

12.03 The State Compact Officer/Chief Administrator must ensure criminal history record checks on approved Contractor and Sub-Contractor employees with access to CHRI are completed by the Authorized Recipient, if such checks are required or authorized of the Authorized Recipient personnel by federal statute, executive order, or state statute approved by the United States Attorney General under Public Law 92-544. Criminal history record checks should be no less stringent than the checks performed on the Authorized Recipient personnel. Criminal history record checks must be completed prior to accessing CHRI under the contract.

12.04 Coordinate with the Authorized Recipient for the review and approval of the Contractor's Topological drawing which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourcing function(s).

12.05 90 Day Compliance Review

a. The State Compact Officer/Chief Administrator shall work in coordination with the Authorized Recipient to conduct an audit of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.

b. The State Compact Officer/Chief Administrator shall review the Authorized Recipient's audit certification to ensure compliance with the Outsourcing Standard.

i) The State Compact Officer/Chief Administrator shall address concerns with the Authorized Recipient resulting in non-compliance with the 90 day audit of the Contractor.

ii) The State Compact Officer/Chief Administrator shall have the right to terminate an Authorized Recipient's Outsourcing approval to a Contractor(s) for failure or refusal to correct a non-compliance issue(s).

12.06 The State Compact Officer/Chief Administrator shall coordinate with the Authorized Recipient to review the Contractor's Security Program. The program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJIS Security Policy. During the review, provisions will be made to update the Security Program to address security events and to ensure changes in policies and standards, as well as changes in federal and state law, are incorporated.

12.07 The State Compact Officer/Chief Administrator shall audit the Authorized Recipient and/or Contractor's operations and procedures. This may be done at scheduled and unscheduled times.

12.08 The State Compact Officer/Chief Administrator shall assign a unique

identifying number to each Authorized Recipient, Contractor, or Sub-Contractor to ensure system security.

12.09 The State Compact Officer/Chief Administrator shall require immediate (within four hours) notification by the Authorized Recipient of any security event, to include security violations and incidents or termination of the contract, to include unauthorized access to CHRI made available pursuant to the contract. The State Compact Officer/Chief Administrator shall receive a written report from the Authorized Recipient of any security event (to include unauthorized access to CHRI by the Contractor) within five calendar days of receipt of the written report from the Contractor, that must include any corrective actions taken by the Contractor and Authorized Recipient to resolve such security event. (See the CJIS Security Policy {www.fbi.gov/about-us/cjis/cjis-security-policy-resource-center/view})

12.10 Suspension or termination of the exchange of CHRI for security events.

a. The State Compact Officer/Chief Administrator may suspend or terminate the exchange of CHRI for security events or refusal or incapability to take corrective action to successfully resolve a security event.

b. The State Compact Officer/Chief Administrator may reinstate access to CHRI between the Authorized Recipient and the Contractor after receiving written assurance(s) of corrective action(s) from the Authorized Recipient and/or the Contractor.

12.11 The State Compact Officer/Chief Administrator shall provide written notification to the FBI Compact Officer of the termination of a contract for security events to include the security events involving access to CHRI; the Contractor's name and unique identification number; the nature of the security event; whether the event was intentional; and the number of times the event occurred.

12.12 The State Compact Officer/Chief Administrator reserves the right to investigate or decline to investigate any report of unauthorized access to CHRI.

12.13 The State Compact Officer/Chief Administrator is authorized to perform a final audit of the Contractor's system following termination of contract.