National Crime Prevention and Privacy Compact Council

Security and Management Control Outsourcing Standard for Non-Channeling

Approved by the Council on
May 8, 2025

SECURITY and MANAGEMENT CONTROL OUTSOURCING STANDARD for NON-CHANNELING

This Security and Management Control Outsourcing Standard (Outsourcing Standard) outlines the individual and collective responsibilities of the parties involved in an outsourcing agreement, so that the security and integrity of the criminal history record information (CHRI) is not compromised.

This Outsourcing Standard is applicable to the "Authorized Recipient," the "Contractor," the Federal Bureau of Investigation (FBI), and the Compact Officer/Chief Administrator. An Authorized Recipient is an entity with the authority to receive CHRI for noncriminal justice purposes. A Contractor is an entity selected by an Authorized Recipient to perform noncriminal justice administrative functions with access to CHRI on behalf of the Authorized Recipient. Please note, this Outsourcing Standard is not applicable to the administration of criminal justice functions performed by a noncriminal justice agency (e.g., Section 151 of the Adam Walsh Child Protection and Safety Act of 2006.)

The intent of this Outsourcing Standard is to require that the parties involved in an outsourcing agreement maintain security practices consistent with federal and state laws, regulations, and applicable standards (including the FBI Criminal Justice Information Services [CJIS] Security Policy [CJISSECPOL]) and with the rules, procedures, and standards established by the Compact Council and the United States (U.S.) Attorney General.

Pursuant to this Outsourcing Standard, an Authorized Recipient is not permitted to designate an entity as a Contractor for the sole purpose of disseminating the CHRI for that entity's own use or purpose.

This Outsourcing Standard is divided into the following six sections:

Section 1 - "Definitions"

Section 2 - "Responsibilities of the Authorized Recipient"

Section 3 - "Responsibilities of the Contractor"

Section 4 - "Responsibilities of the Compact Officer/Chief Administrator"

Section 5 - "Miscellaneous Provisions"

Section 6 - "Exemption from Above Provisions"

SECTION 1
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.

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 U.S. Attorney General to receive CHRI for noncriminal justice purposes.

1.03 *Authorized Recipient Point of Contact (ARPOC)* means the individual appointed by the Authorized Recipient to serve as the point-of-contact at the Authorized Recipient for matters relating to CJIS information access. The ARPOC administers FBI CJIS systems programs within the Authorized Recipient and oversees the Authorized Recipients' compliance with CJIS systems policies. The ARPOC must be an employee of the Authorized Recipient, and the ARPOC role cannot be outsourced.

1.04 *Authorized Recipient Security Officer (ARSO)* means the individual appointed by the Authorized Recipient to coordinate and oversee Information Security by ensuring that the Contractor is adhering to the CJISSECPOL and Outsourcing Standard, verifying the completion of annual Awareness and Training Program, and communicating with the FBI CJIS Division on matters relating to Information Security. The ARSO must be an employee of the Authorized Recipient, and the ARSO role cannot be outsourced.

1.05 *Chief Administrator* means the primary administrator of a Nonparty State's criminal history record repository or a designee of such, which is also referred to as the State Identification Bureau (SIB) Chief. The Chief Administrator and/or their designee must be a regular full-time employee of the state's criminal history record repository, and the role cannot be outsourced.

1.06 *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.

1.07 *CJIS Advisory Policy Board (APB)* means the oversight body whose purpose is to make recommendations to the FBI Director concerning policy proposals and proposals for new and expanded uses of the various criminal justice information systems managed by the FBI CJIS Division. The CJIS APB functions solely as an advisory body in compliance with the Federal Advisory Committee Act.

1.08 *CJISSECPOL* means the most current FBI-published document that provides Criminal Justice Agencies and Noncriminal Justice Agencies with a minimum set of security requirements for access to FBI CJIS Division systems and information and to protect and safeguard Criminal Justice Information (CJI). This minimum standard of security requirements ensures continuity of information protection. The essential premise of the CJISSECPOL is to provide the appropriate controls to protect CJI, from creation through destruction, whether at rest or in transit.

1.09 *CJIS Systems Agency (CSA)*, means a duly authorized state, federal, international, tribal, or territorial criminal justice agency on the CJIS network providing statewide (or equivalent) service to its criminal justice users with respect to the CJI from various systems managed by the FBI CJIS Division. There shall be only one CSA per state or territory. In federal agencies, the CSA may be the interface or switch to other federal agencies connecting to the FBI CJIS systems.

1.10 *CJIS Systems Officer (CSO)*, means the individual located with the CJIS Systems Agency responsible for the administration of the CJIS network on behalf of the CJIS Systems Agency.

1.11 *Compact Council* means the council established by the National Crime Prevention and Privacy Compact Act of 1998 to promulgate rules and procedures for the effective use of the III System for noncriminal justice purposes.

1.12 *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.

1.13 *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 an outsourcing agreement with an Authorized Recipient to perform noncriminal justice administrative functions requiring access to CHRI. The term Contractor also includes a subcontractor(s) that has contracted with a Contractor and supports the outsourced noncriminal justice administrative functions being performed by the Contractor on behalf of the Authorized Recipient.

1.14 *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.

1.15 *Dissemination*, for the purposes of this Outsourcing Standard, means the disclosure of 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 U.S. Attorney General.

1.16 *Noncriminal Justice Administrative Functions*, for the purposes of this Outsourcing Standard, 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

1.17 *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.

1.18 *Outsourcing Agreement*, for the purpose of this Outsourcing Standard, means a contractual agreement between an Authorized Recipient and a Contractor, in which the Contractor agrees to perform noncriminal justice administrative functions requiring access to CHRI on behalf of the Authorized Recipient. When outsourcing occurs between governmental agencies, the outsourcing agreement may be an interagency agreement.

1.19 *Outsourcing Standard* means a document approved by the Compact Council after consultation with the U.S. Attorney General which establishes rules and guidelines for an Authorized Recipient and a Contractor. Pursuant to 28 CFR part 906, 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 outsourcing agreement, and contains such other provisions as the Compact Council may require.

1.20 *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.

1.21 *Physically Secure Location*, for the purposes of this Outsourcing Standard, 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.

1.22 *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.

1.23 *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.

1.24 *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 U.S. Attorney General; or (C) the CJISSECPOL.

[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 via email at compactoffice@fbi.gov.

SECTION 2
RESPONSIBILITIES of the AUTHORIZED RECIPIENT

2.01 Prior to engaging in outsourcing any noncriminal justice administrative functions with a Contractor, the Authorized Recipient shall request and receive written permission from the Compact Officer/Chief Administrator[2]. The written request must include the Authorized Recipient's specific statutory authority for access to CHRI.

2.02 Outsourcing Agreement:

a. The Authorized Recipient shall execute an outsourcing agreement prior to providing a Contractor access to CHRI. The outsourcing agreement shall, at a minimum, incorporate by reference this Outsourcing Standard and the CJISSECPOL. Upon request, the Authorized Recipient must provide the Compact Officer/Chief Administrator or the FBI[3] with all portions of the current outsourcing agreement that relate to CHRI.

b. Pursuant to an outsourcing agreement with the Authorized Recipient, when a Contractor requests to subcontract noncriminal justice administrative functions requiring access to CHRI, the Authorized Recipient must receive outsourcing approval from the Compact Officer/Chief Administrator for the subcontractor prior to performing the noncriminal justice administrative functions. The outsourcing agreement must not be entered into until outsourcing approval is granted. Following outsourcing approval by the Compact Officer/Chief Administrator, the outsourcing agreement between the Contractor and the subcontractor must:
   i. Incorporate by reference this Outsourcing Standard and the CJISSECPOL.
   ii. Authorize continuing access to the physical or logical space by the Contractor, the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI.
   iii. Ensure controlled access to the physical or logical space limited to subcontractor employees.

[2] State or local Authorized Recipients submitting fingerprints through a state criminal records repository pursuant to state or federal statutes shall contact the State Compact Officer/Chief Administrator. Authorized Recipients which are federal agencies, federally-regulated agencies, or other entities that do not submit fingerprints or request CHRI through a state criminal records repository shall contact the FBI Compact Officer.

[3] See Section 5.08 for FBI contact information.

iv. Require the same level of physical and data/information security required of the space and system currently maintained by the Contractor.
v. Authorize the same level of auditing, oversight, and compliance required of Contractor under the current Outsourcing Standard and CJISSECPOL

Upon request, the Authorized Recipient must provide the Compact Officer/Chief Administrator or the FBI[4] with all portions of the outsourcing agreement between the Contractor and subcontractor that relate to CHRI.

2.03 The Authorized Recipient shall be responsible for ensuring the most updated version of the Outsourcing Standard and the CJISSECPOL are incorporated by reference at the time of outsourcing agreement, outsourcing agreement renewal, or within the 60-day notification period of updates to the Outsourcing Standard and the CJISSECPOL, whichever is sooner.

2.04 The Authorized Recipient shall, in those instances when the Contractor is to perform duties requiring access to CHRI:

a. Specify the terms and conditions of such access.
b. Limit the use of such information to the purposes for which it is provided.
c. 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.
d. 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 U.S. Attorney General.
e. Ensure the security and confidentiality of CHRI.
f. Provide for audits and sanctions.
g. Provide conditions for termination of the outsourcing agreement.

2.05 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 U.S. Attorney General under

[4] See Section 5.08 for FBI contact information.

Public Law 92-544.[5] The Authorized Recipient shall maintain updated records of Contractor personnel who have access to CHRI, update those records within one-business day when changes to that access occur, and maintain a list of Contractor personnel who have successfully completed criminal history record checks. Criminal history record checks must be completed prior to accessing CHRI under the outsourcing agreement.

2.06 The Authorized Recipient is responsible for knowing and understanding how CHRI is processed, transmitted, and stored by the Contractor which has access to federal or state records through, or because of, its outsourcing relationship with the Authorized Recipient.

2.07 The Authorized Recipient shall request and approve a network diagram 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.

2.08 The Authorized Recipient shall provide written notice of any early voluntary termination of the outsourcing agreement with the Contractor to the Compact Officer/Chief Administrator.

2.09 The Authorized Recipient shall appoint an ARSO. Within 30 calendar days of the initial outsourcing approval, the Authorized Recipient shall notify the Compact Officer/Chief Administrator of the appointment and provide contact information for the ARSO. The Authorized Recipient must also notify the Compact Officer/Chief Administrator within 30 calendar days when this individual changes.

2.10 The Authorized Recipient shall provide a copy of the written approval of a Contractor's Security Program and Awareness and Training Program to the Compact Officer/Chief Administrator, upon request.

[5] The national criminal history record checks of Contractor personnel with access to CHRI cannot be outsourced and must be performed by the Authorized Recipient.

2.11 The Authorized Recipient shall develop and maintain a written incident reporting plan for security events to include violations and incidents. The written incident reporting plan must include information regarding the procedures for discovering, investigating, documenting, and reporting on major incidents that significantly endanger the security or integrity of the noncriminal justice agency systems to the Compact Officer/Chief Administrator, FBI CJIS Division Information Security Officer, and, if applicable, the CJIS Systems Officer

2.12 The Authorized Recipient shall notify the Compact Officer/Chief Administrator and the FBI[6] of any PII breach or security violation within one hour of notice from the Contractor. The Authorized Recipient shall also provide a written report of any PII breach or security violation within five calendar days of receipt of the initial notification from the Contractor. The written report must detail the corrective actions taken by the Authorized Recipient and, if necessary, the Contractor to resolve the issue; the applicable Contractor's name; a summary of the violation; the date and time of the violation; whether the violation was intentional; and the number of times the violation occurred.

2.13 The Authorized Recipient may initiate a termination of its outsourcing agreement with the Contractor due to the following:

a. The Contractor commits a PII breach or security violation involving access to CHRI obtained pursuant to the outsourcing agreement.
b. The Contractor fails to notify the Authorized Recipient of a PII breach or security violation or to provide a written report of a violation.
c. The Contractor refuses to, or is incapable of, taking corrective actions to successfully resolve a PII breach or security violation.

2.14 If the Authorized Recipient fails to notify the Compact Officer/Chief Administrator or the FBI[7] of a security violation, then the Authorized Recipient's access to CHRI may be suspended pursuant to Title 28. Code of Federal Regulations, section 906.2(d). If the exchange of CHRI is suspended, it may be reinstated after the Compact Officer/Chief Administrator, the Authorized Recipient, and the Contractor have provided satisfactory written assurances that the security violation has been resolved to the Compact Council Chairman or the U.S. Attorney General.

[6] See Section 5.08 for FBI contact information.
[7] See Section 5.08 for FBI contact information.

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

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

2.17 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[8] 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.

2.18 The Authorized Recipient has the option to establish Contractor site security requirements that are more stringent than those set by the CJIS APB, as defined in the CJISSECPOL.

2.19 The Authorized Recipient 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.

[8] See Section 5.08 for FBI contact information.

SECTION 3
RESPONSIBILITIES of the CONTRACTOR

3.01 The Contractor and its employees shall comply with all federal and state laws, regulations, and standards (including the CJISSECPOL) as well as with rules, procedures, and standards established by the Compact Council and the U.S. Attorney General.

3.02 Upon request, the Contractor must provide the Compact Officer/Chief Administrator with all portions of the current and approved outsourcing agreement with the Authorized Recipient that relate to CHRI.

3.03 The Contractor shall provide written notice of any early voluntary termination of the outsourcing agreement with the Authorized Recipient to the Compact Officer/Chief Administrator.

3.04 The Contractor shall ensure that each employee performing work under the outsourcing agreement 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 outsourcing agreement.

3.05 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 CJISSECPOL. The Security Program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJISSECPOL. In addition, the Contractor is also responsible to maintain and enforce the standards for the selection, supervision, and separation of personnel who have access to CHRI. If the Contractor is using a corporate policy, it must meet the requirements outlined in this Outsourcing Standard and the CJISSECPOL. If the corporate policy is not this specific, documentation must be established to support these requirements. The Contractor's Security Program must be approved in writing by the Authorized Recipient.

3.06 The Contractor's Security Program shall comply with the CJISSECPOL in effect at the time the Outsourcing Standard is incorporated into the Contractor-Authorized Recipient outsourcing agreement, and with successor versions of the CJISSECPOL.

3.07 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 CJISSECPOL.
b. Awareness and training Program.
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 CJISSECPOL).
    ii) A process in place for reporting security violations.
d. Standards for the selection, supervision, and separation of personnel with access to CHRI.

3.08 The Contractor's Security Program is subject to review by the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI. Based on this review, the Contractor must update the Security Program to address any security violations and to incorporate any changes in policies, standards, and federal and state law.

3.09 Except when the Authorized Recipient retains the training requirement, the Contractor shall develop an Awareness and Training Program in accordance with the CJISSECPOL. All Contractor personnel with access to CHRI shall complete the training prior to their appointment/assignment. The Contractor's Awareness and Training Program must be approved in writing by the Authorized Recipient. The Contractor shall also provide training to all personnel with access to CHRI 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 U.S. Attorney General. The Contractor shall administer annual refresher training to all Contractor personnel with access to CHRI. The Contractor shall annually, no later than the anniversary date of the outsourcing agreement, certify in writing to the Authorized Recipient that annual refresher training was completed for those Contractor personnel with access to CHRI.

3.10 The Contractor shall maintain updated records of employees who have access to CHRI, update those records within 24 hours when changes to employee access occurs, and notify the Authorized Recipients via an agreed upon method within one-business day of any changes to employee access.

3.11 The Contractor shall protect against any unauthorized person(s) having the ability to access CHRI. In no event shall responses containing CHRI be disseminated other than as governed by this Outsourcing Standard or more stringent outsourcing agreement requirements.

3.12 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. The Contractor must also permit the Authorized Recipient, the state, or the FBI to review its network configuration as it relates to the outsourced function(s) upon request.

3.13 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.

3.14 The Contractor shall only disseminate CHRI with 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 U.S. Attorney General.

3.15 The Contractor shall maintain a log of any dissemination of CHRI, for a minimum of one year. This log must clearly identify:

a. The Authorized Recipient
b. The Transaction Control Number (TCN)
c. The date of dissemination
d. The statutory authority for access to CHRI
e. The means of dissemination.

3.16 The Contractor is responsible for protecting all PII in its possession and control pursuant to the approved outsourcing agreement with the Authorized Recipient.

3.17 In accordance with the Authorized Recipient's written policy, the Contractor shall discipline Contractor employees who violate the security provisions of the outsourcing agreement, which includes this Outsourcing Standard that is incorporated by reference.

3.18 The Contractor shall ensure compliance with the Authorized Recipient's written policy regarding the suspension/termination of access to CHRI and potential reinstatement of access to CHRI for contractor personnel that violate security provisions.

3.19 The Contractor shall notify the Authorized Recipient, the Compact Officer/Chief Administrator, and the FBI[9] of any PII breach or security violation to include unauthorized access to CHRI within one hour of discovery. Within five business days of such discovery, the Contractor shall provide the Authorized Recipient, the Compact Officer/Chief Administrator and the FBI[10] with a written report of any PII breach or security violation. The written report must detail the corrective actions taken by the Contractor to resolve the issue; a summary of the violation, whether the violation was intentional; and the number of times the violation occurred.

[9] See Section 5.08 for FBI contact information.
[10] See Section 5.08 for FBI contact information.

SECTION 4
RESPONSIBILITIES of the COMPACT OFFICER/CHIEF ADMINISTRATOR

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

a. 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 U.S. Attorney General under Public Law 92-544, the Compact Officer/Chief Administrator 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.

b. 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.

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

4.03 The Compact Officer/Chief Administrator shall notify Authorized Recipients of updates to the Outsourcing Standard and the CJISSECPOL and shall make available the most current versions of both documents within 60 calendar days (unless otherwise directed) of such notification.

4.04 The 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 U.S. Attorney General under Public Law

92-544. Criminal history record checks may not be less stringent than the checks performed on the Authorized Recipient personnel. Criminal history record checks must be completed prior to accessing CHRI under the outsourcing agreement.

4.05 The Compact Officer/Chief Administrator may require the Authorized Recipient to coordinate with the Compact Officer/Chief Administrator for the review and approval of the Contractor's network diagram which depicts the interconnectivity of the Contractor's network configuration as it relates to the outsourced function(s).

4.06 90-Day Compliance Review

a. The Compact Officer/Chief Administrator may require the Authorized Recipient to coordinate with the Compact Officer/Chief Administrator when conducting the audit required by section 2.17 of the Contractor within 90 days of the date the Contractor first receives CHRI under the approved outsourcing agreement.
b. The Compact Officer/Chief Administrator, or designee, shall review the Authorized Recipient's audit certification to ensure compliance with the Outsourcing Standard.
    i) The 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 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).

4.07 The Compact Officer/Chief Administrator may require the Authorized Recipient to coordinate with the Compact Officer/Chief Administrator when reviewing the Contractor's Security Program as required by sections 2.10 and 3.05. The program shall describe the implementation of the security requirements outlined in this Outsourcing Standard and the CJISSECPOL. 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.

4.08 The Compact Officer/Chief Administrator must establish an audit process to triennially audit a sample of Authorized Recipients and Contractors engaged in outsourcing. These audits of Authorized Recipients and Contractors may be completed at scheduled and unscheduled times.

4.09 The Compact Officer/Chief Administrator shall require the Authorized Recipient and Contractor to provide initial notifications and subsequent written reports regarding PII breaches, security violations, or outsourcing agreement terminations within the required timeframes.

4.10 Pursuant to 28 CFR section 906.2(d) the Compact Officer/Chief Administrator may suspend the Authorized Recipient's access to CHRI or suspend or terminate the Authorized Recipient's exchange of CHRI with the Contractor for a PII breach or security violation, the failure to notify the Compact Officer/Chief Administrator of a PII breach or security violation, or the refusal or incapability to take corrective action to successfully resolve a PII breach or security violation. The Compact Officer/Chief Administrator may reinstate the Authorized Recipient's access to CHRI or the exchange of 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.

4.11 The Compact Officer/Chief Administrator shall provide written notification to the FBI[11] of the termination of an outsourcing agreement for security events to include the security events involving access to CHRI; the Contractor's name; the nature of the security event; whether the event was intentional; and the number of times the event occurred. The notification to the FBI[12] shall be made to the FBI Compact Officer.

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

4.13 The Compact Officer/Chief Administrator is authorized to perform a final audit of the Contractor's system following termination of an outsourcing agreement.

[11] See Section 5.08 for FBI contact information.
[12] See Section 5.08 for FBI contact information.

SECTION 5
MISCELLANEOUS PROVISIONS

5.01 The provisions of this Outsourcing Standard are established by, and can only be modified by, the Compact Council pursuant to 28 CFR Part 906 and are subject to the scope of that rule. The provisions apply to all personnel, systems, networks, and facilities supporting and/or acting on behalf of the Authorized Recipient.

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

5.03 The CJISSECPOL is incorporated by reference and made part of this Outsourcing Standard.

5.04 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 NGI system and the CHRI accessed there from and it is understood that there may be terms and conditions of the Authorized Recipient-Contractor outsourcing agreement which impose more stringent requirements upon the Contractor.[13]

5.05 The minimum security measures as outlined in this Outsourcing Standard may only be modified by the Compact Council. The minimum security measures outlined in the CJISSECPOL may only be modified through the CJIS APB process. 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 U.S. Attorney General.

[13] 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.

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

5.07 The Compact Officer/Chief Administrator, Compact Council, and the U.S. 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 U.S. Attorney General, and the state are authorized to perform a final audit of the Contractor's systems after termination of the outsourcing agreement.

5.08 Appropriate notices, assurances, and correspondence to the FBI, FBI Compact Officer, Compact Council, and the U.S. Attorney General required by this Outsourcing Standard shall be forwarded by First Class Mail to:

FBI Compact Officer
FBI CJIS Division
1000 Custer Hollow Road
Clarksburg, WV 26306

SECTION 6
EXEMPTIONS from ABOVE PROVISIONS

6.01 Authorized Recipients providing Contractors with escorted access to CHRI are exempt from the requirements outlined in this Outsourcing Standard if one of the following situations exist:

- The Authorized Recipient controls the Contractor's physical access to CHRI by authenticating Contractor staff before authorizing escorted access to the CHRI or the physically secure location where CHRI is stored or processed. The Authorized Recipient must escort Contractor staff at all times and monitor the Contractor's activity. The use of cameras or other electronic means used to monitor a physically secure location does not constitute an escort. Please refer to the CJISSECPOL for further information regarding the definition of the term escort.

- An Authorized Recipient may permit the Contractor remote access for privileged functions only for compelling operational needs but shall document the technical and administrative process for enabling remote access for privileged functions in the security plan for the information system. The Authorized Recipient must virtually escort Contractor staff performing remote access for privileged functions. Virtual escorting of privileged functions is permitted only when all conditions in CJISSECPOL, Maintenance (MA) control MA-4 Nonlocal Maintenance are met. Please refer to the CJISSECPOL for further information, including for the definition of the term virtual escort.

6.02 An Authorized Recipient's outsourcing agreement need only include Sections 1.0, 2.01 through 2.06, 2.08, 2.10 through 2.15, 3.01, 3.02, 3.04, 3.10 through 3.13, 3.16 through 3.19, 4.01 through 4.04, 4.07 through 4.12, and 5.0 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 outsourcing 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 outsourcing agreement 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.

6.03 The Authorized Recipient is responsible for all the actions of the contractor and shall monitor the contractor's compliance to the terms and conditions of the Outsourcing Standard for Non-Channeling. An Authorized Recipient's outsourcing agreement need only include Sections 1.0, 2.01 through 2.05, 2.08, 2.11 through 2.13a, 2.14 through 2.16, 2.19, 3.01, through 3.03, 4.01 through 4.04, 4.09 through 4.12, and 5.0 of this Outsourcing Standard for Non-Channeling when all of the following conditions exist:

1. Contractor personnel have access to CHRI while performing the duties covered by the outsourcing agreement, whether essential or incidental to the duties being performed.
2. The Authorized Recipient maintains complete control of the contractor's access to CHRI.
3. All functions requiring access to CHRI are performed within the Authorized Recipient's facility or pursuant to a remote work agreement with the Authorized Recipient and only using Authorized Recipient issued equipment that is compliant with the CJISSECPOL requirements.
4. The Authorized Recipient's personnel directly supervise the contractor personnel.
5. The Authorized Recipient retains all other duties and responsibilities for the performance of its authorized noncriminal justice administrative functions, unless it executes a separate outsourcing agreement to perform such noncriminal justice administrative functions, subject to all applicable requirements, including this Outsourcing Standard for Non-Channeling.
6. The Authorized Recipient provides security and privacy literacy training annually to contractor personnel in accordance with the CJISSECPOL.

7. The Authorized Recipient has procedures that ensure contractor personnel performing work under the outsourcing agreement is aware of the requirements of the Outsourcing Standard. These procedures include:
   a. Prior to performing work under the outsourcing agreement, contractor personnel shall provide written certification that he/she understands the Outsourcing Standard for Non-Channeling requirements and laws that apply to his/her responsibilities.
   b. Contractor personnel certification must be retained in a file subject to review during audits.
8. The Authorized Recipient has a written policy in accordance with the CJISSECPOL regarding the suspension/termination of access to CHRI and potential reinstatement of access to CHRI for contractor personnel that violate security provisions.